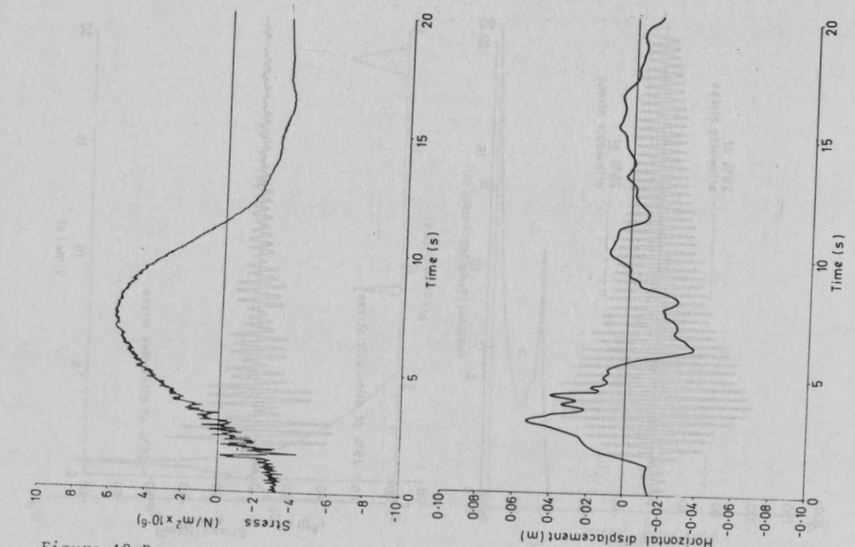

Figure 18 Response to Level 2,torpedo on rock,horizontal shear stress in leg

Figure 19 Response to Level 3,torpedo on rock,horizontal displacement

PROBLEMS IN HAZARD ANALYSIS AND RISK ASSESSMENT

N C HARRIS*

The increasingly widespread use of hazard analysis and risk assessment techniques is disclosing major problems in the execution or the understanding of such work. This paper reviews a selection of the many problems and indicates in some cases how this work may be improved. Examples of risk assessment in the transportation of hazardous materials are used to illustrate some of these problems, and how they are slowly being improved. There are nevertheless many aspects which will not be readily improved and where confidence in the predictions must remain low, necessitating extra care in their preparation and use.

INTRODUCTION

Hazard Analysis and Risk Assessment are terms of fairly recent origin, so it is not surprising that the techniques to which they refer are in many cases still under-developed and often misunderstood. There is nevertheless a rapidly growing use of the techniques in many parts of the world and at the same time a substantial amount of misunderstanding of them, what they can achieve (and what they cannot achieve) and how the results should be viewed by those either receiving them or sponsoring the work.

This paper attempts to distil out some of the principal problems which are involved, whether in carrying out asessments or in utilising the results, and also to suggest how some on the difficulties might be surmounted. It forms part of a session on Risk Analysis and is thus presented to those who are already, or may be, involved in this type of work. But it is also of interest to those outside the Risk Analysis and Assessment field who may require to call for such a study or who may be involved in decision making as a result of such a study. It is important not to forget that these people often have difficulty in understanding Hazard Analysis, or may take apparently irrational decisions as a result of lack of understanding of the report they receive, so it is vital that those actually conducting the work and writing it up bear this in mind and discharge their responsibility to present a fully reasoned and calculated assessment, which can be a true and positive contribution to the improvement of safety.

* Imperial Chemical Industries PLC, Mond Division, Runcorn

NCH/f/A03

First, let us be sure we know the meaning of the terms as used in this paper.

DEFINITIONS

Hazard - A physical situation with a potential for harm to life or limb.

Risk - The probability that a hazard may be realised at any specified level in a given span of time; or the probability that an individual may suffer a specified level of injury as a result of the realisation of a hazard in a given span of time.

Analysis - The process whereby hazards are identified and examined.

Assessment - The process whereby the hazards which have been identified are quantified in order to provide a value for the level of risk.

I have not developed any new definition for hazard and risk, but have used those favoured by the Advisory Committee on Major Hazards (1). There are one or two more which will be included in later sections.

It should now be clear what is meant here by the compound terms Hazard Analysis and Risk Assessment. They are often mis-quoted.

HAZARD ANALYSIS

No Assessment can properly be carried out unless some type of Hazard Analysis is first conducted. It is perhaps the most important section, and if not carried out correctly or in an adequate depth for the purpose required, it can undermine any subsequent quantification or assessment. It can take a variety of forms, which I will briefly describe, and I will indicate some of the problems or limitations which each of these may introduce. Later I will suggest the conditions under which they could be selected.

Two of these are based on the Fault or Event Tree, which is essentially the logical system of displaying the required sequence of faults or events which can cause a hazard to develop. Sometimes more than one event can lead to a hazard, and they are therefore alternative routes, which are linked diagramatically by an "OR" gate. On other occasions it may be necessary for two (or more) events to occur simultaneously in order for a hazard to develop. These events are linked diagramatically by an "AND" gate.

A simple example of a Fault Tree is shown in Fig 1 taken from (2) and describes events associated with the operation of a typical distillation unit. The initiating events or contributory events are shown at the bottom, leading to the top where the eventual hazard is shown. It resembles a tree, with a broad base linked in stages up the tree to the tip or main hazard - the origin of the term Fault Tree. How this fault tree is developed is the basis of the two methods of Hazard Analysis, each showing a large number of detailed differences of a lesser nature. There are many variants, some of which have been discussed in an American survey (3), but the following sections consider the main approaches.

The Top-Down Approach

In this method one first seeks to identify the main hazard (or hazards) one requires to consider. Careful consideration of how this event may arise from the preceeding faults or events will lead to the next layer being identified, and the process is repeated until lower layers are reached. There is a need to have some experience of this way of examining or analysing the problem in order to be proficient at it. Everybody must have his own first attempts to gain experience, and this is best achieved by working through the exercise in conjunction with experienced personnel.

By working down through successive layers, which become more extensive and usually very much more complicated, one is in fact following the top-down approach. There is then the question of how far down one must go. It is perhaps best answered at this point by saying, when an adequate appreciation of the relationship of all the lesser faults or events is obtained, or the ability to quantify with confidence has been reduced.

The Bottom-Up Approach

This is essentially the reverse of the top-down approach, and requires the examination and analysis of a large number of small faults or events, and the development of an event tree from it, progressing upwards to the ultimate hazard. The problem faced here is deciding at what level of subsidiary event to start, although it will be inevitable that the events initially examined will not fall into a single level but into several. Also, many of these events, if progressed upwards, will not lead to a hazard. This approach can take several forms in the way it is tackled, as for example following a Hazard and Operability study ("Hazop") (4), or a Failure Mode and Effect Analysis (FMEA), or a Fault Tree Analysis, a description of one of many techniques is given by Fussell, (5).

Which to Select?

There is really no golden rule, but there are some useful and important guidelines. In all cases the method selected will depend on the objective of the overall exercise and on a set of constraints.

In many of the exercises which are conducted there is a set of constraints, covering time, cost, resource availability etc. If these are exceptionally tight, or for example an answer is required in a day or two, the top-down approach is the one normally followed. By following through the minimum number of layers necessary to obtain a reasonable answer, much effort is in fact saved. One has covered the minimum number of decision points in the fault tree and a final answer has been obtained.

Or has it? It will of course assume that in the lowest level examined, all such events which ultimately contribute to the final major event have been considered and that none has been excluded. Whether this is true or not will depend on the circumstances, but it certainly does not follow that it is complete. In cases where the top-down exercise has been compared with a bottom-up hazard analysis, the latter usually produces more potential events and never less. This in part is due to the top-down approach having been a shorter exercise, but the use of a thorough hazard identification process, such as Hazop, is vital to the need to identify the maximum number of potential events possible. To those who will find that the top-down approach is the only practicable one then, a word of

warning. Do not leave the reader with the impression that a thorough job has been done with nothing left out. Declare the known shortcomings of the method.

Development of improved or simpler methods continues by many organisations, but it is vitally important that simplification is not only worthwhile but is reliable with respect to avoiding down-grading of the assessed risks. Care needs to be exercised when producing or using the results of methods still under development.

ACCEPTABILITY OF RISKS

When discussing the assessment of risk it was said that the numerical value for the level of risk is required in order to compare it with some other value. This might be the level of risk assessed for an alternative method of operation, the comparison then showing which of the two levels is the greater, and by how much. It is again important to bear in mind the degree of accuracy of such estimates since it may not be possible, or correct, to state conclusively that one level is in fact greater than the other, merely to indicate that they are probably of the same order. Nevertheless this is one of the more useful ways of using quantification.

The other comparison that can be made is one of acceptability, to be judged usually against a numerical value for acceptability of risk or a target level. The entire problem of acceptability of risk is one that has been taxing many brains throughout the world for some considerable time, and although progress has been made, the solution is still far from clear. As well as perhaps varying in acceptability to different people, it is likely that there will be different levels in different circumstances, and more recent publications are leaning towards bands outside which risks are either acceptable or unacceptable, and between these limits require further consideration to see what action has to be taken.

Comparable Risks

There are two basic types of risk which are frequently calculated and compared with statistically derived risks for other occupations and activities. These are individual risks and societal risks.

Individual risks:- This is usually a calculation of the risk of death to an individual. It may be a peak risk such as the Fatal Accident Rate to the individual at most risk, or a mean value such as the risk per person per year. It is also relatively simple to compare it with risks similarly calculated, and similarly accepted.

Societal risks:- In this case an estimate is made of the number of people who are expected to be killed in a community at risk, and the frequency with which such events may happen. Several sets of data are normally calculated, resulting in f-n type data, discussed later. Comparisons with other risks are now more difficult to display.

There are many aspects which require special care when conducting such comparisons. For example individual risks from a variety of activities are often displayed in tables, and are obtained by dividing the number of fatalities in the period by the number of people exposed. Or at least so one presumes, yet so often the denominator is simply taken as the population of the country. What proportion of the population for instance smokes or fly?. There is thus a real need for more care and precision in preparing such tabulations. A good example of providing adequate descriptions is Grist (6) who is concerned with average individual risk. Ideally they should all include the following:-

Reference Country - hopefully the same country throughout since standards of acceptability vary.

Reference period - many risks are in fact falling steadily over the years.

No of fatalities in period - from a properly defined classification. Such definitions often exist in national statistical data, but these too vary from country to country.

Risk rate, deaths/person/year - implying a specific population exposed. If not the total national population, the figure used ought to be stated.

This leads to the next aspect, the problem of sub-dividing the table into voluntary and involuntary risks. Accidents at work and deaths from smoking are among these which are normally classed as voluntarily undertaken. But the statistics for smoking may in fact include some non-smokers. Similarly deaths from drowning may have occurred to both those who went swimming and those who fell overboard. Road accidents also present a problem in this respect, and there is a very useful exposition of problems in this area by Sabey and Taylor (7).

A further difficulty comes with the examination of acceptability. Some people are nowadays clamouring for a zero risk situation, believing perhaps that it is either possible to provide (which it will never be) or that it can be made zero to them in some other way, say by relocation, or that it will be possible to do without the activity altogether (albeit at greater cost not always recognised). Much has been written on these topics, and considerable care is necessary in establishing levels of risk which are acceptable to enough people, those affected/those who are not, those who benefit/those who do not, etc. For further elaboration of this very complex issue see for instance Rowe (8), Otway (9), the Council for Science and Society (10), Gibson (11) and Kletz (12), and for a new approach to risk aversion, the subjective influence on attitudes to risk acceptability, see Apostolakis et al (13).

f-n and F-N Curves

Although there are no formally agreed definitions of the two types, it is important to be able to differentiate between the f-n curve and the F-N curve. The former is little more than a curve drawn from a histogram of frequencies (f) of incidents causing n fatalities. The latter is a curve or ogive which describes the frequency (F) of incidents involving N or more fatalities. The F-N curve can be drawn from the f-n curve, but it is important that enough intervals are considered in preparing the curve to give it adequate definition. However excessive sub-division of

the f-n data may infer an unjustifiable level of accuracy and possibly suggest an artificially low frequency caused by such sub-division. In order to sub-divide with confidence, good quality consequence estimates will be necessary, but in practice this is an area where confidence and validation are as yet poor. Thus some compromise is required, and the assessment must declare the assumptions and limitations involved to help those appraising it understand its true status. The F-N curve is being increasingly used to illustrate the relative values of F-N for different types of risk.

Validation

Perhaps the most important feature of any model or sub-model, which describes in mathematical terms the processes occurring in one or more sequence of events, is the degree to which it provides a reliable prediction of events. The way this is normally tested is to subject real events to prediction by the model, where the events have been adequately described in quantitative terms. At this point it is obvious that the problem is usually in identifying events which are accurately described and quantified in the literature or records and which could be used for testing the model.

The basic choice of validation method is between an overall validation of a large complex model, and the validation of each and every sub-model of which the model is composed. Very often it is not possible to identify events which will produce an overall validation, and even when such data is available it is essential that a large variety is tested since it is all too easy with limited data to validate only one aspect of a complex model. Consequently one is usually attempting to validate all sub-models. Some of these are relatively simple to complete, but some may be very difficult. It is in these areas that considerable effort is now needed in order to provide adequate validation of many models now in use.

Attempts at validation of some models have been inadequate since they have not covered the broad spectrum of conditions which might be expected to prevail. It is important that these deficiencies are recognised and effort is directed at improving these models so that they can be useful and not dubious contributors to safety. One major model which is difficult to validate is the US Coast Guards Vulnerability Model (14) and there has been much criticism of its application when inadequately validated. This aspect is now receiving special attention.

Some of the problem areas are now discussed.

Human Error

In the search for improved methods of quantification of risks, much effort is put into obtaining appropriate failure data of suitable accuracy and confidence. This is acknowledged to be a difficult problem, but the continuing gain in experience in reliability engineering undoubtedly has improved confidence in failure data. A word or two of caution is however essential, lest one were tempted to believe the absoluteness of such data.

The experience of those who are engaged in data collection, especially in the process industries, now confirms the important contribution of human error, and this is an aspect where any hope of precision is lacking. Indeed it is well known how variable human behaviour can be, so any

values used must be average values with a large variation. Human involvement occurs in virtually all activities, and can be found in design, manufacture, construction, testing, operation and maintenance. All such aspects ought to be considered if an extensive fault tree were to be prepared, with each of the nodes incorporating the risk of human error intervening. For example many such fault trees limit themselves to - alarm operates: operator responds/fails to respond correctly. Since the effect on a quantification exercise can be so large, major investigation of this problem is essential before any decision to simplify is made.

Common Mode

In recent years awareness by risk assessors of the existence of common mode failure has increased, and the problems resulting are sometimes better identified. It is however a difficult concept to master, since it can appear in a wide variety of forms. To quote a few examples; the existence of a single power supply (ie no redundancy), instruments of a particular type being incorrectly (though consistently) manufactured or repaired, use of duplicate (or triplicate) alarm or trip equipment of the same type when diversity could eliminate the risk of common mode. This latter example would suggest that the fractional dead time of a trip system ought not to be credible at less than say 10^{-4}. The theoretical calculation for multiple channels is only realistic if truly random failure, and not common mode failures were to occur.

It is thus important when conducting or examining a detailed risk assessment to look closely at the fault tree and the assumptions to see whether this problem has been properly considered.

Toxicity

One part of an overall risk assessment where precision is lacking, and is unlikely to be improved much in the near future, is acute toxicity. In general this is due to the virtual absence of any direct data for humans, for obvious reasons, since even in cases where fatalities are known to have occurred, the lethal dosage is seldom known or amenable to estimation.

The basic approach taken by the majority of those utilising estimates of acute toxicity is to examine all the published data, and from the graphical plots of log concentration against log time, deduce the various bands of toxic effect to humans. Not unnaturally there are several features which contribute markedly to uncertainty. An example of this approach is that for chlorine.

Firstly, most published data for chlorine relates to non-fatal effects and is therefore not particularly helpful. Secondly, most of the direct human data is old and often imprecise. Third, any division of the data into several descriptive effects, as originally proposed by Dicken (15) is at best approximate, and lines attempting to demarcate these effects or to identify probabilities of fatalities are no more than best fit algorithms which are more realistically drawn with a broad brush than with a fine pen. Results of risk assessment involving such toxicity estimates must therefore also be subject to the same uncertainty, a fact that is often forgotten. It is for instance quite ridiculous to predict fatalities accurate to 5 significant figures when even the order of magnitude is in serious doubt. We ought not to deceive people, even unintentionally, into thinking that this aspect is well understood.

Dosage

There is a further problem involving toxicity. Due to the concentration of a vapour cloud varying with time, the acute toxic effect on humans is perhaps more correctly considered in terms of dosages, but the dosage which may be fatal is also time dependent. Dosages unqualified by the time involved are not correct statements of the situation and should never be used. There are still mistakes being made in this way.

Probits

A more recent treatment of toxic dosage is the use of probits, the probability of the concentration, in the time of exposure, causing a prescribed effect, say of killing 5%, or 50% of those exposed, (eg LC5 and LC50). The algorithms which are used are derived in this way (14), but there is not universal agreement for some toxic substances.

Escape Factors

The effect of escaping from a cloud of gas is often of considerable importance. Seldom can one consider that people are exposed in a cloud of irritant gas from a steady continuous release for say 15 minutes or more. Normal people will make some attempt to escape such clouds, and unless immobile, trapped etc, they may well succeed unless the concentration were to be very high, ie close to the source of escape. Thus the dosage they receive will be made up for example of a high initial concentration for perhaps a minute or two followed by a decreasing concentration as they seek fresh air. There will of course be many variants in the escape process, but the facts of the situation, as exemplified by the history of large chlorine and ammonia accidents confirm this view. Thus it is probably incorrect for an assessment to include the effects of a toxic gas cloud for a period of greater than say 10 minutes, unless it can be argued in the report that there are circumstances which will force the majority of those exposed to remain in the toxic cloud for the full period.

Experimental work (16) (17) (18) has shown that there is considerable attenuation of the gas concentration reached inside a building which lies in the path of a gas cloud, provided windows and doors are shut, and for most of the relatively short duration releases this will be vitally important. Indeed it is an essential part of emergency procedures in areas close to toxic gas storage. Should the release continue for some considerable time, say for over 30 minutes, problems may arise indoors and this is a situation that is as yet unorganised in most cases. Evacuation, especially of large areas, takes considerable time. At Mississauga for instance, it took 100 minutes to organise, and 24 hours to complete the progressive evacuation of 240 000 people. Most of the initial flash from the chlorine tank had been vented aloft in the fire before evacuation. In an earlier incident (19), a family who had survived indoors 50m from a punctured chlorine tank car evacuated themselves when conditions inside became bad. One child died, the remainder of the family survived, and presumably experienced similar dosages - a further indication of the difficult task of estimating precise values for dosages lethal to humans.

Marshall, in tables A and B of (1), produces a Mortality Index to account for these many variables. It requires careful definition in order to restrict it to well defined types of accident, and it is important also

to consider the range of values exhibited as well as the mean. Thus although historically we might expect 0.3 fatalities per te of chlorine released from major failures of chlorine tanks, in 8 of the 18 cases cited the result of the incident was that nobody was killed. Considerable care in the use of such overall indices is obviously of great importance but they will be useful in checking for order of magnitude.

Future Needs

If risk assessments involving a toxic gas are required for decision making in the future, there is a pressing need for more up-to-date research probably on animals in order to provide better quality data. It will then be possible to improve the confidence of assessed risk rates through the use of toxic or lethal levels where they are better established.

One way in which this can be done is to use modern research into the effects on animals so exposed. Several species, typically the rat are believed to react medically in ways similar to humans. There is of course some variability found, an effect which will always remain in just the same way as individual susceptibility is known to vary. The US Coast Guard and their contractors (14) have taken this evidence and used it primarily to indicate the slope of the lethal dosage lines. Then, using fixed points derived from old literature, the location of these toxicity curves for humans has been established. This appears to be a step forward, but it still relies on the correct positioning of a very few points (which could be in error). An examination of toxic gases and of known toxic curves for lower dosages indicates that some of the lethal curves may still be in error.

One must therefore conclude that there are three important aspects.

(1) The confidence limits of toxic gas risk assessment must remain low for the time being.

(2) There is a need to press ahead with further toxicological research in this field if better definition is seen to be a real need.

(3) The problem of using escape and other mitigating factors remains, which reduce confidence limits in such assessments, and these should continue to be investigated.

In the meantime in the absence of good data, many assessors are concerned largely with the frequency of the event.

Population Densities

In a large number of risk assessments where the risk to the group of people exposed is to be assessed, or where the number of fatalities is to be estimated, there is a need for population distribution data. This can be derived from many sources, but it is very important that the best possible data is obtained since it is easy, even through default, to produce risk assessments from this source which are in error by perhaps an order of magnitude.

An example of the use of simple data is that of the first transport risk assessment for chlorine conducted by Westbrook (20). Here a value of 700 per square mile was used to cover the entire route in question. The figure was obtained by taking the population for the UK and dividing by

the land area. Further investigation subsequent to the original assessment has led to the use of more refined data, for instance separate average densities for rural and urban (non-city) areas in England of 25 and 4000 per square mile. To match this such transport risk assessments require the corresponding route lengths through rural and urban areas. The accident rate is also found to be different for typical rural and urban routes. The immediate effect of this improvement in data is to identify the urban risk as being significantly greater than the rural one. One obvious solution is to reroute all such transport away from urban areas wherever possible. It is significant also that modern motorways avoid the urban areas to a very great extent, and without junctions to cause accidents they are usually the preferred route for road transport bearing in mind safety considerations.

If detailed data for population densitities near to fixed installations is required, local statistics are better still and can ususally be obtained with the assistance of the local authority.

To summarise this aspect of risk assessment, it is very important that a reasonable estimate is made of the population density which is appropriate for the assessment, bearing in mind that averaging of too extensive an area can easily lead to over or under assessment of the risks. The basis of the data ought to be declared in every case; at least it will lead to easier updating later if necessary.

TRANSPORTATION OF HAZARDOUS MATERIALS

This is a very common subject for risk assessments and it is worth looking at them a little more closely since they reveal for instance how techniques have improved in many cases, but not all, and how much still remains to be improved. Two subjects are useful examples of this technique, of the problems they have to tackle and of those not yet satisfactorily resolved.

Chlorine Transport Risk Assessment.

The first assessment of the risks of transportation of liquid chlorine was conducted by Westbrook for ICI (20) in 1971 and published in 1974. It used a very simple model backed by limited UK and US accident data to predict the frequency of accidents and punctures, and the potential number of casualties. Subsequently ICI updated the calculations to include more UK data and less US data, and to provide a wider range of potential accident conditions. Although world rail accident data are published annually by UIC (21), the basis for each country differs markedly and a true comparison is not possible. In many cases use of this data for such an assessment may well be inappropriate. Some assumptions of significance for the studies in this group are shown in table 1 which illustrates the development of the technique to include more sophisticated models and better data, and also an indication of some areas still treated by a relatively simple model.

About the same time the first US assessment was carried out by Simmons et al at UCLA (22) for inclusion as a comparative risk in the assessment of 100 US nuclear reactors (23). There was a major expansion of the detail incorporated into the assessment. Examination of US (and Canada) rail transport accident records since 1930 had disclosed 7 major releases of chlorine, of which 3 were due to brittle anchor failures (which have now

been eliminated). This represented then an accident rate of 0.1/yr. No fault tree type of examination was carried out. If one were now to re-examine this prediction in more detail, one would find that there have been 45 significant chlorine rail tank releases in USA and Canada (anchor failures excluded) in the last 50 years, representing an accident rate of 0.9/yr. Only a small number of these were large releases, most of the escapes being relatively minor (24). There is a potential error of almost an order of magnitude unless it is made clear what size of release is being considered. This requires to be stated very clearly.

The recent risk assessment carried out by Battelle (25) was based instead on a fault tree examination and not on historical data. By assessing the probability of a very large number of basic failure modes, an overall probability of 1.9×10^{-4} per shipment is derived, of which only a proportion will be major releases. By 1985 11 releases per year could be expected in the US, of which 1.8 per year would be large. As the current trend is of the order of 2 per year for all significant leakages, large or small, such a prediction seems out of line. To those who understand the practical aspects of chlorine tranportation and of chlorine releases, it would appear that despite the extensive fault tree, the model is still an inadequate representation of the whole scenerio. One can now appreciate the immense difficulty either of producing an adequately representative model which can be quantified, or even of producing any credible prediction of risk at all.

A new assessment has recently been carried out by TNO (26) with the principal objective of developing a working model. The report uses quantification only to illustrate the working of the model and the figures have no real significance. It is more likely to prove helpful in comparing relative levels of risk rather than providing any satisfactory value for the assessed risk.

Hazardous Material Pipeline Risk Assessment

In relative terms this is perhaps one of the simpler risk assessments to conduct but there are nevertheless some very big problems to overcome. It can be considered as a simple assessment because the majority of the system consists of a simple tube, perhaps many km in length, of fairly uniform thickness etc, and without connections or complexity.

Very extensive failure data and system lengths for many of the world systems exist. However of the 10^6 miles or so world-wide of buried line, a much smaller proportion is relevant to modern standards. ICI reviewed the Federal Power Commission failure data for 1950-1965 (27) and reinterpreted it for modern pipelines eight years ago, and more recent failure statistics such as reported by the Health and Safety Executive (28) confirm such estimates. Modern pipe properly manufactured and tested is at very low risk of external corrosion or crack failure when suitably wrapped and cathodically protected. The most significant cause of failure then becomes third party interference with mechanical digging or ditching equipment. Some modern equipment is particularly powerful, so deeper burying is now being used to reduce the risks. This same equipment is of course able to dig pipe trenches deeper than its predecessors.

The problem in risk assessment comes, not with the hazard analysis or the estimation of failure frequencies, but with the calculation of the consequences. Two particular problems exist. The calculation of the rate of escape of liquefied gases or high pressure gases and liquids is

not easy. Those calculations that are used are usually for initial rates which will probably decay very rapidly, but may also be erratic. Thus calculations on this basis, as for instance by the HSE for the proposed Moss Morran NGL line (28) are fundamentally an over-estimate representing an instantaneous peak situation.

When the second problem is also considered, that of ignition, one has to include factors which relate to the probabilities of ignition before full cloud development (at the initial release rate), at the full cloud development, and as it recedes. These factors may still add up to less than unity, ie non-ignition may be possible, so the risk rate calculated by the HSE report is not a risk of death, but the chance that a fully developed cloud will reach a populated area unignited. The risk to an individual in such a community might well be several orders of magnitude lower, perhaps even zero if he could never be affected by any such release. This difference is vitally important to decision making and would best be helped by stating precisely what the figures mean and also what they do not mean. The problem of estimating ignition probability is not easy to resolve.

Pipelines are also a good example of the difference in risks, individual/societal, peak/average. Peak individual risk probably occurs local to the pipe. Societal risk relates to risks to communities, and may well be an important risk to consider. But the average risk to an individual is not a suitable value to calculate since it depends largely on the area and the population judged to be at risk - the greater the distance considered, the lower the calculated average risk. Care thus has to be taken in selecting relevant risk values and avoiding those which are inappropriate.

DISCUSSION

It is of course impossible when considering hazard analysis and risk assessment to discuss the subject at any length, or to cover the entire field in a paper such as this. Nevertheless it is hoped that it will have helped to tidy up some misgivings, to remove some mistakes, and to stimulate others to improve their projects.

One of the most important aspects is that of conducting an adequate hazard analysis, for without such an exercise, it is all too easy to miss the critical aspects of an activity, and to produce risk estimates which can be fundamentally unsound. Use of the Vulnerability Model (14) is a good example since this model concentrates to a very large extent on the modelling of consequences and inadequate attention has been given to the hazard analysis which must precede calculation of risk. How and why do the accidents happen, and how can they be prevented? Only the hazard analysis, supported by some quantification principally of frequency can provide this information, and if we are to improve safety we must do this. Examination of risk rates achieves nothing on its own.

Secondly, one must use models which are adequately validated, in whole or in part, and declare the extent of this validation. If there is no or inadequate validation a safety factor or a conservative judgement may be used, but this must be declared. Those who are seeking the results of a risk assessment have not only a right to know whether the results can be believed, but they really have a duty to look at this aspect before decision taking. How often is this done today?

Thirdly, both risk assessors and those appraising their assessments have a need to understand the limitations in the exercise, and to what extent they have been recognised and allowance made or assumptions fully declared. Have they for instance, properly taken into consideration human error or common mode; has the time or cost constraint restricted the extent of the exercise such that there has not been developed adequate confidence in the results?

When acceptability of risk is concerned, there must be an appreciation of what it is all about, that there is for instance no such thing as absolute safety, and that when judgement is made, a full and complete balance between risks (or costs) and benefits is examined. Not only is it vitally important for tabulations of risk, or risk curves to be correctly defined, but it is necessary to have a good understanding of the variance, and of such factors as whether the risk is voluntarily undertaken or not, and of risk aversion, particularly for potentially large accidents. Consequently it is imperative that those responsible for decision taking are fully prepared for these responsibilities, and at the present time this is seldom the case.

In conclusion it should be stated that at the present time there are few risk assessments which can correctly be claimed to assess the risks that they set out to estimate with the confidence limits they would like. For a variety of reasons most assessments are inadequate for the job they are trying to do, and more attention is needed to their presentation so that those in the decision making area are given a true and fair picture of their efforts. This does not infer that more detail is required in every case, often only a better explanation of the assumptions, and the validity and the meaning of the assessment is required. Many of those who have conducted risk assessments have found defects and short-comings in the technique and have then developed improvements. But the real value lies in the Hazard Analysis stage for two reasons. Firstly it identifies where and how accidents are likely to happen so that they can be prevented and priority given to the most important. Secondly those who have actually conducted the Hazard Analysis, especially the plant personnel, learn a tremendous amount about their own process which they might otherwise have missed.

Acknowledgement

I would like to thank many colleagues in ICI for their useful discussions over the years which have contributed to the preparation of this paper, also to those engaged in similar work in the Chemical Industries Association and in the process industries at large.

I would like to thank Imperial Chemical Industries for permission to publish this paper. The views experssed are my own and do not necessarily represent the views of the company.

REFERENCES

1 Health & Safety Commission, 1979, Second Report of the Advisory Committee on Major Hazards, HMSO.

2 Gill, D.W., 1978 "The Application of Hazard Analysis Techniques to Pressurised Systems", Conference on "New legislation for Industrial Pressurised Systems", Oyez IBC, London.

3 Faragher, W.E., Pizzo, J T., Rausch, A.H., 1979, "Commercial Vessel Safety Risk Assessment Study - Vol II Risk Assessment Methodology Study", US Coast Guard Report No CG-D-59-79, (AD-A077628).

4 ED: Knowlton, R.E., 1977 "A Guide to Hazard and Operability Studies", Chemical Industries Association, London.

5 Fussel, J.B., 1973, "Fault Tree Analysis - Concepts and Techniques", "Generic Techniques in System Reliability Assessment. Proceedings of the NATO Advanced Study Institute on Generic Techniques in System Reliability Assessment, University of Liverpool, UK., July 17-28, 1973", Henley, E.J and Lynn, J.W (Eds.), Noordhoff, Leyden.

6 Grist, D.R., 1978, "Individual Risk - A Compilation of Recent British Data", Safety and Reliability Directorate Report SRD R 125.

7 ED: Schwing, R.C., Albers, W.A., 1980, "Societal Risk Assessment", Plenum Press, New York.

8 Rowe, W.D., 1977, "An Anotomy of Risk", Wiley.

9 Otway, H.J., 1977, "The Status of Risk Assessment", 10th International TNO Conference, Rotterdam.

10 Council for Science and Society, 1977, "The Acceptability of Risks", Barry Rose Ltd, Chichester, England.

11 Gibson, S.B., 1980, "Hazard Analysis and Numerical Risk Criteria", AIChE, Loss Prevention Symposium, Philadelphia, Pa.

12 Kletz, T.A., 1976, "The Application of Hazard Analysis to Risks to the Public at Large", World Congress of Chemical Engineering, Amsterdam.

13 Wu-Chien, J.S., Apostolakis, G., 1981, "On Risk Aversion in Risk Acceptance Criteria", Reliability Engineering 2, 45-52.

14a Eisenberg, N.A., Lynch, C.J., Breeding, R.J., 1975, "Vulnerability Model: A Simulation System for Assessing Damage Resulting from Marine Spills", US Coast Guard Report No CG-D-136-75 (AD-A015245).

14b Rausch, A.H., Eisenberg, N.A., Lynch, C.J., 1977, "Continuing Development of the Vulnerability Model", US Coast Guard Report No CG-D-53-77 (AD-A044197).

14c Tsao, C.K., Perry, W.W., 1979, "Modifications to the Vulnerability Model - Simulation System for Assessing Damage Resulting from Marine Spills", US Coast Guard Report No CG-D-38-79 (AD-A075231).

14d Perry, W.W., Articola, W.P., 1980, "Study to Modify the Vulnerability Model of the Risk Management System", US Coast Guard Report No CG-D-22-80 (AD-A084214).

15 Dicken, A.N.A., 1974, "The Quantitative Assessment of Chlorine Emission Hazards", AIChE Chlorine Bicentennial Symposium, San Francisco, Ca.

16 DGA, 1975, "Experiments with Chlorine", Directoraat Generaal Van de Arbeid, Voorburg, Netherlands.

17 Bahnfleth, D.R., Moseley, T.D., Harris, W.S., 1957, "Measurement of Infiltration in Two Residences", American Society of Heating and Air-Conditioning Engineers paper No 1615.

18 Cohen, A.F., and Cohen, B.L., 1980, "Protection from being Indoors Against Inhalation of Suspended Particulate Matter of Outdoor Origin", Atmospheric Environment, 14, 183-184.

19 Segaloff, L., 1961, "Community Reaction to an Accidental Chlorine Exposure", Institute for Co-operative Research, University of Pennsylvania, (AD-269 681).

20 Westbrook, G.W., 1974, "The Bulk Distribution of Toxic Substances: A Safety Assessment of the Carriage of Liquid Chlorine". Loss Prevention Symposium, Delft, Netherlands, Elsevier.

21 International Union of Railways, "International Railway Statistics", Published annually by Union Internationale des Chemins de Fer, Paris.

22 Simmons, J.A., Erdmann, R.C., Naft, B.N., 1974, "The Risk of Catastrophic Spills of Toxic Chemicals", Report No UCLA-ENG-7425.

23 Rasmusson, N.C., 1975, "Reactor Safety Study - An Assessment of Accident Risks in US Commercial Nuclear Power Plants", US Nuclear Regulatory Commission, WASH-1400.

24 Harris, N.C., 1978, "Analysis of Chlorine Accident Reports", Chlorine Institute 21st Plant Managers Seminar, Houston.

25 Andrews, W.B., 1980, "An Assessment of the Risk of Transporting Liquid Chlorine by Rail", Batelle Memorial Institute Report No PNL-3376.

26 TNO, 1981, "Eindrapport Proefproject Risicokaart Zuid-Holland", Netherlands Organisation for Applied Scientific Research.

27 Federal Power Commission, 1966, "Safety of Interstate Natural Gas Pipelines", Committee of Commerce, US Senate.

28 Health & Safety Executive, 1978, "A Safety Evaluation of the Proposed St Fergus to Moss Morran Natural Gas Liquids and St Fergus to Boddam Gas Pipelines". Also revised report 1980.

29 Lautkaski, R., Mankamo, T., 1977, "A Risk Assessment of the Rail Transportation of Liquid Chlorine", 2nd International Loss Prevention Symposium, Heidelberg.

TABLE 1 - COMPARISON OF CHLORINE RAIL TRANSPORT RISK ASSESSMENTS

Study	Westbrook (20)	Westbrook revised	Simmons et al (22)	Lautkaski et al (29)	Battelle (25)
Approx Date	1971	1976	1973	1976	1979
Country:	UK	UK	USA	Finland	USA
Failure Analysis	Historical UK rail accident data	Historical UK rail accident data	Historical US chlorine accident data	Historical Finnish rail accident data	Fault Tree Analysis
Puncture model	Yes	Yes	No	Yes	Yes
Size of Tank Car	28 tons	28 tons	90 s tons	45 te	90 s tons
Annual Tonnage	197 000 te	170 000 te	2800 000 te	150 000 te	4490 000 te
Mean Journey	49 km	93 km	400 km	50 km	450 km
Heavy Gas Dispersion model	No	No	$\sigma_z = 0.2\,\sigma_y$	$\sigma_z = 0.2\,\sigma_y$	σ_z reduced
Weather Stability classes	1 (neutral)	6 (A-F)	3(ABC)(D) (EF)	8 sets	4 (B D E F)
Wind Speeds	1 speed	6 speeds	5 speeds	1 speed	5 speeds
Population Density	1 value	2 sets	9 sets	13 sets	3 sets
Chlorine Concentration	20 ppm	20 ppm	35 ppm	100 ppm	1000 + 35 ppm
Evacuation Model	No	No	Yes	Yes	Yes
No of Mortality Bands	-	-	7	360 points	15
Assessed Risk (25) deaths/te km	1.7×10^{-10}	-	1.0×10^{-8}	4.0×10^{-8}	4.6×10^{-9}

NCH/f/A20

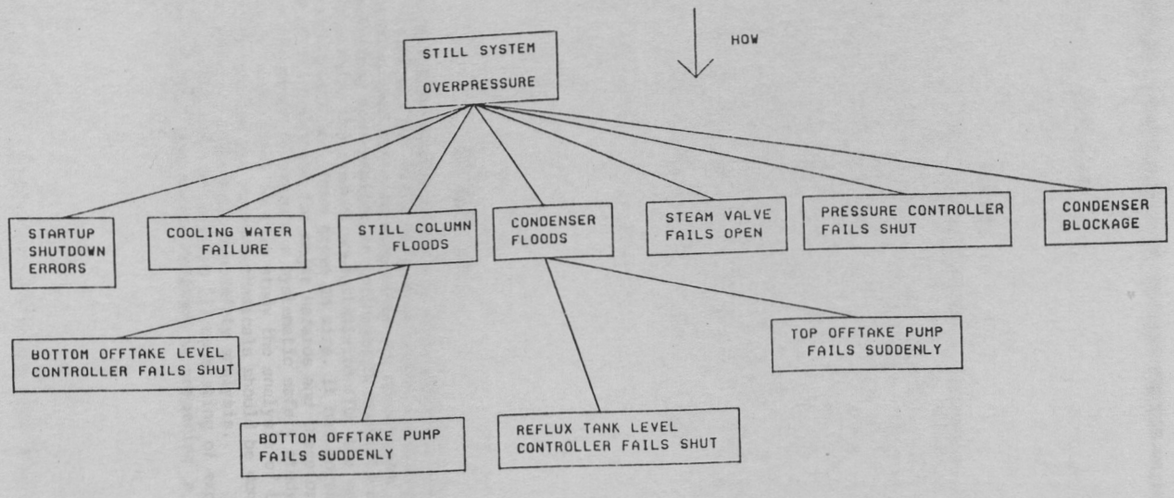

Figure 1 Outline Fault Tree for a typical distillation plant