Chapter 8

Outline of Methods for Hazard and Risk Analysis

8.1 Introduction

Hazard and risk analysis is a large subject in itself, covered by a substantial quantity of published information. The term *hazard analysis* comprises a number of different systematic methods for identifying the hazards to be associated with a given process or plant. Such analyses can also be used as a basis for optimizing the selection of means for preventing and mitigating dust explosions.

Risk analysis consists of four major steps: identification of a representative set of failure cases, calculation of consequences, estimation of failure probabilities, and assessment of overall impact.

Cox (1986, 1987) gave an informative summary of the various techniques in use for hazard and risk analysis, which is quoted more or less literally, under the following five headings.

8.2 Hazard Surveys or Inventories

These methods are essential preliminaries to many safety studies. The survey consists of making an inventory of all stocks of hazardous material or energy and noting relevant details of storage conditions. When carried out at the conceptual stage of a project, such a survey can contribute to layout optimization and may suggest process changes to reduce stored quantities. It generates information that can be used in a preliminary risk assessment, but

the hazard survey itself is little more than a "screening" exercise designed to identify problem areas.

8.3 Hazard and Operability Studies (HAZOP) and Failure Modes and Effects Analysis (FMEA)

These two techniques have very similar objectives and methods of approach. The purpose is to identify systematically all of the possible ways in which the system investigated could fail and to evaluate these and formulate recommendations for preventive and mitigatory measures.

FMEA is the simpler of the two techniques. The procedure is to take each plant item and component in turn, list all possible failure modes and consider the consequences of each. The results are recorded in a standard format in which recommendations for action can be included. The weakness of FMEA is that there is no specified method for identifying the failure modes and their effects. The engineer is expected to do this from first principles or past experience, and the only discipline imposed on him or her is that of the reporting format itself.

HAZOP overcomes this difficulty by introducing a systematic method for identifying failure modes. This involves scrutiny of a large number of possible deviations from normal operating conditions, which are generated by applying guide words such as more, less, reverse, etc., to each of the parameters describing process conditions in each component, plant item, or line in the plant. However, HAZOP in its original form has disadvantages, and some industrial companies have modified the way in which the results of the study are handled. Instead of "recommendations," the output is "identified problems," leaving more room for a coordinated rational design revision that is not only cheaper, but also probably safer.

8.4 Analysis of Systems Reliability by Fault Tree Analysis

This method is applied to complex systems, whether the complexity is due to the nature of the process itself or to the instrumentation required for running the process. In the basic technique, the "Fault Tree Analysis," the failure modes must first be identified, e.g. by HAZOP. These failure

modes are named "top events." An example of a "top event" could be a dust explosion in a milling plant.

For each "top event." the analyst must then identify all those events or combinations of events that could lead directly to the failure. The precise logical relationship between cause and effect is expressed by AND or OR gates and is usually presented in diagrammatic form. The immediate causes of the top event have their own contributory causes, and these can be presented in a similar way so that a complete fault tree is built up. This process ceases when all of the causative factors at the bottom of the tree are of a simple kind for which frequencies of occurrence or probabilities can be estimated.

The synthesis of fault tree is a job that is best done by an engineer with good experience of the type of system under consideration. It is much easier to teach such a person how to construct a fault tree than to teach a reliability specialist everything about the system. However, the quantitative analysis of a fault tree is a separate activity in which the reliability specialist will play the dominant role.

An illustrative example of a quite comprehensive fault tree for a grain dust explosion in a grain storage facility was given by National Materials Advisory Board (1982).

8.5 Quantitative Risk Analysis by Event Tree Analysis

Quantitative risk analysis (QRA) consists of the following steps.

Failure cases are identified first by establishing the location of the main inventories of hazardous material and then by scrutinizing in detail the process flow and instrumentation diagrams using checklist methods or HAZOP.

Once the failure cases have been identified, the consequences of the failure must be calculated. Event tree analysis is a useful method in this process. An event tree is the reverse of a fault tree, starting with the initial or "bottom events" and exploring all possible "top events" that can result from it. Each outcome has further outcomes and all of these can be related by means of decision gates. At each gate the conditional probabilities must be estimated for each of the alternative branches. On this basis the probabilities of the final hazard, or 'top event', can be calculated.

Criteria have been suggested whereby calculated risks can be judged. Almost all criteria proposed so far are based on the concept of comparability with the existing general risk background. Cost/benefit and "risk perception" arguments have been advanced.

Risk analysis has been criticized by pointing at

- inaccurate mathematical models
- incomplete analysis of actual practical problem
- inaccurate primary failure probability data
- inadequate acceptability criteria
- difficulty of checking final result
- complexity and laboriousness of method

Hawksley (1989) discussed the conditions under which the various elements of quantitative risk analysis are useful in the assessment of risks in practice.

8.6 Safety Audits

Once a plant enters operation, hardware and procedures will start to change from those originally established by the commissioning team. Usually, there are good reasons for this: the plant engineers and operators may find simpler or more economic procedures, and the operational requirements themselves may change. However, it is also quite possible that safety standards fall off with time because experience of satisfactory operation leads to overconfidence and a false sense of security.

For these reasons, safety audits are used in many operating companies. These may vary from a half-day tour by the works manager to a review lasting several weeks carried out by a team of engineers covering different disciplines and independent of the regular operational management of the plant. For the most penetrating audits, the study should not be announced in advance.