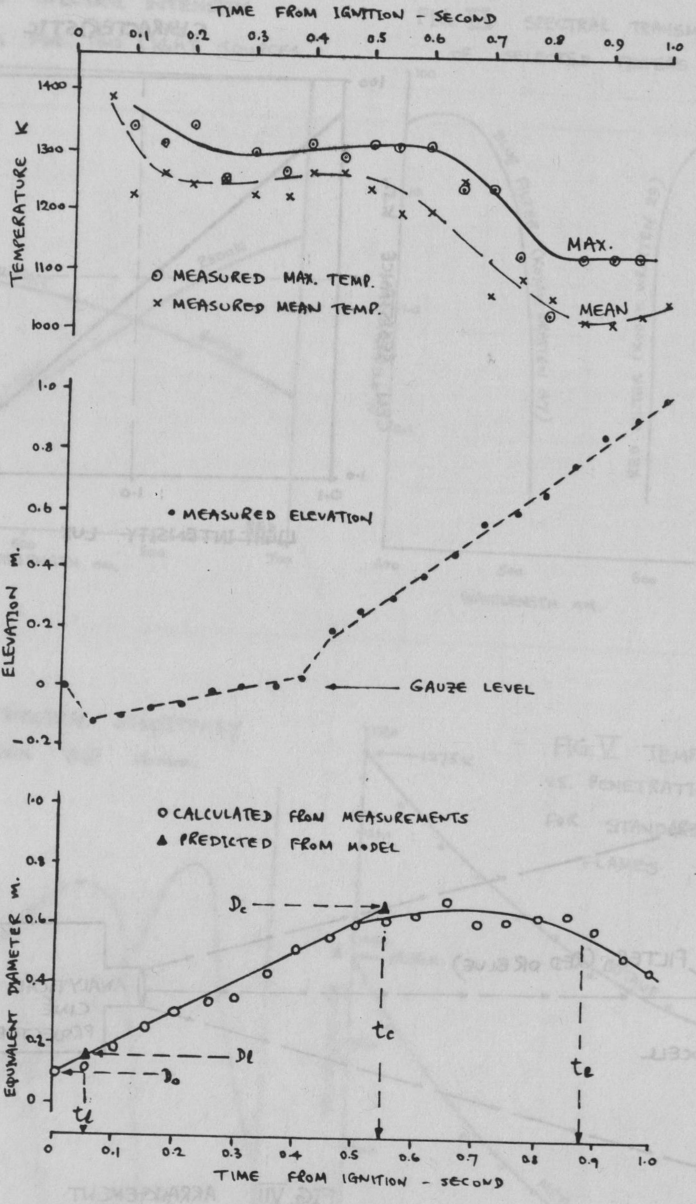

FIG. VIII TYPICAL RESULTS

400 ml. BUTANE ELEVATED CLOUD FIREBALL

QUANTITATIVE ASSESSMENT AND RELIABILITY ENGINEERING OF MAJOR HAZARD PLANTS IN THE CONTEXT OF HAZARD CONTROL

F. P. Lees*

Industry has a problem in gaining acceptance for major hazard plants. One apparent solution is the use of quantitative assessment to show that even if a hazard is very large, the risk is very small, but this approach has not been an unqualified success. Objectors keep returning to the magnitude of the hazard potential. The paper gives a review of quantitative assessment, including historical background, basic elements, regulatory requirements, problem areas and public opposition, and makes two proposals. One proposal is that there should be greater emphasis on the totality of the hazard control measures and that the principle of diversity and redundancy should be applied to the hazard control system itself. The elements of a hazard control system based on this approach are described. The other proposal is that the concept of hazard warning structure should be exploited. Most hazards have a warning structure such that there is a high probability that before the worst case accident occurs there will be a number of near misses, or warnings. The concept of hazard warning structure is described and a formal methodology, including the hazard warning tree and associated mathematics, is outlined.

INTRODUCTION

Within the last fifteen years or so the question of major hazard plants has become a serious problem for the chemical industry. The problem arises partly from the increased scale and severity of operation of plants and partly from the decreased tolerance of hazards by the public and by the regulatory authorities. The industry has responded to this problem by developing the loss prevention approach (1). An important feature of this approach is its emphasis on quantitative methods in general and on reliability engineering in particular.

The application of quantitative methods, however, is by no means uniform. Their use varies both between companies and within a company. They are most obviously valuable as an aid to evaluating alternatives and to obtaining value for money in design. Their use in the public domain in supporting planning applications and in satisfying regulatory authorities is more problematic.

It is the object of the present paper to review the various aspects of quantitative assessment, including the historical development, basic elements, regulatory requirements, problem areas and public opposition, to

* Department of Chemical Engineering, Loughborough University of Technology

describe some further developments, to outline an overall system of hazard control and to indicate the role of quantitative assessment and of reliability engineering in this system.

It is suggested that the principles of diversity and redundancy are applicable to the hazard control system itself and that the system should have a number of different elements of which quantitative assessment is one but only one. This approach appears particularly desirable in relation to hazard control in the public domain, where excessive reliance on quantitative assessment is liable to prove contentious.

One of the elements of the hazard control system proposed is new. This is the concept of the hazard warning structure of a plant. Most hazards have a warning structure such that there is a high probability that before the worst case accident occurs there will be a number of near misses, or warnings, and this probability can be quantified. It is suggested that hazard warning structure may be a useful supplement to conventional quantitative assessment.

QUANTITATIVE ASSESSMENT: HISTORICAL DEVELOPMENT

The way in which quantitative assessment has developed historically has an important bearing on its present use (2).

There appear to be three main reasons why a company gets involved in the quantitative assessment of a hazardous plant:

1) The company makes a quantitative assessment as part of the engineering measures taken to reduce the risk

2) The company makes a quantitative assessment in order to demonstrate to the community, which objects that the hazard is very large, that the risk is very small

3) A requirement for quantitative assessment is imposed on the company by the regulatory authorities.

The differences between these cases are important.

In the UK the chemical industry became involved in quantitative assessment primarily by the first route. It recognised that it had some particularly hazardous processes and decided to fit them with trip systems. In the design of these trip systems fault trees were used qualitatively to discover the fault pathways and develop a suitable instrument configuration. Fault trees were also used quantitatively to assess the accident frequency. This in turn led to the need to develop a risk criterion with which to make comparison. This process is illustrated by the development of the trip systems for ICI's ethylene oxide plant as described by Stewart(3).

This early work in the instrument field was followed by a rapid increase in the application of the techniques of relaibility engineering across the board to all kinds of engineering problem in the chemical industry, including problems of plant availability and maintenance as well as safety.

Quantitative assessment in the public domain is in the UK a later development and has followed a path intermediate between the second and third routes. It is exemplified by the studies done for the Canvey complex (4) and for the St Fergus-Moss Morran pipeline(5).

A significant feature of these two assessments is that they have been carried out not by industry itself but by the Health and Safety Executive. Industry in the UK appears somewhat hesitant about quantitative assessment in the public domain.

It is also significant that the HSE has become increasingly critical of industry's reluctance to defend its position (6). In consequence, the HSE has tended to find itself arguing industry's case for it, which is not a desirable situation.

The approach of the UK nuclear industry appears to have been somewhat different. This industry, which faced a somewhat similar although by no means identical problem rather earlier, has been more prepared to take the initiative in seeking to gain public acceptance for its plants by following the second route.

The historical development of quantitative assessment in other countries has sometimes differed from that in the UK. In some cases there appears to have been greater pressure for quantitative assessment from the regulatory authorities on companies which make relatively little use of these methods.

QUANTITATIVE ASSESSMENT: BASIC ELEMENTS

Quantitative assessment as currently practised involves the assessment of two basic features of the realisation of a hazard, the consequences and the frequency.

The assessment of the consequences is based on consideration of a set of scenarios of events occurring in the plant, and in particular of loss of containment of hazardous materials. These events give rise to phenomena such as heat radiation, overpressure and toxic concentration, which are estimated from appropriate hazard models (1, 7). The effects of these phenomena on the exposed population are then estimated from intensity-response relations, which may be formulated as probit equations (1,7, 8). In estimating the population exposure allowance may be made for mitigating features such as escape and shelter (1,9).

There are two ways in which the frequency is assessed, depending on whether or not historical frequency data are available. If data on event frequency are available and are considered applicable, the frequency may be estimated from these. If the data are sparse, the confidence limits will be wide (1,10).

A special case arises where the event has never occurred, but where a number of event-free installation-years have been accumulated. In this case it is possible to estimate to a given confidence level an upper bound on the event frequency. Again, if the number of installation-years is limited, the upper bound will be high (1, 10).

If historical data are not available for the event of interest, it is necessary to synthesise its frequency. Generally this is done using the fault tree method (9, 11 -13). It is still necessary to have historical data, but in this case the data required are those for more common events such as equipment failure and thus tend to be more readily available.

The availability of data on the event of interest determines the nature of the assessment. This is illustrated clearly in two well known hazard assessments, the Canvey Report (4)and the Rasmussen Report (9). The Canvey Report is effectively a set of hazard assessments. The assessments refer to events such as vessel failure, pipeline break, rail crash, etc. Since these events have occured in the past, though generally not with the worst consequences, historical data are available for them. Therefore it was not necessary to make synthetic frequency estimates and the report contains hardly any fault trees. The Rasmussen Report, by contrast, deals with an event, a nuclear reactor meltdown with disastrous consequences, which has never occurred and for which many layers of protection are provided. In this case it was necessary to make a synthetic estimate of the frequency and the report contains a thick appendix full of fault trees.

QUANTITATIVE ASSESSMENT: REGULATORY REQUIREMENTS

As indicated earlier, there are several reasons why quantitative assessment may be undertaken. These are to assist in the engineering design of the plant, to gain public acceptance and to satisfy the regulatory authorities.

In the UK the main application of quantitative assessment by industry is to the engineering design of the plant.

As far as statutory requirements are concerned, there is no explicit requirement to use quantitative assessment in plant design, although the Health and Safety at Work etc. Act 1974 effectively makes the duty of care, and hence of good industrial practice, a statutory one and it is arguable that good practice now includes quantitative assessment, at least in the engineering design.

Probably the clearest guidance available is that given in the Second Report of the Advisory Committee on Major Hazards (14), which gives as an appendix a set of Model Licence Conditions. The report states that regardless of whether licensing is adopted as a means of regulation, these Model Licence Conditions may be regarded as a code of practice for major hazard plants.

Quantitative assessment is dealt with in Licence Condition 5: The Arrangements for the Assessment of Hazards. This reads:

"The organisation should show that the hazards identified by means described in the preceding section have been removed or that the associated risks have been reduced to a minimal level.

In this context 'minimal' means that the probability that an employee or member of the public will be killed or injured or that property will be damaged is at least as low as in good modern industrial practice.

The method of demonstrating that the risks are at a minimal level should be comprehensive and logical.

The method may consist of

a) The use of codes of practice generally recognised in the industry
b) The use of special testing
c) The use of calculations based on appropriate data.

In many cases it will be sufficient to show for all or at least some aspects of the hazard that a generally recognised and accepted code of practice is applicable and has been followed.

Where there is any aspect of the hazard, the risk of which cannot be reduced to a minimal level by following a recognised code of practice or by special testing, then, whenever meaningful, quantitative methods should be used to demonstrate that the risk has been reduced to a minimal level. These quantitative methods will normally consist of three steps:

a) An estimate of the consequence to employees and the public

b) An estimate of the frequencies with which hazardous situations will occur

c) Comparison of (a) and (b) with the other risks to which people are normally exposed in order to show that the risk under consideration is relatively small.

The management system should contain a formal requirement that such methods of hazard assessment shall be applied.

The organisation should show that it has access to people competent to implement these methods."

The licence condition quoted is followed by a background commentary which should be consulted for further explanation and amplification.

The approach taken here is broadly on the following lines. The structure of the hazard may be envisaged in the form of a fault tree. The problem is to eliminate or minimise the contribution of the various branches of the tree. For most hazards it can be expected that the majority of branches will be taken care of by the use of codes of practice or standards but that for some branches a different approach will be necessary.

It is appropriate here to sound a note of caution concerning codes of practice. Generally codes of practice are not drawn up primarily for major hazards and this fact needs to be borne in mind in using them in the way described. If the contribution of the branch is sufficiently significant, it may still be necessary to make a further assessment even for a feature which is covered by a code. For example, in the Canvey Report the failure of pressure storage vessels was investigated, despite the fact that pressure integrity is well covered by codes, because the contribution of this branch to the overall risk was significant.

A further assessment may take several forms. The licence condition refers to special testing and to calculations. Calculations may seek to establish

1) Equivalent safety level

or

2) Absolute safety level.

The equivalent safety approach seeks to demonstrate that the proposed arrangement involves no greater risk than do other arrangements which are permitted in codes, the absolute safety approach that the proposed arrangement involves a risk which is low by some absolute standard. The latter approach therefore involves the use of a risk criterion by which to evaluate the assessed risk, while the former avoids risk criteria altogether. The equivalent safety approach is illustrated by the studies by Kletz (15) and by Lawley and Kletz (16) on the relative risks of pressure relief valves and of trip systems.

It sometimes appears to be assumed that hazard assessment is synonymous with use of fault trees, but, as indicated in the previous section, this is not so. It is necessary to use a fault tree to determine an event frequency only if data are not available and the frequency must be synthesised.

The overall approach described is illustrated by the hazard assessment scheme shown in Figure 1.

The interpretation of the licence condition depends critically on the phrase 'where meaningful'. This implies that in the first instance at least it is for the company to judge whether in a particular case quantitative assessment is a useful exercise.

The licence condition leaves open the question of the extent and type of quantitative assessment. In particular, it does not specifically call for an assessment of multiple fatality accidents to the public such as are typically represented by a frequency-scale, or fN, curve (9,17-19). In so far as it leaves the initial judgement to the company and the current practice of industry is to use quantitative assessment as an aid in engineering design, it may perhaps be regarded as biased towards this latter practice.

Another indication of possible developments in regulatory requirements is the current practice of the HSE. Here the situation is unclear. On the one hand the HSE has carried out in the Canvey Report and the St Fergus-Moss Morran Report asssessments of accidents which could involve multiple fatalities to the public and it has expressed the view that industry should be more forthcoming in arguing its own case. On the other hand it does not appear as yet to have any explicit requirement for assessments of this kind.

It may well be that the HSE considers that this is a case where it is undesirable to let regulatory requirements run too far ahead of industrial practice and of the recommendations of the ACMH.

It would be unwise, however, to assume that such quantitative assessment may not be required in due course. It seems probable that the question is one on which the ACMH may have more to say.

QUANTITATIVE ASSESSMENT: PROBLEM AREAS

There is now sufficient experience with quantitative assessment to indicate that there are a number of problem areas (20-22). Some critics consider these so serious as to call in question the validity of the whole exercise (23-24).

One main problem which is serious but relatively straightforward is that in some cases the assessed risk appears rather high (4). There are two possible explanations for this. The risk really may be high or the assessment may be pessimistic.

There is some reason to believe that estimates may be biased towards pessimism. Certainly there is a wide gap between historical experience and theoretical estimates of casualties (14). This is an area, however, in which very little has been done, although mention may be made of work by Marshall (25) on the mortality index of historical accidents and by Taylor (26,27) on validation of fault tree assessments and of comments made by Simmons, Erdmann and Naft (28) in their work on risks of chlorine transport.

Work on this problem needs to cover both hazard models and risk estimates. Weak points in current models are mixing with air during initial emission, dispersion of heavy gases over all types of terrain and of neutrally buoyant gases over plant and built-up areas, and effects of mitigating features such as escape and shelter.

Another problem which is both serious and complex is the difficulty of making estimates which are reproducible and acceptable to other workers. This difficulty has been considered by some critics to be so severe that the whole activity of quantitative assessment has been described as 'trans-science' (23).

In part this problem is caused by the opacity of some of the studies conducted. For example, the Rasmussen Report was criticised as being virtually impossible to evaluate by the normal processes of peer group assessment (22).

The other main aspect of the problem is the extent to which it is necessary to use rather inadequate data and to make rather arbitrary assumptions. Data are often sparse or non-existent. The applicability of such data as do exist is frequently open to doubt. It is generally necessary to make a number of arbitrary assumptions about data and other aspects and to use a degree of judgement. In addition, there are some particular difficulties which occur when it is necessary to synthesise frequency assessments using methods such as fault trees. One is the difficulty of being sure that all the initiating events have been identified so that the list of events is complete. Another is the possibility of common cause failure, which in a high reliability system can increase the failure frequency by orders of magnitude.

These difficulties, particularly those of data, are aggravated if the quantitative assessment is in the public domain. Practices which are adequate where the technique is used as an aid in engineering design appear dubious and contentious where they are used to provide absolute estimates of risk.

A third problem, and perhaps the most difficult, is the acceptability of the risks assessed. A set of risk criteria has been developed by industrial workers (29-31) covering the risk to individual employees and to individual members of the public and risk of multiple fatality accidents. The question of acceptable risk and of risk criteria is a complex one and has generated a considerable literature (9,32-36). Also it is one which is not a purely engineering matter and to which other disciplines have a contribution to make. Here it is sufficient to note only a few salient points. The use of quantitative assessment as an aid in engineering design is now quite widespread in industry and so also is the use of a criterion for risk to an individual employee. The most widely utilised criterion appears to be the Fatal Accident Rate (FAR), originally termed Fatal Accident Frequency Rate (FAFR) (29). On the other hand, there is, not unnaturally, much less agreement on, and much greater reluctance to use, a criterion for large multiple fatality accidents. In so far as there is a criterion it tends to be the frequency-scale, or fN, curve. Some experts have put considerable effort into the development of this criterion, but in contrast to the FAR there are few published examples of its use (19).

QUANTITATIVE ASSESSMENT: PUBLIC OPPOSITION

Increasingly quantitative assessment is being used as a means of gaining public acceptance of major hazard plants, but it is apparent that this has been only partially successful.

The arguments come most sharply into focus when there is a public inquiry. Generally the company presents a hazard survey which describes in qualitative terms the nature of the hazard and the measures taken to control it. Often this does not satisfy the objectors, who emphasise repeatedly the scale of the hazard. The logical development is that the company then presents a quantitative assessment which seeks to demonstrate that although the hazard is large, the probability of its realisation during the life of the plant is very small. In practice, industry itself has appeared reluctant to get involved in quantitative assessment in the public domain. It is the HSE which has taken the lead in making public such assessments.

Sometimes the objections are based on the fact that the assessed risk is high. In some cases this may be due to the use of pessimistic models. It may be expected that in due course this difficulty will be resolved as the models become more refined. In other cases the risk really may be high. The correct course is then to take measures,appropriate to the severity of the hazard, to reduce the risk.

A more fundamental problem arises where the assessed risk is low but the objections are still sustained. The opposition may deploy various arguments. It may emphasise the difficulties involved in quantitative assessment, which were described in the previous section, and may express a lack of confidence in the results obtained. Or it may go further. It may accept the figures given for the assessed risk but may still argue that for such a hazard any risk is too great. The result is an impasse.

Faced with this situation it is probably futile simply to go on refining the methods and the criteria. It is necessary to seek alternative approaches.

One such approach is to try to get away from too great a reliance on quantitative assessment and to develop a diversity of methods of which quantitative assessment is one but only one.

Another approach is to seek to give greater assurance that the quantitative assessment is correct and that, if it is not, there will be adequate warnings and appropriate action.

These two approaches are now described.

HAZARD CONTROL SYSTEM

In reliability work generally it is a basic principle to exploit diversity and redundancy in order to achieve reliability and, equally important, credibility. This philosophy is applicable to the hazard control system itself.

It is convenient to describe the hazard control system proposed in terms of the system required by the regulatory authorities. It should be emphasised, however, that the prime responsibility for control of the hazards which it creates lies with industry itself and that therefore most of the activities described should be undertaken in the first instance by the company.

Elements of a hazard control system based on the approach proposed include the following:

1) Notification and survey arrangements
2) Major hazard code
3) Hazard reviews

   a) Hazard potential
   b) Inherent safety
   c) Cost benefit

4) Exposure reviews

   a) Employee exposure
   b) Public exposure and siting guidelines

5) Conventional hazard assessment

   a) Employee risk
   b) Public risk

6) Hazard warning structure assessment.

Item 1 is covered by the draft Hazardous Installations (Notification and Survey) Regulations 1978 (37). These regulations are still held up pending resolution of the related EEC Directive, but this can hardly be delayed much longer.

As already mentioned,the Model Licence Conditions in the Second Report of the ACMH (14) constitute a code of practice for major hazard plants and thus cover item 2. This is a rather comprehensive code and its application to all major hazard plants would go a long way towards ensuring that all plants meet the standards of the best.

The most fundamental principle of hazard control is that if reasonably practicable the hazard should be eliminated or at least reduced. This is covered by item 3, which comprises a review of the hazard potential of the proposed plant, of any more inherently safe alternatives and of the cost benefit of the plant and the alternatives.

The concept of inherent safety as a design objective has been strongly urged, particularly by Kletz (38), and it appears to be finding increasing acceptance. Licence Condition 10 of the ACMH Model Licence Conditions, which deals with documentation, contains a requirement for the following:

"A statement of any less hazardous process which could have been used and the reasons for selecting the particular process

> in question. This might include outstanding economic advantages, factors relating to the availability of raw materials, the avoidance of particularly difficult engineering operations or the necessity of making a product of a particular purity."

As yet, however, it is not apparent what the impact of this approach will be or how far the regulatory authorities will wish to go in pressing it. What is clear is that inherent safety has an important contribution to make to the reduction of hazard potential.

A particular aspect of inherent safety is the limitation of inventory. The importance of the limitation of inventory was emphasised in the Flixborough Report (39). Licence Condition 10 of the ACMH also contains a requirement for the following:

> "A statement of the inventory of all hazardous materials in process and of the steps taken to keep this at the lowest level consistent with safe and efficient operation."

The concept of cost benefit is perhaps more problematic. The cost benefit approach is essentially an attempt to reduce the different aspects of the decision on a hazard to a common scale of measurement by which they can be evaluated (36). Whatever view is taken of some of the more contentious applications of the method, the decision on a major hazard plant must inevitably involve a cost benefit assessment of some kind. Indeed the concept of 'reasonably practicable', which underlies British safety legislation in general and the HSWA in particular, implies a judgement on cost benefit.

The limitation of the hazard potential needs to be complemented by the limitation of exposure to the hazard of people, whether employees or public. The limitation of exposure of personnel is discussed in detail in the Second Report of the ACMH (14) and is the subject of Licence Condition 7: The Arrangements for the Minimisation of Exposure of Personnel.

The limitation of the exposure of the public is equally important but appears as yet to be less well developed. The two reports of the ACMH (14,40) have said relatively little on this and on siting. It is known, however, that the HSE is working on guidelines for siting of and, presumably, for population density near to major hazard plants. The question is one to which the ACMH may be expected to return.

Conventional hazard assessment, which has already been discussed in some detail, is covered by item 5. Generally, the discipline of hazard assessment proves to be invaluable irrespective of the risk values obtained. The latter, although therefore not the sole benefit of the assessment, are nevertheless important also. Two types of hazard assessment are listed. One is hazard assessment conducted as an aid in engineering design dealing primarily with employee risk and using typically the FAR criterion. The other is hazard assessment in the public domain dealing primarily with public risk, especially large multiple fatality accidents, and using typically the fN curve criterion.

While it seems probable that the latter type of hazard assessment will also come into use, this is not certain. Assuming, however, that it is accepted, it is important that it be used properly. Its proper role is as one element in a total system. Thus satisfaction of the associated risk criterion, say an fN curve, is then a necessary but not sufficient condition for acceptance of the proposed plant. This approach helps to avoid putting on hazard assessment a weight which alone it is not able to bear.

Finally, in item 6 there is introduced the concept of hazard warning structure (41), which may be briefly summarised as follows. The warning structure of most hazards is such that there is a high probability that before the worst case accident occurs there will be a number of near misses, or warnings, and this probability can be quantified. The hazard warning structure approach can therefore be used to give assurance that even if the main hazard assessment is deficient and the risk is greater than assessed, there is nevertheless a high probability that there will be a number of warnings and that if such warnings occur, appropriate action will be taken. The concept of hazard warning structure is discussed more fully in the next section.

HAZARD WARNING STRUCTURE

The ratio of lesser accidents to the worst case accident is high and often very high. This fact is generally appreciated. It is the basis of the accident pyramid and of the total loss control approach (42,43).

Thus most hazards have a structure such that before the worst case accident occurs there is a high probability that a number of lesser accidents, or 'near misses', will occur. This also is generally understood. It underlies the concept of learning from near misses.

In effect, there is a hazard warning structure. The implications of this structure appear, however,not to be fully appreciated or exploited. The step which has not been taken is to apply the concept in a formal way in real time to the monitoring of the hazards on an operating plant and to use the fact that such monitoring will be done to enhance the credibility of the original hazard assessment.

The hazard warning structure can be analysed by formal methods. One of the most widely used representations of hazard structure is the fault tree. For the analysis of hazard warning structure it is convenient to use a hazard warning tree. A hazard warning tree is a special kind of fault tree which is constructed according to a particular convention. This convention is that a severer accident is represented as the outcome of a lesser accident and of the failure of a mitigating feature.

A typical hazard warning tree is illustrated in Figure 2. The top event T is a worst case accident, the base event B is the lesser accident and the condition C is the failure of the mitigating feature. If the frequencies of events T and B are λ_1 and λ_2, respectively, and if condition C occurs on a proportion p of occasions

$$\lambda_1 = p\,\lambda_2 \qquad (1)$$

Over a given time interval t the probability $\overline{P}_T(t)$ that the top event will not occur is

$$\overline{P}_T(t) = \exp(-\lambda_1 t) \qquad (2)$$

The probability $P_B(t,k \geqslant n)$ that the base event will occur at least n times is

$$P_B(t,k \geqslant n) = 1 - \exp(-\lambda_2 t) \sum_{k=o}^{n-1} \frac{(\lambda_2 t)^k}{k!} \qquad (3)$$

Then it can readily be shown that the probability $\overline{W}(t,k \geqslant m)$ that there will not be at least n warning base events is

$$\overline{W}(t,k \geqslant n) = 1 - \overline{P}_T(t) P_B(t,k \geqslant n) \qquad (4)$$

In order to exploit fully the concept of hazard warning structure it is necessary to do a formal analysis using methods such as those just described. This means defining severer accidents and expressing them as the outcome of lesser accidents and of failure of mitigating features. These may then be represented in the form of a hazard warning tree.

It is then possible using the equations given to calculate the probability that a worst case accident will not be preceded by a given number of lesser accidents or warnings, i.e. the probability of the failure of warning. Generally, if the risk of the worst case accident is itself low, the risk of failure of warning will also be low.

The number of warnings which hazards may be expected to give varies. Some will give more warnings than others. In other words, there are high and low warning hazards.

This feature of hazard structure is illustrated by some of the assessed risks (before proposed modifications) given in the Canvey Report as shown in Table 1. The figure in the first column is approximately equal to the sum of those in the second and third columns. The ratio of the figure in the second column to that in the first column gives the proportion of occasions when the accident is a near miss in the sense that it causes no offsite casualties. For items 1-4 this ratio as high, for items 5-7 low and for item 8 zero. In this sense these sets of hazards are high, low and zero warning, respectively.

The concept of hazard warning structure has been developed in the first instance as a means of enhancing the credibility of conventional hazard assessment. A hazard assessment can be used to demonstrate that the risk of a worst case accident is very low. By itself, however, such hazard assessment may lack the degree of credibility necessary where the hazard potential is very large. It may be complemented, therefore, by a hazard warning structure assessment which demonstrates that the risk that the worst case accident will not be preceded by some specified number of warnings is also very low.

The hazard warning structure assessment may then be used at the stage of planning, siting and design to give the following reassurance. A threshold number of lesser accidents will be set. If the number of lesser accidents which occurs during operation is much less than the threshold, there is good assurance that the hazard assessment is not seriously defective and that the hazard is under control. If, however, the number of lesser accidents approaches the threshold, action will be taken.

At the stage of the operation the hazard warning structure makes it possible to interpret any lesser accidents, or near misses, which do occur and to give good assurance that despite these accidents the hazard is under control.

It will be apparent that it is more difficult to apply this approach to a low warning hazard. However, it is generally highly undesirable to let such a hazard persist. Instead the attempt should be made to alter its warning structure. Apart from the fact that it gives few warnings, a low warning hazard tends also to have a higher risk.

The concept of hazard warning structure is in the first instance a tool for the company, but it will be apparent that it is also well adapted to the requirements of the regulatory authorities.

A more detailed account of hazard warning structure has been given in another paper (41).

A slightly different but related concept, that of risk reduction by shared experience, has been put forward by Bowen (44) in Appendix 24 of the Canvey Report. This is discussed more fully in the paper just mentioned (41).

HAZARD SEVERITY STRUCTURE

There is another feature of hazard structure to which attention needs to be drawn. This is the frequency-scale, or fN, structure of actual hazards as revealed by hazard assessment. This feature has already been mentioned by Kletz (31).

This aspect of hazard structure is illustrated by some of the assessed risks from the Canvey Report which were given in Table 1. A selection of these risks are plotted as fN curves in Figure 3. The important feature is that in contrast to most fN curves which are proposed in the literature as risk criteria, these curves for assessed risks of actual hazards do not exhibit a rapid decrease in the frequency f as the number N of casualties increases.

The hazard severity structure of actual hazards thus appears from this evidence to be rather different from that which tends to be implicitly assumed in constructing risk criteria. On the other hand further work may show that these results are an artefact of the way in which these assessments have been done.

It is not appropriate to purse this point here, but it is clearly an important one.

CONCLUSIONS

The application of quantitative methods to the hazard assessment of chemical plants is now widespread. The principle of quantification is well established, but the practice has revealed a number of problems and the precise role of quantitative assessment is not fully defined. In particular, the use of quantitative assessment as a means of gaining public acceptance of major hazard plants has not been an unqualified success.

Two main proposals have been made in this paper to try to overcome this problem. One is to place greater emphasis on the totality of measures taken to control the hazard and thus to apply the principle of diversity and redundancy to the hazard control system itself. The elements of a hazard control system based on this approach have been described.

The other proposal is the use of the concept of hazard warning structure as a means of enhancing the credibility of the conventional quantitative assessment. A formal methodology, including the hazard warning tree and

and associated mathematics, has been outlined.

SYMBOLS USED

n	= number of events or warnings
p	= probability
P(t)	= probability of event
P(t,k≥ n)	= probability that event will occur at least n times
t	= time (y)
W(t,k≥ n)	= probability that there will be at least n warnings
λ	= event rate (events/y)

Subscript

B	= base event
T	= top event

Superscript

—	= negation

REFERENCES

1. Lees, F. P., 1980, Loss Prevention in the Process Industries (Butterworths, London).

2. Lees, F. P., 1980, Chem. Engr, Lond., 363, 736.

3. Stewart, R.M., 1971, in Major Loss Prevention in the Process Industries, p.99, IChemE, London.

4. Health and Safety Executive, 1978, Canvey: An Investigation of Potential Hazards from Operations in the Canvey Island/Thurrock Area (HMSO, London).

5. Health and Safety Executive, 1978, A Safety Evaluation of the Proposed St. Fergus to Moss Morran Natural Gas Liquids and St. Fergus to Boddam Gas Pipelines, London.

6. Dunster, H.J. and Vinck, W., 1979, Nuclear Engng Int., August.

7. Eisenberg, N.A., Lynch, C.J. and Breeding, R.J., 1975, Vulnerability Model. A Simulation System for Assessing Damage Resulting from Marine Spills, Nat. Tech. Inf. Serv., Springfield, Va.

8. Finney, D.J., 1971, Probit Analysis (Cambridge Univ. Press, London).

9. Atomic Energy Commission, 1975, Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plant, Rep. WASH 1400, Washington, D.C.

10. Green, A.E. and Bourne, A.J., 1972, Reliability Technology (Wiley, New York).

11. Haasl, D.F., 1965, "Advanced concepts in fault tree analysis",System Safety Symposium, The Boeing Co., Seattle, Wash.

12. Barlow, R.E., Fussell, J.B. and Singpurwalla, N.D. (eds), 1975, Reliability and Fault Tree Analysis (Soc. for Ind. and Appl. Mathematics, Philadelphia, Pa).

13. Fussell, J.B., 1976, in Henley, E.J. and Lynn J.W. (eds) Generic Techniques in System Reliability Assessment, p.133 (Noordhoff, Leyden).

14. Harvey, B.H. (chrmn), 1979, Second Report of the Advisory Committee on Major Hazards (HMSO, London).

15. Kletz, T.A., 1974, Chem. Processing, 20 (9), 77.

16. Lawley, H. G. and Kletz, T.A., 1975, Chem. Engng, Albany, 82 May 12, 81.

17. Farmer, F. R., 1967, J.Br.Nucl. Energy Soc., 6 (3), 219.

18. Griffiths, R. F., 1981, in Griffiths,R. F., op.cit., p.54.

19. Lees, F. P., 1981, Chem. Engr, Lond., 366, 121.

20. Fairley, W. B., 1977, in Fairley,W.B. and Mosteller, F., Statistics and Public Policy, p.331 (Addison Wesley, Reading, Mass.).

21. Davis, L.N., 1979, Frozen Fire (Friends of the Earth, San Francisco).

22. Lewis, H.W. (chrmn), 1978, Risk Assessment Review Group Report to the U.S. Nuclear Regulatory Commission, Nuclear Regulatory Commission, Rep. NUREG/CR-0400, Washington, D.C.

23. Weinberg, A.M.,1972, Minerva, 10,209.

24. Critchley, O.H., 1976, J.Br. Nucl. Energy Soc.,15 (1), 18.

25. Marshall, V.C., 1977, Chem. Engr, Lond., 323, 573.

26. Taylor, A., 1979, "Comparison of predicted and actual hazard rates", Second Nat. Reliab. Conf.

27. Taylor, A., 1981, in Reliable Production in the Process Industries, p.105,IChemE, Rugby.

28. Simmons, J.A., Erdmann, R.C. and Naft, B.N. , 1974 , "Risk assessment of large spills of hazardous materials", Nat. Conf. on Control of Hazardous Material Spills, San Francisco, Calif.

29. Kletz, T.A., 1971, in Major Loss Prevention in the Process Industries, p.75, IChemE, London.

30. Kletz, T.A., 1976, "The application of hazard analysis to risks to the public at large", World Cong. Chem. Engng, Amsterdam.

31. Kletz, T.A., 1981, "Hazard analysis - a review of criteria", unpublished paper.

32. Lowrance, W. W., 1976, Of Acceptable Risk (William Kaufman, Los Altos, Calif.).

33. Rowe, W. D., 1977, An Anatomy of Risk (Wiley, New York).

34. Council for Science and Society, 1977, The Acceptability of Risks (Barry Rose, London).

35. Warner, Sir F. and Slater, D.H. (eds), 1981, The Assessment and Perception of Risk (Royal Society, London).

36. Griffiths, R. F. (ed.),1981, Dealing with Risk (Manchester Univ. Press, Manchester).

37. Hazardous Installations (Notification and Survey) Regulations 1978 (draft) (HMSO, London).

38. Kletz, T.A., 1978, Chemy Ind. May 6, 287.

39. Parker, R.J. (chrmn), 1975, The Flixborough Disaster. Report of the Court of Inquiry (HMSO, London).

40. Harvey, B.H. (chrmn), 1976, First Report of the Advisory Committee on Major Hazards (HMSO, London).

41. Lees, F. P., "The hazard warning structure of major hazards ", Trans. IChemE, under review

42. Heinrich, H.W., 1959, Industrial Accident Prevention, 4th ed. (McGraw-Hill, New York).

43. Bird, F.E. and Germain, G.L., 1966, Damage Control (Am. Mgmt. Ass., New York).

44. Bowen, J.H., 1978, in Health and Safety Executive, op.cit. (Ref.4), p 190.

ERRATA

Quantitative Assessment and Reliability Engineering of Major Hazards Plants in the Context of Hazard Control by F.P. Lees

Further work has indicated defects in equation (4) as a hazard warning index. A more appropriate index may be obtained by replacing equation (3) and (4) as follows:

$$P_B\,(t, k \leqslant n) = \exp\,(-\lambda_2\,t) \sum_{k=o}^{n} \frac{(\lambda_2\,t)^k}{k!} \qquad (3)$$

$$P_T\,(t,k \leqslant n) = \exp\,(-\lambda_2\,t) \sum_{k=1}^{n} p(k)\,\frac{(\lambda_2\,t)^k}{k!} \qquad (4)$$

$$p(k) = \sum_{j=1}^{k} (-1)^{j-1} \binom{k}{j}\, p^j \qquad (5)$$

$$\overline{W}\,(t,k \geqslant n) = P_T\,(t,k \leqslant n) \qquad (6)$$

A fuller description of this index is given in Reference 41.

TABLE 1 - Some assessed risks given in the Canvey Report (before proposed modifications)(4)

Hazard	Frequencies in units of 10^{-6}/y								
	Frequency of initiating event	Frequencies for numbers of offsite casualties exceeding							
		0	10	1500	3000	4500	6000	12000	18000
1. Oil overtopping of bund by process explosion (Occidental)	1000	975	25	18	8	4	-	-	-
2. LPG ship collision	6640	6490	196	124	64	31	-	-	-
3. LNG ship collision remote from jetty	50	45	5	3	1	0.5	0.3	0.2	0.1
4. LNG jetty incident	2000	1830	168	118	83	56	37	16	7
5. Ammonia storage sphere spontaneous failure	100	30	68	40	28	21	15	7	3
6. Ammonia ship collision	375	140	235	153	122	96	72	54	41
7. HF release (Occidental)	200	30	168	144	132	120	114	80	70
8. Ammonium nitrate storage explosion	85	0	85	85	85	17	17	_	-

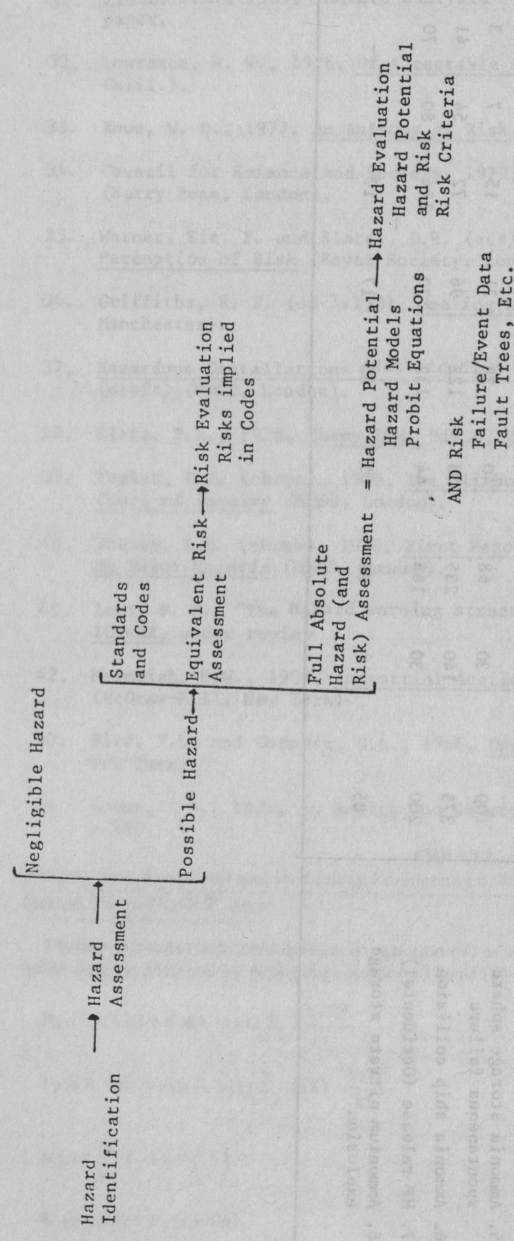

Figure 1 . A hazard assessment scheme

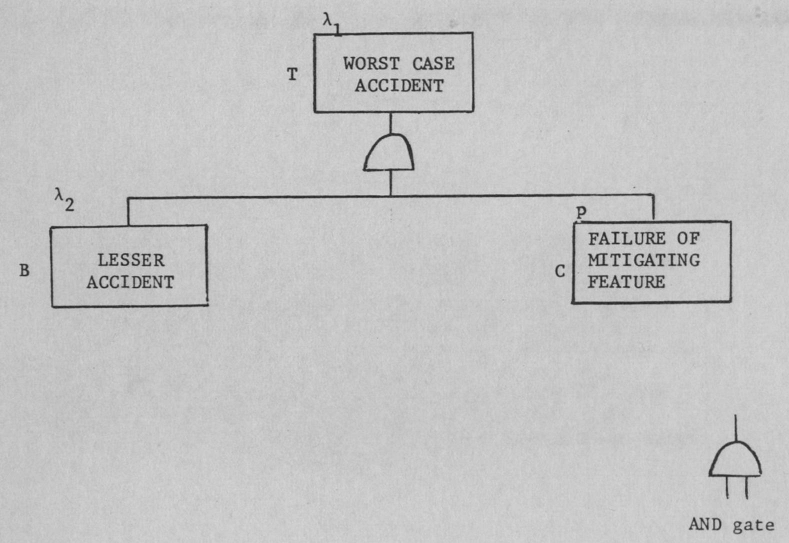

Figure 2 A hazard warning tree

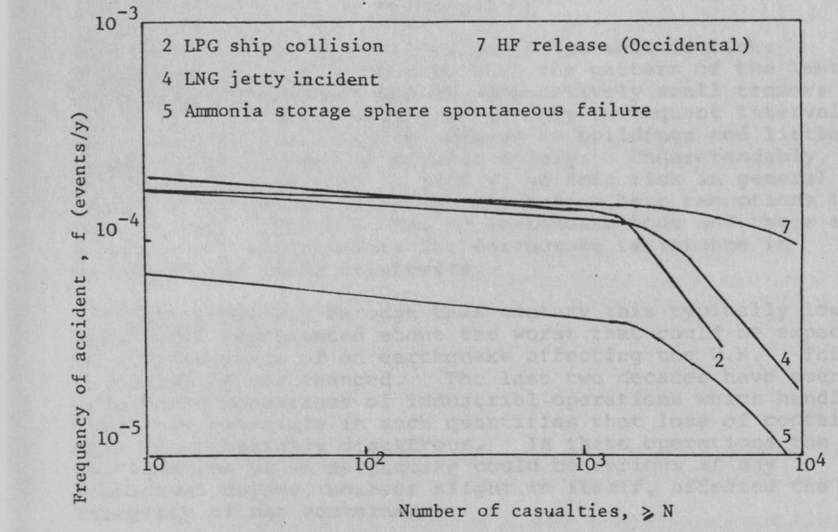

Figure 3. A frequency-scale, or fN curve, for some assessed risks given in the Canvey Report (before proposed modifications) (4)