DEVELOPMENTS IN RISK ASSESSMENT AND ITS APPLICATIONS IN PROCESS PLANT SAFETY STUDIES

P L Holden*

As applications of risk assessment in process plant safety have expanded, the need to be able to identify the causes of accidents and predict their likelihood and consequences has led to a considerable degree of development in the underlying techniques which, in turn, has increased their usefulness. Risk assessment has proved to be an effective tool for improving designs and for justifying the level of safety built into a plant. It now makes a major contribution to planning decisions concerning major hazard plant and regulatory controls of these plants will further extend its role. These developments have not occurred without controversy and a number of bodies have set up study groups to consider risk assessment.

INTRODUCTION

Applications of risk assessment to plant safety, involving estimation of the likelihood and severity of accidents, already has a history of at least two decades. Although the precise origins of fundamental techniques, such as fault tree analysis, are shrouded in the mists of time, the concepts and potential of risk assessment were sufficiently advanced for Farmer[1] and Starr[2] to present their seminal papers on risk criteria in the late 1960s. At about the same time the Chief Inspector of Factories, in his annual report[3], brought attention to the growing concern about the potential for accidents from plants handling large quantities of hazardous substances, now commonly referred to as "major hazards". At the present time, an authoritative study group[4] has pronounced that clear *risk criteria have not yet emerged and regulations*[5] *placing substantial duties* on the owners of certain plants, by virtue of their inventory, will come into force in stages over the next few years. In the intervening time assessment techniques have developed considerably and applications have steadily become more widespread.

DEVELOPMENTS IN ASSESSMENT TECHNIQUES

In the last fifteen years major developments in assessment techniques have been promulgated in the areas of hazard identification and consequence analysis. There have been developments associated with analytical methods, particularly in the area of computerised fault tree evaluation, by algebraic solutions or using algorithms. However, this has been a process of building on the basic techniques of fault and event tree analysis, which have proved to be capable of studying systems in ever increasing detail and complexity. These tools have proved to be extremely flexible and capable of contributing to the understanding of causes of failure in almost all types of major accident. This certainly

* Safety and Reliability Directorate, UKAEA, Culcheth, Warrington WA3 4NE

includes the analysis of active systems such as process plant and procedural operations such as loading and unloading of cargoes but also includes analysis of passive systems including structures such as dams.

Hazard Identification

In the early 1970s formalised procedures were devised for studying deviations from design intent[6] adding significantly to the methods available for Hazard Identification. This type of study, based on application of guidewords to stages in the operation or procedure and known as a Hazard and Operability Study, has proved to be one of the most powerful and useful analytical tools and rapidly become a standard technique[7]. While capable of revealing all significant deviations, the method relies upon knowledge and experience to assess whether any of the situations identified are dangerous. This type of knowledge and experience is of course an essential input to any safety study. Other inputs are also necessary: for example experience of using the technique itself. It is therefore usually recommended that this type of study is best carried out by a multi-disciplinary team, carefully selected to bring together the various backgrounds required in a particular case.

Although fault tree analysis generally does not lend itself to such a formalised team approach, it is important to remember that the same variety of ingredients are necessary. A common criticism of fault tree analysis as a hazard identification technique is that omissions may occur and that checking for completeness can be difficult. However, there is also no guarantee of complete hazard identification using the Hazop method. Not only may deviations not be recognised as being hazardous, but also the highly methodical procedure is not usually applied to all possible combinations of deviations: in practice this would be impossible for all but the simplest systems. The fault tree approach in fact provides a very strong prompt for the analyst to consider pathways to dangerous situations and experience and benchmark tests[8] have shown it to be a highly effective hazard identification method. However, it can only be applied practicably to a limited number of critical events or systems in a study whereas it is quite feasible to apply Hazop to an entire design. Most authors conclude that no single procedure is ideal for hazard identification, that the choice of approach depends on the particular case for study and that complementary use of different techniques is often beneficial. It should however be noted that Hazop can only fruitfully be applied to active systems or procedures, where there is some process or operation taking place from which deviations may occur. Other methods must be used for passive systems.

Consequence Analysis

In recent years a large amount of theoretical and experimental work has been carried out on the modelling of the effects of accidents involving hazardous substances. For example, only a decade ago, there were very few papers available on the dispersion in the atmosphere of gas clouds heavier than air, despite the preponderance of materials with a molecular weight greater than that of air amongst the gases handled in bulk quantities, such as chlorine and LPG. Indeed, it was probably only the growing emphasis on research into dense gas dispersion which revealed what perhaps should have been clear enough from observations of accidents - that gases with a lower molecular weight than air could, under some circumstances, form denser than air gas clouds, notably ammonia[9]. In the years since Van Ulden's paper[10] on heavy gas theory and experiments the subject has progressed to the point where the technical knowledge and interest can support entire volumes and symposia dedicated to it. The understanding of the phenomena of clouds dispersing over open, flat terrain

has progressed to the point where it is worthwhile and feasible to start considering the modelling of features of real situations such as obstacles and topography.

Although the progress in other areas of consequence analysis may not have been so dramatic, confidence in the ability to estimate the effects of events has improved, particularly in the case of combustion events such as pool fires and fireballs. Comparison of predictions with data from accidents generally reinforces the belief that the predictions, although by no means precise, are meaningful. (See for example, two comparisons with fireball case histories in Reference 11). There is now generally greater confidence in estimates of the consequences of an event than in estimates of its likelihood of occurrence, whereas a decade ago it was usually the other way around. Some sort of consequence analysis will be necessary to meet the requirements of CIMAH regulations[5] 10, 11 and 12, covering emergency plans and information to persons liable to be affected by an accident. The availability of satisfactory calculational methods to carry out the necessary analysis is therefore of great importance.

The predictions of analytical models have tended to overestimate consequences compared with accident experience, particularly for large toxic releases. It has generally been assumed that a major cause of this has been the use of simplifying assumptions which usually, although not always, introduced an element of conservatism by ignoring potentially mitigating factors such as evacuation, escape, taking shelter and medical treatment. The availability of improved basic methods for prediction of the variation in the intensity of dangerous effects with distance from the source means that some of these simplifying assumptions could now be replaced with analysis. However, the benefit from potentially mitigating factors does not necessarily materialise in practice and so caution is required. The recent disaster at Bhopal may show that, under some circumstances, the large numbers of casualties predicted in assessments can be realistic. For example, it would clearly be unjustifiable to take too much account of emergency and medical services if, in the event of a large accident, such services were likely to be overwhelmed. These and other factors may have varying degrees of effect depending on the specific circumstances and this should be taken into account probabilistically.

However, it has become increasingly apparent in recent years that the greatest uncertainty in the assessment of toxic releases is due to the paucity of relevant toxicity data. The effects of this on hazard range predictions for ammonia and chlorine were studied by Griffiths and Megson[12]. Statements released to the press soon after the accident at Bhopal inferred that the effects of exposure to methyl isocyanate were virtually unknown. In fact the effects seem to correspond all too well with what was known. In terms of knowledge of its toxicology, methyl isocyanate is not amongst the best documented of the substances listed in the CIMAH regulations[5] and the underlying CEC directive[13] but it is by no means the worst.

Estimates of Event Frequency

Although more information is being published on the probability of occurrence of events there is generally a very limited amount of data available on which to base assessments. Although human error is a particularly important contributor to uncertainty in many studies, in practice the major problem in taking design decisions is usually identification of possible errors: although there will always be uncertainty there is some basis for taking decisions concerning the significance of errors once identified. There is considerable

scope to improve the available data base on failures of all kinds. However, it is important to acknowledge that there will never be completely satisfactory probability data. It has been pointed out[14] that this is why a probabilistic approach must be adopted, otherwise things would just be a matter of statistics. The real test is whether meaningful results can be obtained. Improvements in the data, although desirable, may only produce limited effects, particularly since the treatment of uncertainties is gradually becoming more sophisticated.

DEVELOPMENTS IN RISK ASSESSMENT APPLICATIONS

Probabilistic risk assessment has not yet and may never become a formal requirement of the licensing or regulation of hazardous installations. Even in the case of nuclear installations the status of risk assessment is vague, although it is a well established technique in design and safety justifications. However, it has grown considerably in importance in the nuclear field in recent years in both the USA and the UK, as shown by the presentation to the Sizewell inquiry of a full probabilistic study[15] of severe accidents for the proposed pressurised water reactor.

A number of companies in industries other than the nuclear industry have also begun to make significant use of risk assessment in the last decade, as part of their decision making process on design safety issues. In particular, formal hazard identification procedures such as Hazard and Operability Studies are now commonplace and detailed studies, including fault tree analysis are often carried out on critical areas of a design where high reliability must be ensured. Although full probabilistic studies of the likelihood and consequences of failure are relatively rare, many elements of risk assessment are routinely applied.

One common difficulty in interpreting precisely what sort of assessment has been carried out is purely semantic - what do people mean by terms such as hazard analysis and risk assessment?

Because this difficulty over the meaning of terms which are now in common usage was clearly causing difficulties, the Institution of Chemical Engineers set up a working party to consider nomenclature in risk assessment for the process industries. The resulting report[16] may help to improve matters, although it has had to recognise that some terms are used to mean different things and cannot therefore be given single, precise definitions. The report is intended to provide a useful introduction to the subject as well as recommending meanings for some 140 terms.

One of the effects of the Flixborough explosion in 1974 was a wider recognition of the potential for offsite harm and damage from severe process plant accidents. It was this concern which led a technical assessor of a public inquiry into a proposed refinery at Canvey Island, where there was already a number of similar installations, to recommend that the issue of whether the concentration of developments posed an unjustifiable level of risk to the public should be resolved by estimating the level of that risk. This was a far sighted recommendation given the status of risk assessment at that time, and it led to the Health and Safety Executive being requested to carry out an evaluation of the risks to the public, which was published in 1978[17]. Soon afterwards a study of similar plant in Holland was carried out[18] as a pilot study exercise. The Canvey report[17] and the subsequent reassessment[19] were each used in evidence and subject to cross examination at public inquiries. These major studies clearly showed that it was possible, albeit with some uncertainty and at significant expense, to estimate this kind of risk. The value of such a study

was made clear by the inspector of the most recent public inquiry into the installations at Canvey, who recorded[20] the agreement of the major parties represented that risk assessment was an essential first step in taking decisions about the safety of such installations.

The use of quantitative risk assessments in taking planning decisions has extended beyond Canvey. Several papers have been published concerning work carried out in connection with planning approval, for example[21,22]. In case one should doubt that local authorities find this kind of detailed information useful, one such authority[23] with a number of large plants retains a consultant to carry out assessments and give advice on developments at or adjacent to the plants, additional to that given by HSE which is necessarily limited by the number of cases which they have to consider. This local authority finds the cost of such studies is justified by the information gained.

There can be little doubt that the CIMAH regulations[5] will lead to wider application of risk assessment techniques. As we have seen, some elements of risk assessment will be virtually necessitated by the introduction of the regulations and, although probabilistic methods are not explicitly required, they may well prove a convenient and useful way of showing that the obligations have been met. This would be expected to lead to a wider awareness of the capability of the techniques. As experience becomes more widespread, organisations who have not yet made use of the methods may find benefits in applying this experience to their other plants as part of their design and safety procedures.

Risk assessment has become established more rapidly in areas which might be described as being "new" or at least "young" technology - not just the nuclear industry but, for example, the offshore industry. However, industries with a longer history are now finding it harder to sustain the view that a good safety record alone is proof of satisfactory standards. Risk assessment will therefore probably gain much wider application, beyond the mainstream chemical and process industries, wherever major accidents could occur.

One other trend which is likely to develop is for a more rigorous estimation of the entire risk associated with an activity and its alternatives: for example, the inclusion of transport of a hazardous substance and possibly its use as well as processing and storage. Such "whole cycle" assessments have, of course, been attempted for competing electricity generating systems[24] and assessments of transport operations, although growing in importance, are hardly new[25].

THE VALUE OF RISK ASSESSMENT

There is a consensus amongst practitioners of risk assessment that the value of carrying out assessments goes beyond the provision of numerical estimates which provide an input to decision making. The insights gained into engineering and safety issues, particularly into what is important and what is not, are generally not attainable by any other means and are often insensitive to the considerable uncertainty usually present in the overall estimates. The contribution of risk assessment to safe operation, which is often doubted, stems mainly from the discipline enforced by the need to ask searching questions and obtain detailed information and understanding in order to carry out the analysis. More often than not, this reveals weaknesses or the need for further study or for more information to be obtained. In most cases these discoveries could have been made without carrying out a risk assessment but, in practice,

they generally would not have been. This is primarily because the risk assessment approach provides a structure on which to base safety programmes, clarifies and orders the available information and helps to ensure that relevant knowledge and experience is brought to bear.

Quantitative information on the benefit to safety from adopting this approach has been given by Illidge[26] of ICI. During the 1970s ICI introduced a methodical system of hazard analysis, based on rigorous identification of hazards on selected plants, quantitative estimation of the residual risk to staff onsite and comparison with a target based on accident statistics. This resulted in a dramatic decrease in the accident rate attributed to "process risks" over a ten year period, from 2.9 to 0.5 per 10^8 man hours, saving 27 lives while increasing total plant costs by only 0.1 to 0.2%. There is no basis for believing that traditional safety methods could have gained a similar reduction, at least not for such a small cost penalty.

Applications which rely on estimates of risk to the public have proved the most controversial. The debate over criteria for public risk has, to date, only produced tentative guidelines for risk to individuals, leaving judgements on societal risk to remain largely a matter for case by case consideration[4]. Further, publication of risk studies is traditionally considered to focus attention on the easily understood maximum potential consequences, while probability estimates, even when related to the chance of death by other causes, are often assumed to be incomprehensible to the layman. However, in practice, publication of risk assessments has not led to public alarm about the possibility of accidents. It has provided a common language for dialogue between the various parties involved, which has proved particularly useful at public inquiries. The most useful feature is often the avoidance of an insistence on absolute safety, which removes the understandable urge to ban all activities which present any danger. Having recognised that absolute safety cannot be guaranteed, the acceptability of a situation becomes a matter of the degree of risk. There is little alternative to attempting to evaluate this risk if one wishes to demonstrate that the controls adopted are appropriate.

CURRENT VIEWS ON RISK ASSESSMENT

Risk assessment has steadily become a significant feature in taking safety decisions - initially internally in some large organisations, but increasingly playing a role in discussions with planning and regulatory authorities. This progress has not been without controversy and many papers attacking the validity and usefulness of the probabilistic approach have been published. A number of study groups have been set up to consider risk assessment, most notably by the Royal Society[4] but, more specifically to the process industries, by CONCAWE, an organisation of downstream oil industry companies and by the Loss Prevention Working Party of the European Federation of Chemical Engineers.

The CONCAWE study group examined the implications of risk assessment for the oil refining sector of industry and reported in 1982[27]. They concluded that the rigorous analytical procedures for risk assessment have the potential to contribute to better decisions on risk reduction measures and that these methods will be used increasingly to rank hazards, compare technical alternatives and determine cost effectiveness. Their main reservations concerned human factors and the accuracy of consequence analysis.

The EFCE International Study Group on Risk Analysis (ISGRA) was set up in 1980 with a wide membership covering industry, regulatory bodies, research institutions, insurance and universities, drawn from 11 European Countries

report[28] is due to be published in early 1985. ISGRA stressed the importance of hazard identification, whether or not the risks are subsequently quantified. The procedures for hazard identification were considered to be the best developed element of risk analysis. Like the CONCAWE study group, their conclusions include recognition of the definite advantages available to plant safety from the intelligent use of risk assessment, including an improved understanding of the relative importance of failure causes and the development of improved designs. In the public sphere ISGRA recognised that cultural attitudes and regulatory frameworks are different in the various European countries, notwithstanding harmonised legislation following on from CEC directives such as the "Seveso" directive[16]. ISGRA was concerned about the apparent certainty of the numerical output of risk analysis, which could be attractive to some regulatory bodies and could lead to the sentencing of proposals by comparison with arbitrary risk criteria. In some countries there may be a danger of such an absolutist approach, if risk assessment becomes a legal requirement. The ISGRA view was that this could be counterproductive, diverting attention away from genuine improvements to safety and therefore not necessarily leading to safer plants. A much more flexible approach is required to achieve an acceptable balance between the often competing political, social and economic demands. ISGRA also concluded that the future role of risk assessment will depend on its ability to provide information which can be understood and used in decision making in industry and in the public sphere.

Both the CONCAWE and ISGRA reports emphasise the importance of the more traditional elements of process plant safety in the form of design standards, good engineering, operating procedures, qualified personnel and good management. Indeed, risk assessment has never been put forward as a replacement for any of these, but rather as a means of judging the adequacy of these factors in particular situations.

CONCLUSIONS

The assessment of acute risks from large inventories of hazardous substances has matured considerably over the last decade. The availability of such techniques can be shown to have played a major role in improving designs and reducing risks without prohibitive costs. It is increasingly accepted that the only rationale for accepting a large potential for harm is the low probability of that harm being realised, based on an evaluation of the stringency of the controls adopted, which should reflect the potential for harm. The recent major accidents at Mexico City and Bhopal reinforce the need for planning and regulatory controls. Risk assessment will provide a valuable tool for demonstrating that an appropriate level of safety is engineered into a plant and its operation. It is therefore almost certain to continue to grow in importance in process plant safety and is likely to continue to find applications in other fields where a large potential for harm exists.

ACKNOWLEDGEMENT

The author acknowledges the permission of the United Kingdom Atomic Energy Authority to publish this paper which contains personal views which do not necessarily reflect the views or policy of the UKAEA.

REFERENCES

1 FARMER F R, (1967) Nuclear Safety Vol 8, No 6, 539-548.

2 STARR C, (1969) Science, Vol 165, 1232-1238.

3 Factory Inspectorate, (1967) Annual Report of Chief Inspector of Factories. HMSO.

4 The Royal Society, (1983) Risk Assessment. A Study Group Report.

5 Control of Industrial Major Accident Hazards Regulations SI 1902, 1984.

6 LAWLEY H G, (1974) Chem Eng Prog Vol 70, No 4, 45-56.

7 A Guide to Hazard and Operability Studies. Chemical Industries Association, London, 1977.

8 Private Communication.

9 HADDOCK S R and WILLIAMS R J, (1978) The Density of an Ammonia Cloud in the Early Stages of Atmospheric Dispersion. UKAEA Report SRD R103, also published (1979). J Chem Tech Biotechnol 29, 655-672.

10 VAN ULDEN A P, (1974) Loss Prevention Symposium, The Netherlands, pp221-226. Elsevier, Amsterdam.

11 HYMES I, (1983) The Physiological and Pathological Effects of Thermal Radiation. UKAEA Report SRD R275.

12 GRIFFITHS R F and MEGSON L C, (1984) Atmospheric Environment Vol 18, No 6, 1195-1206.

13 Council of the European Communities, (1982) Directive 82/501/EEC.

14 LEVINE S and STETSON F, (1984) Nuclear Engineering International, Vol 19 No 350, 38-43.

15 GITTUS J H, (1983) CEGB Proof of Evidence to Sizewell B Public Enquiry on Degraded Core Analysis. CEGB/P/16 Vols 1 and 2.

16 Nomenclature for Hazard and Risk Assessment in the Process Industries. I Chem E. (1985).

17 Health and Safety Executive (1978) Canvey, An Investigation. HMSO.

18 COVO Steering Committee (1982) Risk Analysis of Six Potentially Hazardous Industrial Objects in the Rijnmond Area, a Pilot Study. Reidel.

19 Health and Safety Executive, (1981) Canvey, A Second Report. HMSO.

20 DE PIRO A, (1982) British Gas Methane Terminal, Canvey Island. Report of the Inquiry Inspector. Dept of Environment. London.

21 RAMSAY C G, SYLVESTER-EVANS R and ENGLISH M A, (1982) I Chem E Symp Ser 71, 335-351.

22 CONSIDINE M, (1983) I Chem E Symp Ser 80, I23-I35.

23 BROUGH C, (1984) The Attitudes of Local Planning Authorities to Risk Management. The Management and Regulation of Technological Risk, University of Manchester, June 1984.

24 COHEN A V and PRITCHARD D K, (1980) Comparative Risks of Electricity Production Systems: A Critical Survey of the Literature. HSE Research Paper 11, HMSO.

25 WESTBROOK G W, (1974) Loss Prevention Symposium, The Netherlands, pp197-210. Elsevier, Amsterdam.

26 ILLIDGE J T, (1983) Loss Prevention Bulletin 053, p1-6. I Chem E.

27 CONCAWE (1982) Methodologies for Hazard Analysis and Risk Assessment in the Petroleum Refining and Storage Industry. Report No 10/82 CONCAWE, Den Haag, Netherlands. For Synopsis see Hope S, (1983) I Chem E Symp Ser 80, B1-B8.

28 Risk Analysis in the Process Industries: A Report by the International Study Group on Risk Analysis. I Chem E (1985).