ELSEVIER

Journal of Hazardous Materials 130 (2006) 307–310

Journal of Hazardous Materials

www.elsevier.com/locate/jhazmat

The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: A step forward towards convergent practices in risk assessment?

Richard Gowland *

Director European Process Safety Centre, 161-189 Railway Terrace, Rugby, Warwickshire CV 21 3 HQ, UK

Available online 1 September 2005

Abstract

In the last ten years, layer of protection analysis (LOPA) emerged as a simplified form of quantitative risk assessment (QRA). The European Commission funded project Accidental Risk Assessment Methodology for Industries in the context of the Seveso 2 Directive (ARAMIS) has recently been completed. ARAMIS has several modules which give a consistent simplified approach to risk assessment which does not approach the complexity or expense of full QRA. LOPA is potentially a means of carrying out the assessment of barriers required in ARAMIS. This paper attempts to explain the principles of LOPA and the means by which it can be used within ARAMIS.

Keywords: ARAMIS; Barrier; Bow-tie; Cause–consequence; Failure mode and effect analysis (FMEA); Hazard and operability study (HAZOP); IEC 61511; Independent layers of protection; Layer of protection analysis (LOPA); MIMAH; Probability of failure on demand; Protection layer; Risk mapping; Safety integrity level (SIL); Target frequency

1. Introduction

In the late 1990s, International standards such as the International Electrotechnical Commission's (IEC) 61511 for control systems on computer controlled facilities in the process industry emerged. The task of compliance with these standards in a consistent manner led to the introduction of layer of protection analysis (LOPA) for determination of the necessary safety integrity levels (SILs) for the automated safety functions in production facilities in the chemical industry. This was conceived and promoted by the Center for Chemical Process Safety (CCPS) in the United States. LOPA has been proposed as a simplified form of quantitative risk assessment. The ARAMIS methodology has several modules which enable this. LOPA is potentially a means of carrying out the assessment of barriers required in ARAMIS. The ARAMIS methodology is able to accommodate LOPA.

The model used to picture the LOPA method was an "onion" that has several skins. These layers of protection were provided by safety systems built into:

- inherently safer process design,
- safe operating parameters,
- normal process control and safe shut down,
- mechanical devices,
- physical and organizational barriers,

which would reduce the frequency or scale of an undesired event. Additionally, where these barriers are not sufficient to prevent an incident occurring more layers might be provided by safety instrumented systems.

2. Starting the LOPA process—deciding on the 'tolerable' frequency or risk acceptance targets for an event (impact)

The user body sets its own criteria where there are none set by the governing authorities. Typically, the target is a

* Tel.: +44 1788580233.
E-mail address: Rgowland-epsc@icheme.org.uk.

0304-3894/$ – see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.jhazmat.2005.07.007

Target Frequency/yr	'Target Factor'	Impact on People	Impact on People
		On-site	Off-site
1.00E-02	2	Discomfort	
1.00E-03	3	A minor injury with no permanent health damage	Nuisance complaint.
1.00E-04	4	Serious permanent injury - one or more persons	An event requiring neighbours being told to take shelter indoors
1.00E-05	5	Single fatality	An event leading to the need to evacuate neighbours.
1.00E-06	6	5 fatalities	Minor (recoverable) injury
1.00E-07	7	More than 10 fatalities	Neighbour serious injury
1.00E-08	8	100 fatalities	Fatality
1.00E-09	9	Catastrophic event - many fatalities.	More than 1 fatality

Fig. 1. A conservative example of suggested tolerability targets from a user.

frequency for a hazardous event scenario being studied. In the LOPA study, the target frequency (the LOPA target) is the frequency which the user considers to be entering the tolerable or acceptable frequency region. Targets should vary according to an estimate of the severity of an unwanted event. An example is shown in Fig. 1.

This approach is commonly used and may vary according to the outlook and corporate standards of the user company. This will lead to variations from establishment to establishment which may not be acceptable to stakeholders. Some companies may not be in a position to set corporate standards. Clearly, where a national regulator sets some standards for tolerable individual and or societal risks, the selection task is easier. In the lack of national rules, ARAMIS provides an example similar to Fig. 1 linking the frequency target according to the severity of the event. In all cases, the methodology (MIMAH) within ARAMIS where this is not the case, ARAMIS (MIMAH) methodology offers a procedure which can achieve beneficial convergence.

3. Selecting the scenario

There are several method for selecting scenarios. Hazard and operability study (HAZOP), failure mode and effect analysis (FMEA), "What if" are three examples. Some users have been able to set up libraries of standard scenarios for their processes. This is particularly common where a company operates a similar process in several different establishments. This has been a fruitful approach since it ensures that a "core" set of scenarios is always studied and the "core" is continually updated by input from the teams studying the hazardous processes. The potential for overlooking a potentially hazardous event is thus minimised.

4. Application of the "bow-tie" concept

Within MIMAH, the ARAMIS method uses the "bow-tie" concept extensively.

When scenarios are compiled in LOPA, the initiating event, such as a failure of a process control loop, is coupled with a description of what could happen if the situation such as a leak of flammable material proceeds to the final hazardous event without intervention or mitigation. Each scenario can contain several "cause–consequence" pairs. The consequence may be then assessed for severity and "tolerable frequency" by reference to a chart such as Fig. 1. The severity estimate may be a straightforward choice or it might require for example, dispersion modelling. The "bow-tie" is a graphic representation which details the initiating event, the other factors such as probability of ignition (where applicable), probability of exposure, etc., and the safety barriers which may be present. The "bow-tie" operates as a fault/event tree, taking into account the "ANDs" (events or conditions which must both be true for a hazard to develop) and "ORs" (events or conditions, either of which, if true will allow a hazard to develop). Provided that care is taken, a cumulative risk frequency can emerge, although this may prove to be complex.

Layer of protection analysis operates in a similar way (see Fig. 2). When addressing barriers, its rules are robust enough to ensure that independence must be guaranteed

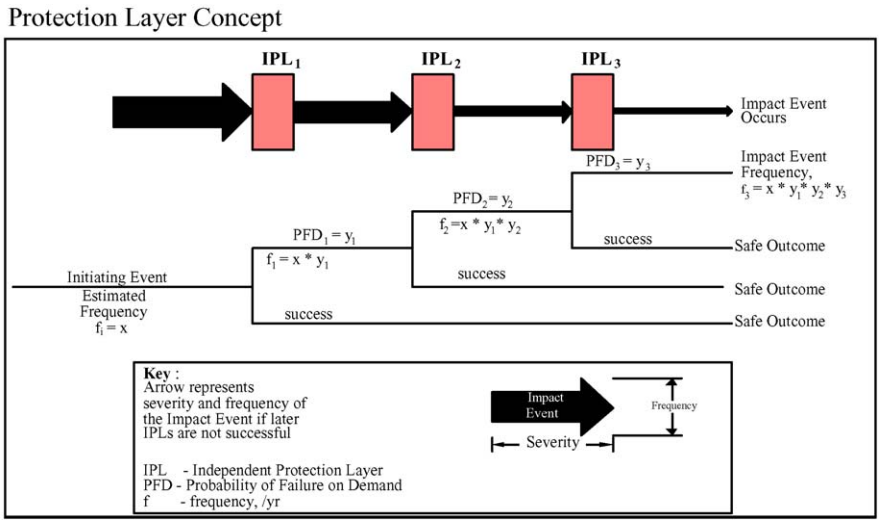

Fig. 2. CCPS.

before they can be considered legitimate. LOPA concentrates on the "ANDs". Each scenario must be studied for each of its "cause–consequence" pairs. Care needs to be taken when a single consequence can be caused by several different initiating events, thus affecting the cumulative risk. Whilst this might prove to be difficult to reconcile, most users of the method apply very conservative frequencies for initiating events and probability of failure on demand for independent layers of protection or barriers which ensure that overall risks are tolerable.

In the example shown in Fig. 2, the impact event frequency is the product of the original initiating failure event frequency and the probability of failure on demand (PFDs) of the three layers of protection. As each layer is called upon to function, the failure frequency of the entire system becomes progressively smaller. Each layer of protection needs to satisfy the definition: *A layer of protection that will prevent an unsafe scenario from progressing regardless of the initiating event or the performance of another layer of protection*. This concept of 'independence' is extremely important.

5. Barriers and their effectiveness

LOPA requires the listing of *independent* layers of protection as described earlier. Independence must guarantee that the barrier is not involved in the initiating event and does not rely on another layer of protection if that second one is already considered. The process of study and its rules are extremely good at raising legitimate doubts about true independence. This can lead to some straightforward and economical upgrading of systems where the hardware or software is present whose "architecture" which does not ensure independence. Generally, LOPA users find it easy to assess barriers which interrupt the scenario and return the process to a safe state. Difficulty is sometimes encountered when assessing the value of mitigation barriers such as containment systems, such as dikes or bunds and the true effect of procedural barriers, such as management or inspection systems. The conservative operator may ignore these barriers. Alternatively, it can be argued that they reduce the severity of the scenario.

The ARAMIS approach not only addresses the independence issue but offers a methodology to assess the performance of each barrier through evaluation of probability of failure on demand, effectiveness and response time. This applies to the hardware, software and organizational barriers considered.

The systematic approach to these matters within, for example, the management system audit, should help the LOPA user enhance his appraisal of these and allow them to be considered appropriately in his analysis. Furthermore, the ARAMIS approach specifically addresses the issues of uncertainty and sensitivity which some authorities require and which are a necessary step in any objective analysis.

6. Risk mapping

The ARAMIS risk mapping facility does not have an equivalent in LOPA. Any need for a LOPA user to plot a risk map is fully met by application of this module in the ARAMIS method.

7. Conclusion

The layer of protection analysis method has been in place for approximately 5 years and has developed with time. Several competent authorities have lent support to its application, particularly on process control and the International Electrotechnical Commission Standards relating to it. It offers

some potential advantages as a simplified quantitative risk assessment method by addressing a wider range of issues in addition to process control. Initiating events such as:

- human error,
- procedural failures,

and barrier performance such as:

- operator response,
- management systems.

Some LOPA users may have established ways of incorporating these into their study, however their task may be made easier, and greater consistency result from using the tools which are available within ARAMIS. The scope of the ARAMIS method is wider than LOPA and offers the LOPA user an opportunity to "close the loop" by assessing uncertainty, sensitivity and carrying out risk mapping. Both LOPA and ARAMIS are able to reveal gaps in the systems and provide answers on effective and economical ways to close them.

Certainly, the two approaches are compatible and each has the potential to enhance the other. A mature LOPA process can be incorporated without difficulty into an ARAMIS approach.