*Journal of Hazardous Materials*, 6 (1982) 249—260
Elsevier Scientific Publishing Company, Amsterdam — Printed in The Netherlands


# IMPROVING RISK ASSESSMENT METHODS FOR PROCESS PLANT

R.A. COX
*Technica Ltd., 11 John Street, London WC1N 2EB (Gt. Britain)*
(Received July 6, 1981; accepted November 4, 1981)

## Summary

This paper considers the usefulness of risk assessment in the analysis of hazards due to chemical process plant and similar installations. Risk assessment is first defined as a technique in which the probabilities and consequences of all possible accidents are quantified. The outputs from such an analysis may take the form of 'frequency versus magnitude' graphs, contours of constant risk or overall average rates of death or injury. The applications of the technique include siting and layout studies, comparison of alternative designs, ordering priorities for remedial action and setting insurance rates. Criticisms of the method include: inaccuracy (mainly in the probabilities); incompleteness; difficulty of checking final results; inadequate criteria for evaluating the results; and complexity and laboriousness of the method. Each of these criticisms is considered in the paper, and it is concluded that, while they all have some merit, the problems they represent can be overcome. Moreover, risk assessment is the only method available for dealing with the inherently probabilistic nature of the problems. Finally, priorities for future improvements in the methods are identified; these include achieving a consensus regarding the prediction of consequences and probabilities, developing labour-saving analytical techniques, and testing the final results against the actual experience of accidents.

## 1.0 Introduction

This paper examines the current state of the art in risk assessment of chemical process plant, firstly by reviewing the usefulness of the technique in different applications, and secondly by consideration of the various criticisms of risk assessment that have been made in recent months, and the lessons that can be learned from them. Finally, guidance is given on the likely avenues for future improvements.

To avoid any possible confusion, it is important to state at the outset what is meant by "risk assessment" in this paper. The essential concept is that the impact of possible process accidents is assessed by reference to both the consequences and the likelihood of those events. The evaluation is usually, but not necessarily, quantitative in nature, and for the most part the total impact of a plant is required, rather than the assessment of one particular detail. Therefore, a number of very useful loss prevention techniques, the primary purposes of which are as aids to detailed design (for example, Hazard and Operability Study and Fault Tree Analysis) are excluded from consideration here.

As will be seen later, risk assessment is most relevant at the early planning stage of a project, when fundamental decisions about location and layout have to be made. Often, these decisions are made in an atmosphere of controversy, and inevitably risk assessments have been brought into the arguments, so that the mathematical models and their results, and indeed the whole philosophy of the approach, have been closely scrutinised and questioned. This paper attempts to review all the arguments that have been put forward during debates of this kind, and to identify any implications for the future development of the subject.

## 2.0 General method of risk assessment

Although individual studies vary in content and style, they nearly all conform to a general logical structure illustrated in Fig. 1. The first step is to define a set of failure cases based on an engineering appraisal of the plant. Checklists [1] or Hazard and Operability Study [2] may be used for this purpose, and if the final objective is to evaluate the total risk impact of the whole plant, then this failure case list must be checked to ensure that it is truly representative of the spectrum of events that could actually occur — that is, there should be no gaps or overlaps between cases.

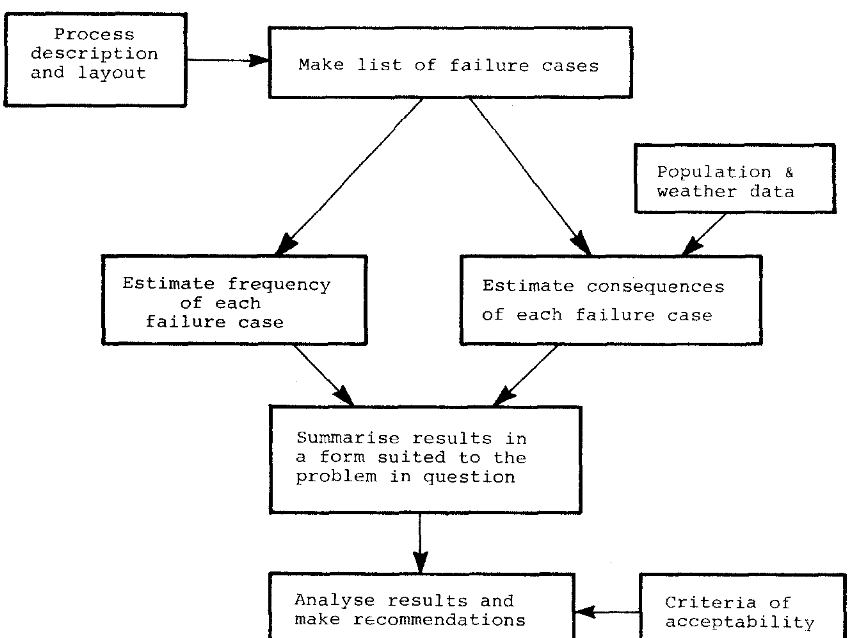


**Fig. 1. Overall logic diagram of risk assessment.**

The mathematical modelling phases, on which large amounts of research and development effort have been expended, appear in the 'Frequency' and 'Consequences' boxes of Fig. 1, and will not be discussed further in this paper because these details do not influence the main purpose here. A good example of a set of models for this purpose has been published by TNO (Netherlands Organisation for Applied Scientific Research) [3].

The key activity in the diagram is the summation of the impact of all the failure cases and the analysis of the results of this step. This can be done in various ways depending on the problem under consideration, as is now described. Note first that each failure case may have several final outcomes associated with it, depending on factors such as operator intervention and wind direction. Suppose that there are $n$ such outcomes in all, numbered 1, 2, 3, . . .$i$ . . .$n$, and for each such outcome there is a frequency $F_i$, a magnitude $C_i$ and a geographical area $A_i$ within which a given level of damage occurs. It is assumed that $F_i$, $C_i$ and $A_i$ can all be estimated using the mathematical models. It is then possible to summarise these results in many ways, but in the following ways specifically:

*2.1 Cumulative frequency curves*

These are usually presented as graphs of the frequency of events exceeding a given magnitude, $C$:

$$F(C) = \sum_i F_i \text{ (subject to } C_i > C)$$

This form of presentation is particularly useful for dealing with the problem of multiple-fatality accidents, however the curves contain no information about the geographical distribution of risk. Figure 2 is an example, calculated for an ammonia installation in Rotterdam [4].

*2.2 Contours of constant risk*

The risk at an individual point near a hazardous plant is given by:

$$R(x,y) = \sum_i F_i \text{ (subject to } A_i \text{ including the point } (x,y)).$$

If this risk is evaluated at many points on a co-ordinate grid around the plant, then 'iso-risk' lines may be drawn which are very useful for site selection and safety zone studies. However, the contours contain no information about multiple-casualty accidents. Figure 3 is an example, calculated for the same installation as Fig. 2 [4].

*2.3 Overall rate of death, injury and damage*

This type of parameter can be obtained by summation:

$$\text{Rate} = \sum_i F_i \times C_i$$

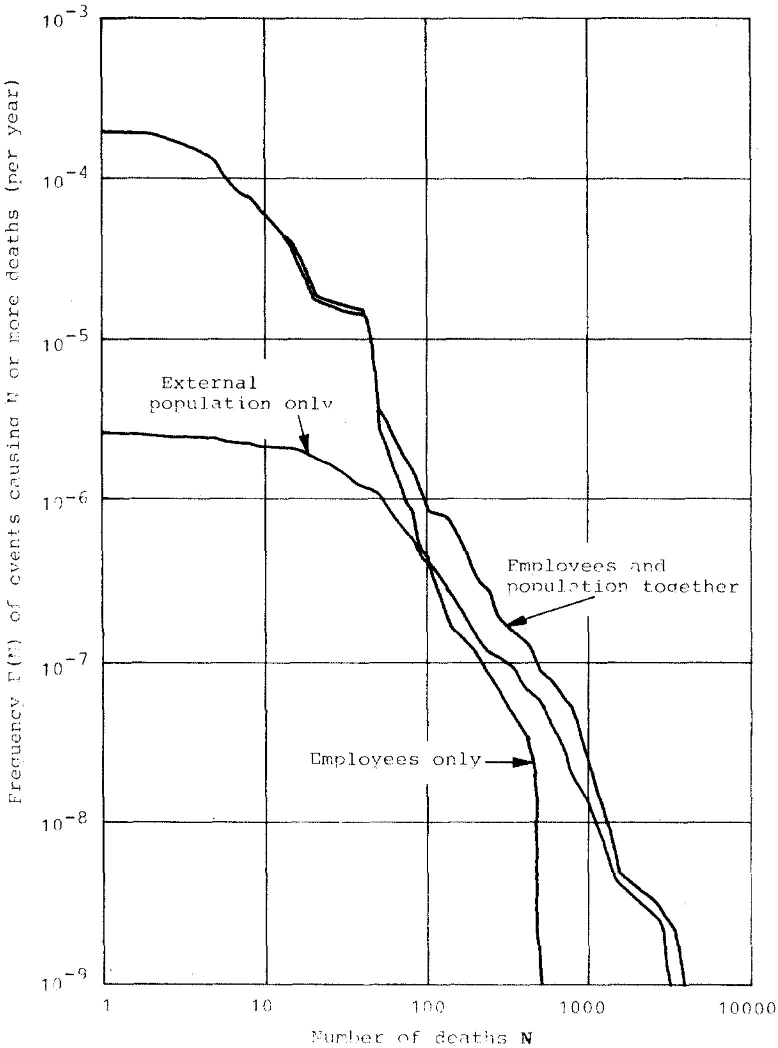


**Fig. 2. Example of cumulative frequency curves — ammonia storage installation [4].**

Clearly, it contains no information about the size spectrum of the failure cases, nor about the geographical distribution of risk, but it is argued by some to be a measure of the total 'risk cost' of the plant.

For each of these methods of presentation, the failure cases which contribute most to the risk can be identified by presenting the results for each case separately. This information can be very useful in guiding the designer towards improvements either in plant location, layout or detailed design.

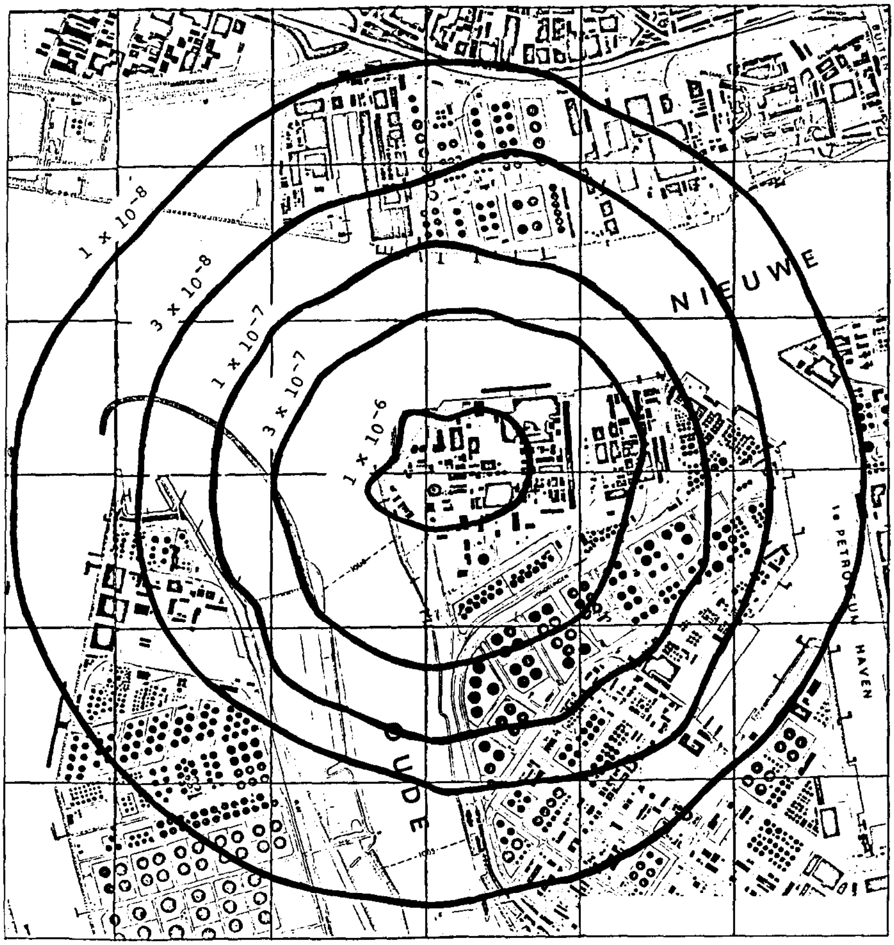


Fig. 3. Example of risk contours — ammonia storage installation [4].

## 3.0 Applications of risk assessment

### *3.1 Planning studies*

A list of typical planning problems is given below, to illustrate the sort of questions which have to be answered in practice:

(i) Should a new process plant be permitted on a particular site in its existing geographical context?

(ii) Should a new housing estate/individual residence/hospital/non-hazardous factory/hazardous factory be permitted near to an existing hazardous process plant?

(iii) Should anything be done about an existing hazard near to existing communities?

(iv) Is re-housing or compensation appropriate for residents close to the site of a new hazardous process plant?

Each of these questions involves plant-to-community interactions, so they are concerned with relatively large accidents, which are known to be very rare. Since it often happens that the maximum possible accident is so large that no practicable separation policy could completely eliminate the hazard to the community, it follows that some degree of risk has to be accommodated and the problem is to define and control it. Moreover, in the real world of government and politics, justice must not only be done, but be seen to be done. Risk assessment, in conjunction with some suitable criteria of acceptability, is very helpful in addressing this kind of problem, although the accuracy is low when the results have to be used in the form of absolute values, as here.

*3.2 Comparative studies*

It is often the case that a project could develop along several alternative lines, and economic considerations are frequently the sole determinant of the final outcome. Increasingly, however, one finds safety and environmental issues coming in at this stage, if only because of fears of delay in getting needed permissions from government. This has given rise to a few comparative studies, and for this purpose risk assessment methods accurately reflect the differences between the alternatives, although the absolute accuracy is, as always, rather poor. One of the difficulties of such comparisons, particularly where alternative process or storage schemes are considered, is in deciding between high probability/low consequence choices and low probability/high consequence ones. Here, the decision maker will always be faced with a delicate problem in trading off unlike factors, but at least risk assessment and corresponding criteria give him a rational statement of the issues and the consequences of his decision.

*3.3 Ordering priorities for action*

An examination of the results of a risk assessment, including the separate contributions of the individual failure cases, will immediately suggest the most promising areas for improvements. One can determine whether attention should be given to increasing reliability of the plant, or to reducing the consequences of failures; and the effect of proposed changes can be judged by the difference they make to the risk assessment outputs. Determining the order of priority for such actions can be done with confidence, although knowing how far to go is more difficult, because here again the results and the criteria have to be used in an absolute sense.

*3.4 Insurance*

The traditional approach used by the insurance industry for evaluating a 'risk' in financial terms has been to classify the risks and to research the actual loss history in each class. The main concern was loss of the plant itself, but now there is increasing interest in 'third party' damage. For many new plants of large hazard potential but high intrinsic reliability, the historical approach to loss rates may not suffice, because the amount of experience is too little.

Risk analysis methods, such as the 'IFAL' method evolved by the Insurance Technical Bureau [5] are being applied to this problem, and they offer a good prospect of getting insurance rates for this type of risk onto an objective basis which will be dependable in the long run.

## 4.0 Discussion of recent criticisms of risk assessment for process plant

Critics of risk assessment as applied to process plant have been concerned with five main areas:
(i) Inaccuracy of some of the mathematical models used.
(ii) Incompleteness in the analyses.
(iii) Difficulty of checking the final result.
(iv) Inadequacy of criteria of acceptability.
(v) Complexity and laboriousness of the technique.
These are discussed in the following sub-sections.

### *4.1 General accuracy considerations*

Several of the sub-models used in risk assessment have to represent highly complicated phenomena which are not always fully understood. As a result, they contain empirical elements which require calibration against large scale tests or observations from actual incidents. Often, the models have to extrapolate well beyond the range in which they have been tested, and for this reason there is a strong preference for models which are based on fundamentally sound physical or chemical principles with a minimum of empirical factors.

In the consequence analysis models, which are endless in their variety, academic arguments can be pursued almost indefinitely, but for practical purposes a consensus is emerging by degrees. For example, Havens [6] in his first review of dispersion models for LNG vapour found a factor of 50 between different predictions of cloud length for the case of a very large accidental spill of LNG — much larger than any experimental spills. This review, however, included certain models which were considered to have major theoretical weaknesses: within a short time the variation among the better current models had been reduced to a factor of 2 or thereabouts (Cox et al., [7]). Most of the models for unconfined vapour cloud explosions also give similar results.

The tendency for the latest models to agree with each other does not mean, unfortunately, that they are necessarily accurate in an absolute sense. Firstly, the same mistakes or biases may exist in several models and, secondly, the experimental data may not be adequate for calibrating all of the features of the models, some of which may be more important at large scale than at experimental scale. However, for several of the most important models, the phenomena are well enough understood to allow considerable confidence that no major omissions exist in the theory. In the specific example of LNG vapour cloud travel mentioned above, the absolute accuracy of current predictions for the straightforward case of dispersion over flat terrain in neutral stability weather conditions is therefore unlikely to be much worse than the variation between the models.

In the estimation of frequencies, the accuracy is generally much lower than for consequences, and this is the main contributor to uncertainty in the final risk values. The greatest problem is in adapting the sparse statistical data on failure rates to the particular case under study. Howland [8] points out that human error is a dominant factor in most process plant failures, and concludes therefore that failure rates calculated from equipment failure statistics are incorrect. This, however, is not a fair criticism in that the statistics do (or should) include failures actually caused through human error. Thus the statistics give a picture of both the average standard of equipment and the average standard of human error. In a given instance, the actual standards may be above, or below, the average, and Howland suggests that with some initial research effort this could be assessed in some way and a correction factor applied to the frequency values. This would only be practicable in the case of existing plant, but it is an idea which merits further study. A risk assessment at the planning stage must continue to use average statistics, relying on later audits and checks to ensure that the standards implied are actually achieved.

The problem of systematic bias throughout a chain of models is a serious one which can lead to substantial errors in the final result, particularly when several probability values have to be multiplied together. This type of error appears to have occurred in the Canvey Report [9] and was commented on by Cremer and Warner in their review [10]. The Canvey investigators followed (on instructions) a policy of 'not erring on the side of optimism' when in doubt. This seems laudable enough, but in some of the scenarios examined, a succession of pessimistic assumptions may have led to a large overestimate of risk. However, this is not a fundamental fault of risk assessment as such, and is relatively easily corrected by use of 'best estimates' instead of 'worst cases', or even better by Monte Carlo simulation where practicable.

Probably the most vehement attack on the inaccuracy of risk assessment is that of Pilz [11], who concluded, after cataloguing many of the theoretical problems, that risk analysis was 'the wrong way of doing things' and that it was not necessary in any case — at least for the purpose of finding the best solution among different design concepts. While it is understandable that this view could be held regarding detailed design matters, Pilz appears to forget that the principal use of risk assessment is in evaluating the plant/community relationship, for which neither he nor any other worker has yet suggested any adequate alternative approach. Moreover, Pilz's appraisal of the accuracy question failed to allow for the fact that the subject is in its infancy as far as chemical plant applications are concerned, and that the enormous efforts currently being made in research programmes internationally, and in the systematic collection of data on actual incidents, are bringing substantial advances in the quality of all the sub-models.

## 4.2 Completeness

### 4.2.1 Simple omissions

There is no method for guaranteeing completeness in a risk assessment. Generally, the larger failure cases are unlikely to be omitted entirely, since they can be found from an inventory of hazardous materials and their properties, but omission of particular causes of failure is of concern to designers, because it could result in an inadequate design which has a very high probability of failure. The solution to this problem, however, should properly arise at the detailed design stage, through the use of design checks and audits. It is perfectly reasonable meanwhile that industry-wide average failure rates for the failure cases should be used in a risk assessment, since these should embody all the causes of failure, including design errors. The same argument applies to omission of preventative factors.

### 4.2.2 Degree and nature of effects other than death

Bjordal [12] argued that risk analysis as it has been practised so far has omitted any mention of consequences other than death, even though these are often of great concern to society. He cites physiological and psychological effects, injury to plants and animals, aesthetic effects and vulnerability to sabotage as examples, and takes the view that people become distrustful of risk analyses when they see that these factors are not allowed for.

There can be no argument about this issue. It represents, however, a major challenge that must be met if risk analysis is to fulfil its potential. The main problem will be to extend consequence models to predict an even greater variety of effects. For injuries to people, many models can be readily adapted, but the accuracy will usually be lower than for deaths because of the difficulties of definition of the different categories of injury. However, a brief study of injury statistics and descriptions suffices to show that this is an important issue in the overall picture of risk.

For psychological and aesthetic impacts, and effects on flora and fauna, society will accept a less precise statement of the scale of possible effects — perhaps totally unquantified — provided that the issues can be seen to have been considered in an objective manner.

## 4.3 Checking the final results

Howland [8] asserts that hazard analysts do not appear to have tested the results of their studies against the known record of catastrophic events. This is largely true, although partial validation has been attempted in at least one study. Certainly, it is now the case that the best current models give predictions of the extent of damage zones which conform well to observations of actual incidents. However, the probability side is more difficult to check. Pilz [11] points out that the risk due to very rare events (which are often the large ones) tends to be underestimated by looking at history, because the observation period is too short. However, for occupational exposure, in which the risks are dominated by many small to medium failures, the predictions of risk assessment can be compared with experience. It is clear that much more work needs to be done on this aspect.

### *4.4 Criteria of acceptability*

#### *4.4.1 Absolute criteria versus cost/benefit balances*

Fixed criteria of acceptability that do not take account of the benefits of the industry are often criticised; Bjordal [12] has advocated the use of cost/benefit analyses incorporating risk assessments for deciding between alternatives, but he points out that people resist the idea of placing a monetary value on human life. This requires some delicacy in decision making when not all of the factors at stake can be expressed in the same terms.

The basic criticism of the cost/benefit approach is that in the case of major hazards, the costs and benefits usually accrue to different groups. Thus there is still a place for 'absolute' criteria in order to ensure that the risk is not distributed in a grossly inequitable way. In the context of new plant, a target level of risk of one in a million years for death of an individual who does not benefit directly from the plant has been shown to be a workable, if somewhat strict, guideline for this purpose.

#### *4.4.2 Uncertainty in 'absolute' criteria*

The criterion for societal risk published by the Provinciale Waterstaat Groningen [13] (Fig. 4) acknowledges the uncertainties involved in both the assessment of risk and the setting of criteria by defining three zones: unac-

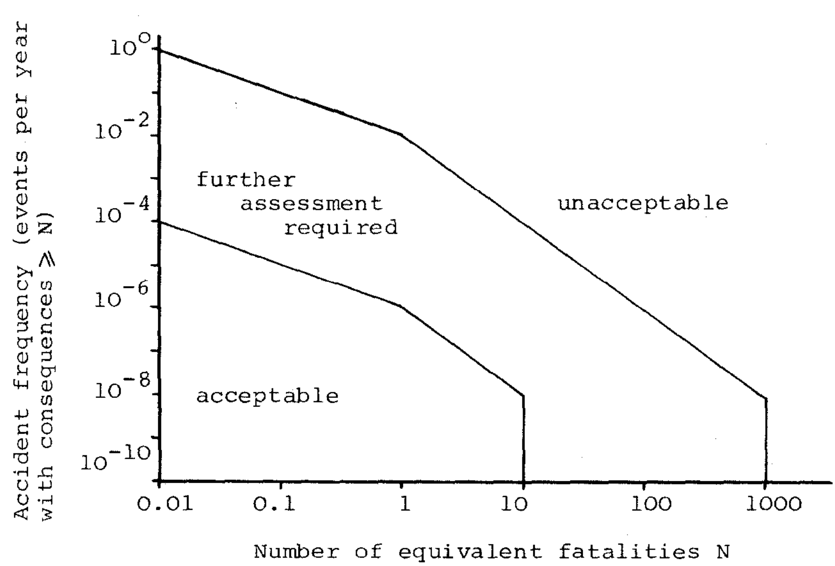


**Fig. 4. Diagram for the evaluation of societal risks suggested by the provincial authorities of Groningen, Netherlands [13].**

ceptable, acceptable, and 'requiring further assessment'. The last of these occupies a band with a width of no less than four orders of magnitude in frequency. This is perhaps too wide, for in practice almost every case examined falls inside this zone, so little is learned. Also, the 'acceptable' zone represents an extremely strict target, which could be relaxed somewhat. A case can be made for eliminating the band and drawing a single criterion line, such as the well-known Farmer curve [14], provided that the uncertainty factors are still borne in mind.

*4.4.3 Perceived risk versus actual risk*

Risk assessment of a technological kind is concerned with objective or 'actual' risk, but many workers have argued, perhaps by analogy with the working of democracy, that what matters is the way the risk is perceived by those who believe themselves to be at risk. This is to a large extent a political question, but there is considerable hope, reinforced at the Royal Society meeting on Perception and Assessment of Risk in November 1980 [15], that the results of the two approaches will converge, given time. This is because (a) education processes will tend to make the public see the risk in more rational and objective ways and (b) risk analysts will include psychological impact as one of the features of the objective risk.

*4.5 Complexity and laboriousness in risk assessment*

The US Reactor Safety Study [16], Canvey [9], Rijnmond [17] and other major studies have tended to confirm the view that risk assessment has to be highly complex and expensive to perform. Blokker et al. [17] quote a figure of two million guilders (about £500,000 at then-current rates) for the total cost of the Rijnmond study, although this figure includes the substantial costs of government and industry as well as those of the consultants who performed the work. A figure of £400,000 was given for the Canvey investigation.

It is obvious that expenditure on such a scale cannot continue to be the norm for this type of work. While a large part of these costs went towards the learning process, and should not have to be repeated, there is still a need to simplify or automate the work, so that resources remain for attending to the residual deficiencies of the technique.

**5.0 Conclusions**

The following priorities for future improvements have been highlighted in this paper:

(i) Achieving consensus of technical opinion on sub-models, frequency statistics and criteria of acceptability.
(ii) Filling gaps in the technique, especially with regard to consequences other than death.
(iii) Simplification of analytical methods.
(iv) Testing the final results against world-wide experience.

Notwithstanding the existence of deficiencies, the place of risk assessment of some kind in planning and insurance problems and for comparing alternatives and ordering priorities appears to be secure, mainly because it is the only method that can deal with the true probabilistic nature of the problems in a rational way.

## Acknowledgement

An earlier version of this paper was originally presented at the Second National Conference on Engineering Hazards, January 1981, and is now published by permission of the organisers, Oyez IBC Ltd.

## References

1 G.L. Wells, C.J. Seagrave and R.M.C. Whiteway, Flowsheeting for Safety, Institution of Chemical Engineers, Rugby, 1977, pp. 44—54.
2 Chemical Industry Safety and Health Council, A Guide to Hazard and Operability Studies, Chemical Industries Association, London, 1977.
3 TNO Bureau for Industrial Safety, Methods for the Calculation of the Physical Effects of the Escape of Dangerous Material, Directorate-General of Labour, Voorburg, Netherlands, 1980.
4 Openbaar lichaam Rijnmond, Rapport van de COVO-Stuurgroep — Risico-analyse voor zes industriële objecten in Rijnmond, Openbaar lichaam Rijnmond, Rotterdam, 1980.
5 G. Munday, H.C.D. Phillips, J. Singh and C.S. Windebank, Instantaneous fractional annual loss — a measure of the hazard of an industrial operation, Proc. 3rd. Int. Loss Prevention Symp., Basel, Sept. 15—19, 1980.
6 J.A. Havens, Predictability of LNG vapor dispersion from catastrophic spills onto water: an assessment, U.S. Coast Guard Report CG-M-09-77, 1977.
7 R.A. Cox, P.J. Comer, M.A.F. Pyman and D.H. Slater, Safety issues in the siting of modern LNG terminals, Proc. GASTECH Conf., Houston, Nov. 1979.
8 A.H. Howland, Hazard analysis and the human element, Proc. 3rd Int. Loss Prevention Symp., Basel, Sept. 15—19, 1980.
9 Health and Safety Executive, Canvey: an Investigation of Potential Hazards from Operations in the Canvey Island/Thurrock area, HMSO, London, 1978.
10 Cremer and Warner, An Analysis of the Canvey Report, Oyez Publishing Ltd., London, 1980, p. 19.
11 V. Pilz, What is wrong with risk analysis?, Proc. 3rd Int. Loss Prevention Symp., Basel, Sept. 15—19, 1980.
12 E. Bjordal, Is risk analysis obsolete?, Proc. 3rd Int. Loss Prevention Symp., Basel, Sept. 15—19, 1980.
13 Provinciale Waterstaat Groningen, Pollution control and use of norms in Groningen — criteria for risks related to dangerous goods, Groningen, Netherlands, April 1979, pp. 43—57.
14 F.R. Farmer, Siting criteria — a new approach, Paper No. SM-89/34, IAEA Symp. on containment and siting of nuclear power reactors, Vienna, April 1967.
15 The Royal Society Study Group on Risk, The Assessment and Perception of Risk, The Royal Society, London, 1981.
16 U.S. Nuclear Regulatory Commission, Reactor safety study — an assessment of accident risks in U.S. commercial nuclear power plants, Report WASH-1400, U.S. Nuclear Regulatory Commission, Germantown, Maryland, U.S.A., October 1975.
17 E.F. Blokker, R.A. Cox, H.J.D. Lans and F.H. Meppelder, Evaluation of risks associated with process industries in the Rijnmond area — a pilot study, Proc. 3rd Int. Loss Prevention Symp., Basel, Sept. 15—19, 1980.