10th INTERNATIONAL TNO CONFERENCE

Risk Analysis: Industry, Government and Society

Co-sponsored by VNCI
(Association of the Dutch Chemical Industry)
and by FME
(Association of the Mechanical and Electrical
Engineering Industries FME)

HILTON HOTEL – ROTTERDAM
24 and 25 FEBRUARY 1977

Published by: Netherlands Central Organization
for Applied Scientific Research TNO
P. O. Box 297
The Hague
Netherlands

Editor: A. Verbraeck

Opening address

Dr. L. B. J. Stuyt
Chairman of the Organization for Applied Scientific Research TNO
The Hague
The Netherlands

It is my pleasure and privilige to welcome you at the tenth TNO-Conference. Before reflecting on the theme we selected for this year's conference I feel prompted to commemorate that to-day we are attending the tenth TNO-Conference in succession. Also, I consider it useful to dwell for a moment on the why and how of these conferences.

Some ten years ago the question arose: Why conferences should not be held in Europe of a type which had already proved to be very successful in the USA and Canada. At such conferences, organized around a given theme, representatives of various disciplines held discussions and tried to understand each other's points of view. When this question was brought to the attention of Prof. Ir. H. W. Slotboom, at that time chairman of the Organization for Industrial Research TNO, he came to the conclusion that this was a concept which fitted into the general tasks of TNO. Thus, he decided to support this idea. In fact, at that time, he coined the phrase that such conferences should be a "Show-window" for TNO. Looking back, I think Prof. Slotboom's vision was right. Over the years, centering around various themes, we succeeded to bring together the outlooks of thinking of R & D and of the financial and economic viewpoints.

I also feel justified to state that the TNO-conferences have been successful and have attracted an international attendance of high caliber. Thus last year the management of TNO, when reviewing the purpose and the results of these conferences, decided to continue their organization. We are glad that as a result of certain subjects, chosen by the Advisory Committee in the course of years, both the Association of Dutch Chemical Industry and the Federation of Metal and Electrotechnical Industries become co-sponsors.

I would like to say a few words on the Advisory Committee. As you may observe from the programme, it represents a cross-section of the Dutch industry together with representatives of the sponsoring organizations.
Their task may not seem very arduous, it is nevertheless of great significance. Once a year they meet to decide on the subject of the next year's Conference. I gladly acknowledge the important assistance they lend TNO in this way.

Over the years the Committee has chosen subjects related to products - in this respect I remind you of the well-attended conferences on "Synthetic Fibres" and "Plastics and Metals" - but also subjects related to managerial problems. In the latter category our 7th conference which dealt with the "Acquisition of Technology for Innovation" was, in my opinion, an outstanding one. This subject was, by the way, a logical continuation of our 6th conference dealing with the subject "Organizing for Technological Innovation".

The success of our conferences was in no small way due to the unerring efforts of Prof. Dr. A. J. Staverman, who was the stimulating power in the Organizing Committee. He also served our conferences as Chairman in a very successful and, I may say, also in a very peronal way. Thus, when last year Prof. Staverman decided to resign from the organization of the TNO-conferences, in view of his increasing workload at the University of Leiden, this decision was very much regretted by the members of both the Organizing and the Advisory Committee. It gives me much pleasure that Prof. Staverman found time to accept our invitation to attend this conference. We are glad that we found Prof. Dr. G. J. M. van der Kerk willing to take over Prof. Staverman's task and I am sure that he will prove a worthy successor.

However, I do not want to dwell on the past any longer and would like now to turn to the subject of the present conference: Risk Analysis.

In our present-day society there is a definite tendency for technological systems to increase in size and complexity. This, of course, is not an autonomous process but rather the result of our tendency to optimize both the technical and economic criteria on which these technological systems are based. This tendency has resulted in an increasing interaction between these technological systems and the social systems composing our society.
Undesirable and mostly unintentional influences of our technological systems on the physical and ecological equilibria of our natural environment are - for the general public - the most eye-catching symptoms of this development. In addition, the sheer complexity of the technological systems and the feeling that only very few people have actual insight in these complexities has caused a feeling of uneasiness and even of fear that we will not be able - like the apprentice sorcerer - to manage the forces we unleashed ourselves.
Therefore it comes as no surprise that attempts have been made and are being made to obtain a hold on the technological developments by drawing up criteria on environmental hygiene, health, safety and other social factors. The establishment of the United States Office of Technology Assessment is just one example of the aforementioned attemps. Urgent needs are recognized for rather broad-based policy studies on the impact on our society of newly introduced technologies and of expansion of existing technologies.

The aim of these studies - which are categorized by the term "Technology Assessment" - is to offer the decisionmaker, who is always working with uncertainties, a number of analyzed alternatives resulting in - it is hoped - better founded decisions.
Within this framework the subject of this conference - risk analysis as a basis for risk management - is chosen.

Technology Assesment may be defined as an analysis of both "costs" and "benefits" of the various alternatives of a technological system. If we accept this definition then Risk Analysis can be distinguished from TA as being oriented rather on the "costs" aspects and in particular how these "costs" affect the individual person, our environment, the capital structures and - in the end - our society as a whole.
From a strictly grammatical point of view, Risk Analysis only indicates one phase of the process which acts as the basis for Risk Management, namely the analytical phase. In order to fulfil his managerial task the decisionmaker must also have at his disposal knowledge about the perception of risks by individuals and groups, about the criteria of acceptance of risks and about the way these criteria are formulated.
In this conference we will use the name Risk Analysis for both phases of the assessment process.

From what I said just before, it will be evident that Risk Analysis, as we will discuss it today and tomorrow, can never be the sole responsibility of scientists and technologists. If ever a subject lends itself particularly well for an integrated approach by natural and social sciences it is Risk Analysis.
I am sure it will become evident from the discussions at this conference, that Risk Analysis shows extreme diversity in methods and techniques, depending on the systems studied. It is understandable that a risk analysis of a system concerning dangerous chemicals will be different from the risk analysis concerning very large datahandling or communication systems. In turn these will be different from an analysis concerning the introduction of new medical drugs or the impact of certain measures of arms control and disarmament. Having said this, I would like to say that in my opinion it would have been unwise to widen the scope of this conference too much.
In the next two days - after the more introductory lectures we will concentrate on risks involved in industry, in major engineering constructions and on those concerning the environment.

From these examples it will be clear what a powerful tool risk analysis has become in providing the decisionmakers with alternatives. But it will also be very clear that the methods and techniques made available by Risk Analysis will never be able to relieve these decisionmakers from making the ultimate choice.
Decision making will always remain a creative process.

Ladies and Gentlemen, I would like to end here. I hope to meet you again to-night and now I would like to ask Prof. Van der Kerk to start our proceedings.

Present Status of Risk Assessment

Dr. H. Otway
Joint IAEA/IIASA Research Project of the International Atomic Energy Agency
Vienna
Austria

The creation of an environment that can be interpreted as providing security and comfort is a basic human need. Historically, man has developed technologies that support this need to view the world as a safe place to live. With the evolution of social systems, political structures and philosophies based upon security-seeking, technological innovations became larger and more complex and this capable of offering increasingly attractive benefits; however, with this increase in scale, negative side-effects, or risks, began to emerge as unanticipated threats to security and comfort. There were also more subtle effects of technological development noted; they included complicated environmental interactions, feelings of dissatisfaction despite increasing standards of living and a sense of isolation from decisions affecting social welfare. As a consequence the values that had been implicitly accepted by technology-intensive societies became increasingly subjected to challenge.

The number of debates about the suitability of technological developments suggests the difficulties that have been encountered in attempting to reconcile technological and social systems in public planning and decision processes. In the past, technological and social systems have, to a large extent, been considered in isolation from one another. The problem which has emerged may be conceived as that of synthesising complex technical data with the needs and wishes of the public - the reconciliation of technical capabilities with social values. Risk assessment has come to describe studies oriented toward providing information on technological risks, and their social aspects, for use in decisions related to the management of risks.

The intent of this paper is to suggest an interdisciplinary framework for risk assessment studies and to provide examples of the methodologies that might be used within this framework. The status of these methodological developments will be summarised and sample results will be given of applications to energy systems. Speculations will be offered on the future of risk assessment - this year's "exciting new research area", or a research direction which has naturally evolved from the technological developments and social movements of the past decades?

Figure 1 presents a theoretical risk assessment framework which was developed (Otway, 1973; Otway, 1975; Otway and Pahner, 1976; Otway, 1977) as a collaborative effort by scientists from a number of disciplines; it is in essential agreement with the approaches used by other researchers in this area (Rowe, 1975; Kates, 1976). This framework does not intend to portray the inter-actions between technological and social systems in any "real-world" sense; rather, it illustrates the relationships among the analyses, originating in various disciplines, which may form a risk assessment study. It will be noted that risk assessment is divided into three sub-topics: risk estimation, risk evaluation and risk management.

Risk estimation is the identification and quantification of the risks associated with technological systems. Risk evaluation is the measurement of social values and their reconciliation with risk estimates through the use of formal decision methodologies. Public planning and decision processes should not be mechanised exercises. The analyses of risk estimation and evaluation provide an ordered list of the options under consideration. The primary benefit of these quantified studies might be an improved understanding of the technical and social systems being investigated, and the acquisition of new insights into their interactions. Risk management, in reality a function carried out at a higher political level than risk evaluation, considers the evaluated options in the

light of the historical and political realities which surround the decision to be taken. The result is a choice among the alternatives offered or recommendations for modifications to technological systems to change their risk characteristics. The emphasis of this paper will be on risk evaluation.

RISK ESTIMATION

Risk estimation is the identification and quantification of the risks posed by the technological system under consideration. Methods for quantification are the most highly developed part of the risk assessment process and thus will not be discussed in much detail here. The identification of new risks will continue to be an activity which requires constant thought and attention.

Unplanned Events

Unplanned events that might occur during normal operations have received considerable attention, and the methodologies and procedures for their analysis are reasonably well understood: identification of possible unplanned events that migth occur during operation, such as accidents, sabotage or mis-use; identification of their consequences; analyses of consequence magnitudes and their distributions in terms of time, space, and social group; and, finally, an analysis of the corresponding probability distributions, and uncertainties, of all events and consequences. Early risk estimation studies on unplanned events in nuclear power plants were largely carried out by individual scientists on an ad hoc basis, e.g., in the UK (Farmer, 1967; Beattie, 1967), and in the USA (Otway, 1969; Otway, 1971). Well-financed, full-scale risk estimation studies were carried out later; the best known of these is that sponsored by the US Nuclear Regulatory Commission, the "Rasmussen Report" (1975). A sample result from this study is shown in Figure 2.

Planned Operations

Risk estimation begins with the identification of the consequences of planned operations of the system. A sample result of a risk estimation study for projected planned operations of fossil-fuel energy production systems is shown in Figure 3 (Niehaus, 1976). Based upon a scenario specifying energy demand, and the contributions of various energy sources, results are expressed in terms of changes in one physical variable (global average temperature change) as a result of CO_2 emissions.

Levels of Risk

Figure 1, in addition to physical risks to health and environment, also includes mention of psychological and social levels of risks. This refers to the potential effects of perceived hazard upon psychological well-being of individuals and the resulting risks to social and cultural structures; this might also include risks to social structures and values that could follow the availability of new benefits. One example might be the changes in life styles brought about through the increased personal mobility offered by the automobile. There are no quantitative methodologies available for dealing with these "higher order" levels of risk.

Status of Risk Estimation

The methodologies developed in analyses such as the US Reactor Safety Study seem to be readily adaptable to other types of systems for the estimation of accident probabilities. The consequences of radiation exposure, including late and genetic effects, can be estimated "with much greater confidence and precision than is the case for most hazardous chemical and physical agents present in the . . . environment" (NRPB, 1976).

The risks of several environmental insults, such as microwaves, and chemicals, are

not very well known and, in some cases, are the subject of scientific controversy. There are many difficulties in determining their risks; chemicals, for example, must first be tested with bacteria and animals for mutagenicity - the ability to damage genetic material. The correlation between mutagenicity and carcenogenicity (the property of including cancer) is not known, thus requiring a series of long-term carcinogen tests. There still remain uncertainties in extrapolating animal results to humans. It appears likely that procedures similar to those used to determine radiation exposure risks and to test pharmaceuticals will be applicable to this matter. The identification of new risks will continue to be a challenging problem.

RISK EVALUATION

Risk evaluation may be thought of as the measurement of social values and their reconciliation with technical risk estimates through the framework of formal decision-making methodologies. The first four blocks in the risk evaluation part of Figure 1 refer to the social response to risk situations and its underlying determinants. Social response is clearly not based only upon theoretical or statistical prediction of risk, but rather is multiply-determined through a variety of psychological functions such as perception, conditioning, and learning. Figure 1 indicates methods for inferring response which are based upon attitudes, utility theory or statistical data; these methodologies arise respectively from research in social psychology, management sciences and economics.

Measures of Social Value: Methodologies

Utility-based methods have been used primarily for assessing the decision-makers' (or experts') expectation of "social utility" as a function of technical variables. Although some of these methodologies could, in principle, be extended to make utility measurements on a public survey basis, the technology for so doing does not exist at present; therefore, this method will not be discussed further here.

Methods Based upon Statistical Data

One of the more primitive risk evaluation methods has been simply to put estimates of risk "into perspective" by comparing them to statistical measures of other risks accepted by society. This method can provide only an indication that a new risk is too high; it cannot predict that a new risk, similar in magnitude to other existing risks, will be accepted. Comparison of different types of risks lacks meaning since each risk is characterised by many variables other than its statistical expectation.

The effects of such variables upon risk perception were graphically illustrated by the work of Fischhoff, et al. (1976) who, as part of a larger experiment, asked a group of 75 subjects to rate thirty different technologies and activities on each of nine postulated dimensions of risk, e.g., degree of voluntariness, extent of individual control, extent to which the person exposed knows about the risk, number of people exposed, etc. Analysis showed that two orthogonal factors were sufficient to account for inter-correlations between items; they were interpreted as representing "new, involuntary high technology with delayed consequences for many people" and "events whose consequences are certain to be fatal (often for large numbers of people) should something go wrong". These factors were labelled respectively "Technological Risk" and "Dread Risk", the latter referring to instinctive, unexplained fear. Figure 4 (after Fischhoff, et al.) shows some of the 30 activities plotted in this two-dimensional psychological space; this figure suggests that, in addition to the statistical predictions of risk, psychological factors play a significant part in their perception. It also suggests the futility of seeking to reassure people that, for example, nuclear power is safe by comparing its low levels of risk with the number of hours of skiing that would provide an equal risk - in a psychological sense they are not comparable. In fact, if this comparison were intuitively made on the dimensions proposed in Figure 4, it would suggest to the individual that nuclear power is much higher on both dimensions and thus have an ef-

fect opposite to that intended.

The perspective offered by attitude formation theory suggests that attitudes toward objects, or risks, would typically be determined by five to ten attributes that are associated with the attitude object. The nature of the attributes will vary from one object, or risk, to another as will the relative importance of each determinant. Statistical data on expected risk is only one informal input into the attitude formation process. An attitude formation model will be discussed in detail later.

The work of Starr (1969), based upon a statistical data approach, offered a broad philosophical basis for beginning risk assessment studies and was instrumental in calling attention to the importance of risk concepts in public decision making. National-level statistics were used as a basis for estimating the risks and benefits from nine technologies or activities. Based upon this analysis mathematical relationships were proposed between some determinants of risk acceptability: /a/ perceived benefit and acceptable levels of risk (R proportional to B^3); /b/ the ratio of acceptable risk levels for voluntary and involuntary risk exposure (a factor of 10^3); and /c/ the "psychological yard-stick" people use to judge the acceptable risk levels (equivalent to the probability of death due to natural causes). This method implicitly assumes that risk levels resulting from past decisions were somehow optimal, thus providing an adequate basis for future decision making, and that those making the decisions had perfect knowledge of the data which were subsequently reflected in the statistical compilations.

A subsequent study (Otway and Cohen, 1975) found fault with the assumptions underlying the methodology and could not reproduce the numerical results using the same data base. The specific variables of interest in such an analysis are seldom recorded separately in the data base; the numerical results were found to be excessively sensitive to the assumptions required to extract these variables from national-level statistical data. Further, there is the difficulty in proving cause-effect relationships between, for example, risk and benefit or participation in a risky activity and the actual risk level. At present, there is no evidence that analyses based upon statistical data could lead to useful rules for specifying risk acceptability or its determinants.

An Attitude-Based Method

An alternative to the statistics-based approach is to use attitude as a measure of value. Fishbein (1975) and his colleagues have developed a model of attitude formation over the past decade which has the feature of synthesising the belief and evaluative components of attitude in a form which preserves the distinction between them. The belief (cognitive) component represents knowledge or opinions about the attitude object while the evaluative component is a measure of affect or feeling. Thus the model allows not only the identification of the specific factors important in attitude formation but also the respective contributions of opinion and feeling to each factor.

Figure 5 (after Fishbein) summarises the relations between beliefs, attitudes, intentions, and behaviours with respect to a given object*. It may be seen that a person

---

* Definitions: A belief is a probability judgement that links some object or concept to some attribute. For example, one might believe that Automobile A (an object) is expensive (an attribute). The strength of the belief is defined by the person's subjective probability that the object-attribute relationship exists, or is true. An attitude is an evaluative judgement that one likes or dislikes the object, that it is good or bad, that he feels favourable or unfavourable towards it. One may have attitudes towards concepts, people, institutions, events, behaviours, outcomes, etc. An intention is a probability judgement that links the individual to some specific action, i. e., the individual's belief that he will perform some specific behaviour. Behaviour is an observable action.

holds many beliefs about an object; that is, he associates that object with a number of different attributes; thus attitudes may be said to be multiply-determined. It has been found that knowledge of a person's beliefs about an object, and his evaluations of the associated attributes, allows an accurate prediction of his attitude toward the object. A person's attitude toward any object is a function of his beliefs about that object weighted by these evaluations; however, it is the entire set of salient beliefs that determines the attitude and not any specific belief. It has been consistently found that a person's attitude toward an object is likely to be determined by a relatively small number (five to nine) of salient beliefs.

One an attitude has been formed, a person is pre-disposed to behave in a consistent manner with respect to that object. Although his attitude does pre-dispose him to perform a set of behaviours, it does not pre-dispose him to perform any specific behaviour. It had previously been assumed that a person's attitude towards some object would influence some particular behaviour with respect to that object, it is now clear that attitudes towards an object may have little or no influence on any specific behaviour. Just as attitude is determined by the entire set of beliefs that a person holds, the attitude only serves to pre-dispose the person to engage in a set of behaviours that, when taken together, are consistent with the attitude. This is shown schematically in Figure 5. The way in which beliefs linking the object to specific attributes and the evaluations of these attributes combine to form attitude can be mathematically written as:

$$A_o = \sum_{i}^{n} b_i e_i \qquad \text{Equation 1}$$

where A_o = the person's attitude toward object o.

b_i = the strength of belief i about object o; i.e., the subjective probability that o is related to some attribute i.

e_i = the subject's evaluation of attribute i.

n = the number of salient beliefs the subject holds about object o.

The measure of attitude obtained from Equation 1 is the sum of the eb products. To verify that this is indeed a measure of attitude, correlations can be made between the Σ eb scores of the subjects and independent, direct measurements of the same attitude. Direct, global measurements of attitude can conveniently and reliably be made using the semantic differential method of Osgood, et al. (1957). The magnitude, and statistical significance, of this correlation coefficient provide a measure of the succes of the model in estimating attitude and, in addition, ensures that the set of attributes used is adequate to describe the attitude object for the group tested. This test of validity is an important characteristic of the model*.

In summary, knowledge of the attitude held towards an object is a useful predictor of the totality of behaviour with respect to that object**. This is an important finding: by

---

* Considerable empirical evidence to support this model can be found throughout the attitude literature in areas such as racial attitudes, family planning, politics, special laboratory experiments. For a review, see Fishbein and Ajzen (1975).

** A discussion of the determinants of specific behaviours is beyond the scope of this paper; however, Fishbein (1967) has developed a theory in which two major variables (i.e., attitudes toward performing the behaviour and subjective norms concerning the behaviour) are viewed as the immediate determinants of an intention to perform a given behaviour.

aggregating individual responses it is possible to describe the totality of the expected social response, or that of any social group. Thus, as suggested earlier, attitude provides a useful measure of value for use in decision making*.

An Application of the Attitude Model

A pilot application of the Fishbein model, to attitudes toward nuclear power, was carried out in order to test its utility in the area of attitudes toward technologies and their risks. A questionnaire was given to a group of thirty people affiliated with a university institute engaged in energy research. Almost all had university degrees and half had had extensive experience in the nuclear energy field. The average age of the group was in the mid-forties, two-third were male, All subjects were presented with a 32-page booklet with the standard instructions for using the semantic differential as the first two pages. Details of the experimental design and elicitation of the attributes used may be found in Otway and Fishbein (1976).

The Spearman rank order coefficient between the estimated and direct attitude scores was 0.66, statistically significant at a level of less than 0.1%, thus demonstrating the validity of this application.

The results for the total sample confirmed what one might intuitively expect from a well educated group of subjects of high socio-economic status, many of whom were professionally experienced in energy research. The three most important determinants concerned waste production, the possibility of destructive mis-use of the technology, and the question of catastrophic accidents affecting large numbers of people. In contrast, the next three determinants associated nuclear power with the positive attributes of providing good economic value, providing essential social benefits and the enhancement of the "quality of life". The risk aspects of nuclear power were more important than the potential benefits.

In order to better understand the factors differentiating between people with favourable and unfavourable attitudes toward nuclear power, two sub-groups were formed from the total sample. Using the direct attitude measurement scores from the semantic differential as the criterion, the ten subjects with the highest scores formed the "pro" group and those with the ten lowest scores the "con" group. Table I presents comparisons, for the total sample and each of the two sub-groups, of importance values and ranks for each attribute. In general, the "con" group, like the total sample, assigned high importance to the risk items while the "pro" group viewed benefit-related attributes as most important.

Table II presents the mean algebraic $\overline{eb}$ scores, the mean belief strengths (b_i), and the mean evaluations (e_i) of each attribute, for the "pro" and "con" groups. This table allows identification of those aspects which most clearly differentiate between the two groups. The algebraic values of the $\overline{eb}$ terms represent their contributions to the overall attitudes; for example, the perceived relationship between nuclear power and "big government or business" contributes positively to the "pro" group's attitude, negatively to that of the "con" group. The reason for this difference can be better understood

---

* The results of this model differ from those of most public opinion polls in several important features. The poll typically measures only the cognitive (opinion) component of attitude, the b_i of Equation 1. Further, results of the model can be verified through correlation with independent, direct measures of attitude; this ensures that the model has indeed measured attitude and that the attributes used were adequate to describe the object. The typical public opinion poll does not have this measure of validity and, finally, the beliefs measured by the public opinion poll are not measures of attitude and, thus, may be completely unrelated to the overall behaviour of the respondent group.

from looking at beliefs and evaluations. It may be seen that both groups strongly believe that nuclear power is in the hands of big government or business. However, while the "pro" group evaluates this attribute positively, the "con" group evaluates it negatively.

There were three additional items for which eb differences between the groups were statistically significant. These items were all related to the benefits of nuclear power: providing benefits essential to society, providing good economic value and enhancing the "quality of life". In all three cases both groups evaluated these attributes positively, although the "con" group valued enhancement of the "quality of life" significantly less than the "pro" group. However, for all three items the beliefs were the major factor contributing to these differences. More specifically, the "pro" group strongly believed that nuclear power offers these benefits, while the "con" group tended to be uncertain to somewhat negative.

There were no significant differences between the groups on the eb scores of any of the items related to risk. Both groups believed that nuclear power is characterised by the attributes of affecting large numbers of people, creating noxious wastes and possible destructive mis-use. Although both groups negatively evaluated these risk-related attributes, it is interesting that the "con" group's evaluation for two of them were significantly more negative. This indicates essential agreement among the groups with respect to nuclear power risks, but suggests that differing attitudes toward nuclear power may be primarily determined by strongly differing beliefs about its benefits*.

It should be noted that the particular group used in this study was not representative, thus one should not assume that the results can be generalised to other populations. For example, among a group of scientists it is not surprising that differences in attitude toward nuclear power were found to be due largely to differences of opinion about its benefits. Even within this group, items referring to nuclear risks evoked differences in the affective component of attitude. However, this application did demonstrate the utility of the model in this area of investigation.

The Decision Maker and Decision Methodologies

The final, integrative step in risk evaluation is an ordering of the alternatives being considered. This may be viewed as the assimilation and balancing of the complex technical data resulting from risk estimation analyses with measures of the corresponding social values. The limitations of the decision maker in handling the large quantities of probabilistic data involved in many public decisions suggest the use of formal decision methodologies to aid in this process.

Cognitive Limitations in Decision-Making

Simon (1957) has proposed the theory of "bounded rationality" which asserts that, in order to deal with the world, cognitive limitations force the decision maker to intuitively construct a much simplified model. He then behaves rationally with respect to this simplified model, but perhaps irrationally with respect to the real situation. Psychological research on "cue utilisation" bears upon the limits of rationality in decision making.

People are often in situations where they must make some prediction, inference or choice on the basis of several items of information, or "cues". Table III (after Wiggins,

---

* In agreement with this result, many surveys on attitude toward smoking have found that smokers and non-smokers tend to agree on the risks associated with smoking; significant differences are found in their perceptions of the benefits.

et al., 1969) shows partial results of a cue utilisation experiment. Here 145 judges were asked to infer the intelligence of each of 75 people based upon nine pieces of descriptive information, or cues, about them. A factor analytic procedure was used to identify the types of judges who had made similar inferences; eight different types were found (Table III shows only five types since 140 of the judges fit into one of these five groups). It may be seen that, for most judges, only a few of the cues correlated significantly with the intelligence estimates, indicating that only these items of information were influential in the inference process.

This, and other, studies of the ways in which people combine these different pieces of information to arrive at their decisions suggest: (1) that some information items are not used at all; (2) people are not able to accurately report which information items they actually used in reaching their decisions; (3) people are also not able to judge the relative importance they gave to the information items they did use*; (4) as decision makers become more experienced they become even less able to subjectively estimate which information items they are actually using; (5) the weights subjectively placed on different information items by different decision makers seem to be a function of personality variables. For example, in Wiggins' sample, judges of types I and II were found to be intelligent and low in ethnocentrism while type III judges were found to be authoritarian and high on religious conventialism.

Another limitation which supports "bounded rationality" in intuitive decision making is that of making corrent inferences from probabilistic data. Slovic, et al. (1976) have reviewed recent research in this area. Although some of this research has been carried out with scientists, trained in statistics, the "experimental results indicate that people systematically violate the principles of rational decision making when judging probabilities, making predictions, or otherwise trying to cope with probabilistic tasks". The evidence suggests that decision makers tend to ignore uncertainties and rely upon habit or simple rules which neglect uncertainty.

In summary, people seem to be unable to use all the information items provided them in arriving at a decision and, even then, do not know which information items have actually formed the basis for their decision. Further, there are limitations in the processing of probabilistic information. Thus, formal decision methodologies appear to be especially attractive for supporting complex, many-variable decisions involving risk, which is probabilistic by definition. These methods allow the decision maker to rationally assign weights to information items in order to develop an ordered list of the options under consideration.

Decision Methods

Decision methods available include multi-attribute decision analysis (Raiffa, 1968; Edwards, 1975), cost-benefit analysis (Mishan, 1971), and cost-effectiveness analysis. These methodologies are, in fact, closely related; cost-benefit analysis may be derived from multi-objective analysis; cost-effectiveness is a special case of cost-benefit analysis. Cost-benefit analysis has been a popular method for making public policy decisions; it requires that all attributes of the decisions be expressed in common units - usually monetary.

A problem arises, however, if there is no observable market price for the attribute in question, such as is the case for most environmental concerns including the risks to the public's health and safety. The interest in assigning values to human life arises

---

* The basis for findings (2) and (3) is the respondent's subjective post-decision statements about the information items which they thought they had used and their relative importance. These statements can be compared with regression analyses which show information items correlated with the decisions actually taken.

from the wish to evaluate changes in mortality risk for use with the cost-benefit methodology. The methods used, and results obtained, are summarised in Table IV (after Linnerooth and Otway, 1977). Linnerooth (1975a, 1975n, 1976) concluded that a rigorous determeniation of life values is not possible because all methods are either dependent only upon income or are difficult to estimate. (The social objective implied by the former methodologies is that of maximising GNP.) It was recommended that a value, such as $300,000 per life, be chosen for use in cost-benefit analysis and this value be weighted by three factors representing: the personal status of those exposed (age, health, dependents, etc.); third-party interest in life saving (the little-girl-in-the-well case); and psychological factors such as those discussed earlier (degree of consent and control, etc.).
Figure 6 (Niehaus and Otway, 1977) shows results of a study which examined the cost-effectiveness of risk reduction provided by remote nuclear power plant siting. The horizontal line drawn at $1000/man-rem represents the recommendation of the US Nuclear Regulatory Commission as the maximum expenditure justified to reduce radiation exposure by one man-rem. This criterion is based upon the physical risks of radiation exposure. The addition of this line to Figure 6 actually changes the study from cost-effectiveness to cost-benefit. The $1000/man-rem criterion reflects a life value of $1,000,000 assuming a linear dose-consequence relationship.

An alternative procedure to placing a monetary value on each of the impacts or attributes of the decision consequence is to evaluate them in terms of "utility". In the terminology of multi-attribute decision analysis the problem of valuing each of the decision consequences in terms of utility is referred to as assessing a multi-attributed utility function over the n attributes. The basic idea of multi-attribute utility measurement is to elicit the value of each attribute in terms of the decision maker's preferences, one attribute at a time, and then to aggregate them using a suitable aggregation rule and weighting procedure. For a good review of multi-attribute utility theory, see von Winterfeld, 1975.

Probably the most widely used, and certainly the simplest aggregation rule and weighting procedure, is the SMART (Simple Multi-Attribute Scaling Technique) procedure (Edwards, 1975), which involved taking a weighted linear average. This can be written:

$$U_i = \sum_j w_j u_{ij} \qquad \text{Equation 2}$$

where w_i = normalized importance weight of j^{th} value dimension.

u_{ij} = utility of i^{th} alternative on the j^{th} dimension.

U_i = aggregate utility of i^{th} alternative.

There has been virtually no experience in using public attitudes, i.e., indicators of overall social response, as a formal input in such methodologies. A recent demonstration experiment (Otway and Edwards, 1977) reported encouraging results in using attitudes measures in Edwards' technique. In this experiment a group of decision makers was given technical descriptions of six nuclear waste disposal sites as well as information on public attitudes towards these sites. Preliminary results indicated that the decision process and that public attitudes were an important factor in the decisions taken by the group.

Status of Risk Evaluation

The evaluation of technological risks is in an early stage of development. Suitable methodologies have been developed in separate academic disciplines of the social and behavioural sciences. They have yet to be adopted for routine application to technological risks. The applicability of risk evaluation methodologies to practical problems

involving technological risks is not as well developed as are the risk estimation methodologies.

RISK MANAGEMENT

Looking again at Figure 1, the section called Risk Management refers to the actions one might take, given the information on the technical system, its risks, and the corresponding social attitudes. The possibilities to resolve conflicts lie basically in changing the technological system, the social system or the decision process.

Technology Change

Risk estimation studies identify risks that might be too high and analyse ways to change the technology in order to reduce the risk. However, attitudes would be expected to be sensitive to changes in the physical characteristics of the technology primarily if the change could be directly observed (e.g., reduction in airport noise). This is not necessarily the case where evidence of the change is in the form of new information provided, e.g., an improved safety system in a nuclear plant. The description of a changed technology provides only one of many informational inputs and would not necessarily be reflected in the cognitive structure underlying attitude.

Social System Change

A survey of the social psychology literature on attitude change suggests that there is no quick and easy way to change people's attitudes. Research has failed to show any evidence of consistent and controlled attitude change. The regularity with which people conduct their daily lives and the persistence of customs, myths, ideals, and mores demonstrates the basic stability of attitudes and their tendency to evolve rather than to change abruptly. This research has revealed a large number af variables, all important in attitude change, which demonstrate its complexity. These variables include: impact effects, anchoring and double anchoring, personal involvement, reference sets, discrepancy between initial attitude and communication, and the credibility of the information source.

A few general principles emerge from this literature which are of interest. First the credibility of the communicator is generally agreed to be an important variable. That is, if you want people to believe what you have to say, then you yourself must be believable to them. This is obvious. Credible persons are those known for expertness or prestige in the subject at hand, or, sometimes, on another subject. For the non-prestigeous, credibility is established by simply always providing factual and balanced information. Another variable agreed to be important is the discrepancy between the message and the initial attitude. People have a "tolerance band" about the position of their initial attitude in which they are willing to accept and, at least, process information. This evidence suggests that extreme messages, which fall outside this tolerance band, tend to have an effect opposite to that intended. For example, a strongly positive message may sound very appealing to an industry executive, but it might very well tend to change, in a negative direction, the attitudes of those who are uncommitted. A few simple points might be noted which could help make public communications about technological issues more effective, they are: (1) always be factual; (2) give both sides of the story; and (3) avoid taking extreme positions.

In summary, attitude change does not seem to be a productive area for risk management activities.

Decision Making

A promising area for risk management is in improving the decision process and in helping to broaden participation in decisions affecting the public through the use of de-

cision methodologies. This does not mean that the decision process can be "mechanised"; however, it should be possible for the decision-making group to evaluate alternatives using a decision model, and then, by an iterative procedure, make the model results and their holistic decisions agree. This would provide a record of what variables were used in reaching a decision, what weights they were given and, most important, what values were assigned to them. This information could provide a starting point for increasing the transparency of the decision process. The wish for more participation in public decision processes is one of the important underlying issues in the opposition to technology.

CONCLUDING REMARKS

The proposed framework for risk assessment studies allows an interdisciplinary approach to the formal consideration of social values in decision making. Risk assessment is still in a research stage. At present, the major contribution of such studies is an improved understanding of the technical and social systems being investigated and the acquisition of new insights into their interactions; that is, the interdisciplinary process involved may be more valuable than the numerical results produced.

Risk estimation methodologies for technical systems are quite well understood and several practical analyses have been carried out in the nuclear energy field. The extension of these methodologies to some other technologies may be complicated by the uncertainties about the biological effects. Methodologies suitable for risk evaluation have been developed within several specialised academic disciplines; their utility in describing the social response to technological risks, and the use of these data in decision making, has been demonstrated in pilot applications. A considerable amount of developmental work is required to bring these methodologies to the point of practical use.

It has been suggested that the real value of risk assessment studies may be an improved understanding of the technical and social systems being investigated and the acquisition of new insights into their interactions. The exchange of knowledge between persons with different disciplinary backgrounds has already been instructive. For example, those with backgrounds in the natural sciences have often found difficulty in understanding that the public response to a technolgy could be "out of proportion" to estimates of the risks to be expected. Psychological research indicates that one would expect a more complex cognitive structure, that between five and ten salient attributes would determine attitude, and that the risk estimates provide only one information item in the attitude formation process.

Current discussions about the acceptability of technologies are providing a forum to evaluate philosophies underlying different visions of the future. Public planning and decision processes are the mechanisms to resolve the implied value conflicts - the problem may be conceived as the reconciliation of technological capabilities with the needs and wishes of the public. This problem of integrating social values with technologies will assume increasing and lasting importance. Risk assessment may be only a transitory form in a developing analytical process, but the importance of the issues being addressed suggests that research along these general lines will continue.

REFERENCES

Arrow, K., Social Choices and Individual Values. Wiley, New York (1951).

Beattie, J.R., "Risks to the Population and the Individual from Iodine Releases", Nuclear Safety, 8, (1967) 573.

Edwards, Ward. "Public Values: Multi-Attribute Utility Measurement for Social Decision Making". (Proceedures of a workshop on Decision Making with Multiple Conflicting Objectives). International Institute for Applied Systems Analysis, Laxenburg (1975).

Farmer, T.R., "Reactor Safety and Siting: A Proposed Criterion". Nuclear Safety, 8, (1967), 539.

Fishbein, M. Attitude and the Prediction of Behaviour. Readings in Attitude Theory and Measurement (Fishbein, M., ed.), John Wiley and Sons, Inc., New York (1967).

Fishbein, M., I. Ajzen. Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research. Addison-Wesley Publ. Co., Reading, Massachusetts (1975).

Fischhoff, B., et al., How Safe is Safe Enough? A psychometric study of attitudes towards technological risks and benefits. To be published. Private communication (1976).

Kates, R.W., Risk Assessment of Environmental Hazard. SCOPE Report 8, Scientific Committee on Problems of the Environment, Paris, France (1976).

Linnerooth, J. "The Evaluation of Life-Saving: A Survey". Research Report RR-75-21, International Institute for Applied Systems Analysis, Laxenburg (1975b).

Linnerooth, J. "A Critique of Recent Modelling Efforts to Determine the Value of Human Life". Research Memorandum RM-76-67, International Institute for Applied Systems Analysis (1976a).

Linnerooth, J. "Methods for evaluating mortality risk", Futures, 8, (1976).

Linnerooth, J., H.J. Otway. "The Implied Social Objectives of Methods Used for Mortality Risk Evaluation". Research Memorandum RM-77-XX, International Institute for Applied Systems Analysis, (1977), in press.

Mishan, E.J. Cost-Benefit Analysis. Allen and Unwin, London (1971).

National Radiological Protection Board. Radiological Protection Standards in the United Kingdom. NRPB-R46. Her Majesty's Stationary Office (1976).

Niehaus, F. "A Non-Linear Eight Level Tandem Model to Calculate the Future CO_2 and C-14 Burden to the Atmosphere". Research Memorandum RM-76-35. International Institute for Applied Systems Analysis, Laxenburg (1976).

Niehaus, F., H.J. Otway. The Cost-Effectiveness of Remote Nuclear Reactor Siting. Accepted for publication in Nuclear Technology, (1977).

Osgood, C.E., et al., The Measurement of Meaning. University of Illinois, Urbana, (1957).

Otway, H.J., R.D. Erdmann. "Reactor Siting and Design from a Risk Viewpoint". Nuclear Engineering and Design, 13 (1969), 365.

Otway, H.J., R.K. Lohrding, M.E. Battat. "A Risk Estimate for an Urban-Sited Reactor". Nuclear Technology, 12 (1971), 173.

Otway, H.J. "Risk Estimation and Evalution". (Proceedings of the IIASA Planning Conference on Energy Systems), PC-73-3, International Institute for Applied Systems Analysis, Laxenburg (1973).

Otway, H.J. "Risk Assessment and Societal Choices". Research Memorandum RM-75-2, International Institute for Applied Systems Analysis, Laxenburg (1975).

Otway, H.J., J.J. Cohen. "Revealed Preferences: Comments on the Starr Benefit-Risk Relationships". Research Memorandum RM-75-5, International Institute for Applied Systems Analysis, Laxenburg (1975).

Otway, H.J., R. Maderthaner, G. Guttmann. "Avoidance-Response to the Risk Environment: A Cross-Cultural Comparison". Research Report RR-75-14, International Institute for Applied Systems Analysis, Laxenburg (1975).

Otway, H.J., P.D. Pahner. "Risk Assessment", Futures 8, 2, (1976) 122-134.

Otway, H.J., M. Fishbein. "The Determinants of Attitude Formation: An Application to Nuclear Power". Research Memorandum RM-76-80, International Institute for Applied Systems Analysis, Laxenburg (1976).

Otway, H.J. "A Review of Research on the Identification of Factors Influencing the Social Response to Technological Risks". To be presented at the IAEA Conference on Nuclear Power and Its Fuel Cycle. To be held from 2 through 13 May, 1977, at Salzburg, Austria (1977).

Otway, H.J., Ward Edwards. "An Application of Multi-Attribute Utility Theory to the Selection of Waste Disposal Sites". Research Memorandum RM-77-XX, International Institute for Applied Systems Analysis, Laxenburg (1977), in press.

Pahner, P. "A Psychological Perspective of the Nuclear Energy Controversy". Research Memorandum RM-76-67, International Institute for Applied Systems Analysis, Laxenburg (1976).

Raiffa, H. Decision Analysis. Addison-Wesley, Reading, Massachusetts (1968).

Rowe, W.A. An "Anatomy" of Risk. United States Environmental Protection Agency (1975).

"Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants". WASH-1400 (NUREG-75/014), United States Nuclear Regulatory Commission, Washington, D.C. (1975).

Simon, H.A. Models of Man. Wiley, New York (1957).

Slovic, P., B. Fischhoff, S. Lichtenstein. "Cognitive Processes and Social Risk Taking", Cognitive and Social Behaviour (Carrol, J.S., J.W. Payne, eds.), Lawrence Erdlbaum Assoc., Potomac (1976).

Starr, C., "Social Benefits vs. Technological Risk". Science, 165, (1969) 1232-38.

Wiggins, N.P., P.J. Hoffman, T. Tabler. "Types of Judges and Cue Utilization in Judgement of Intelligence: Journal of Personality and Social Psychology", 12, (1969) 52-9.

Winterfeld, D. von. "An Overview, Integration, and Evaluation of Utility Theory for Decision Analysis". SSRI Research Report 75-9. Social Science Research Institute, University of Southern California, Los Angeles (1975).

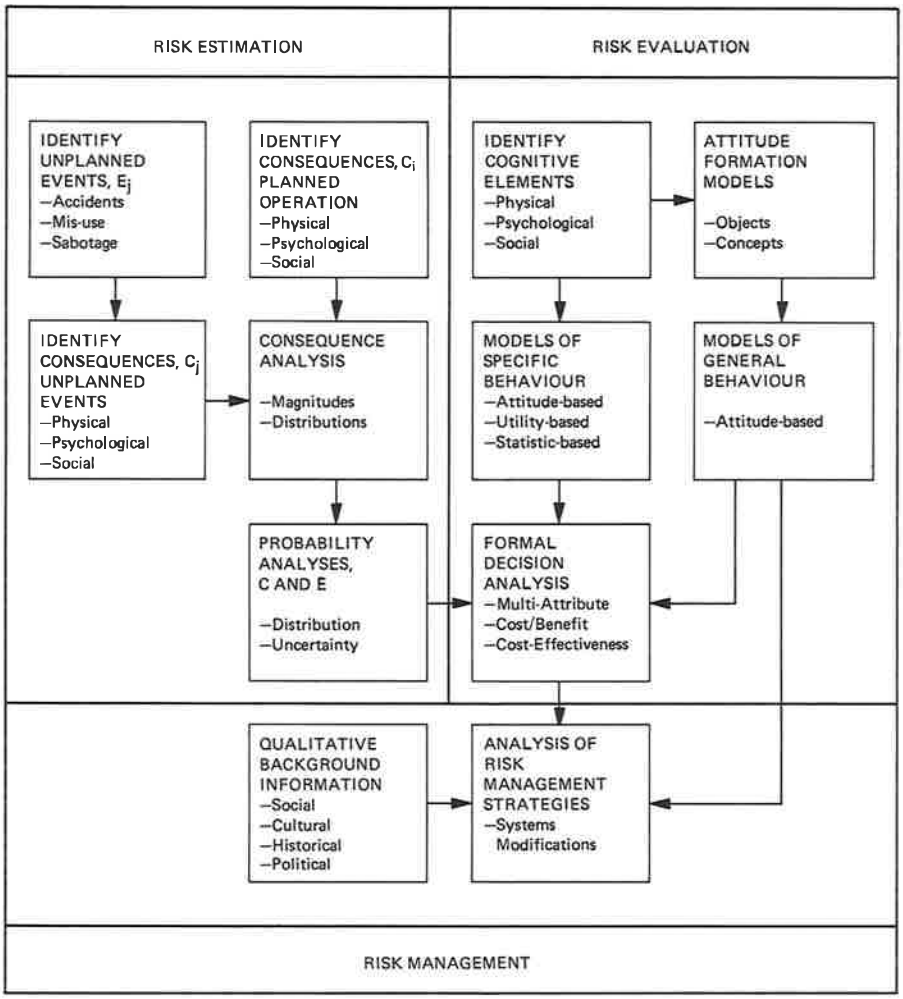
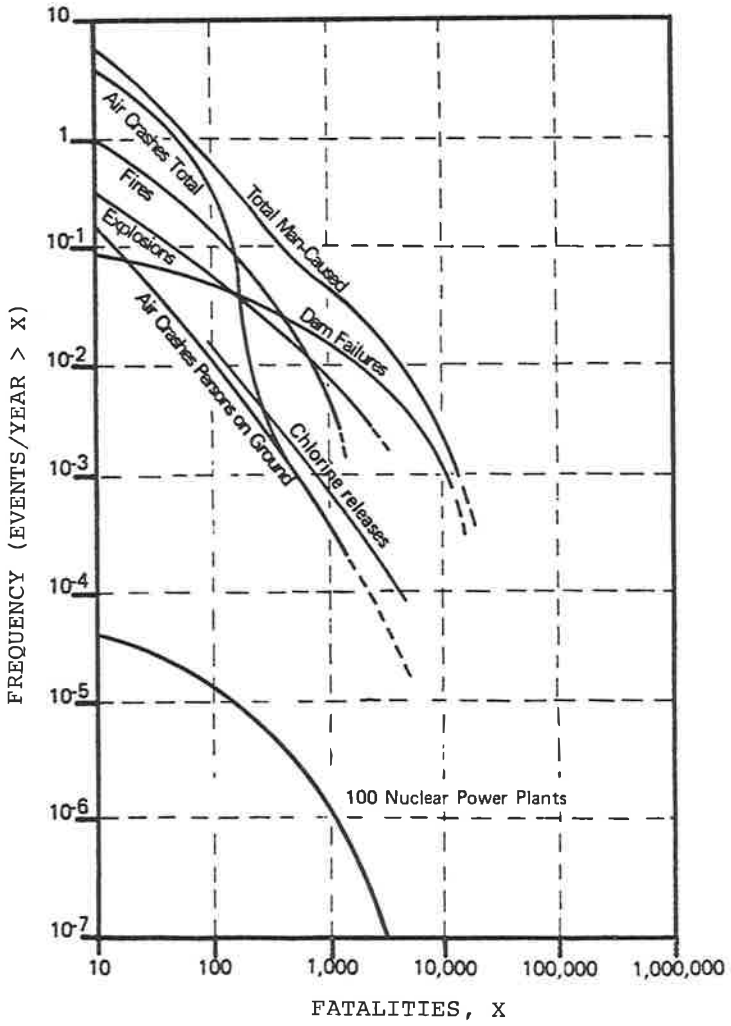

RISK ESTIMATION
RISK EVALUATION
IDENTIFY UNPLANNED EVENTS, E_j
–Accidents
–Mis-use
–Sabotage
IDENTIFY CONSEQUENCES, C_i PLANNED OPERATION
–Physical
–Psychological
–Social
IDENTIFY COGNITIVE ELEMENTS
–Physical
–Psychological
–Social
ATTITUDE FORMATION MODELS
–Objects
–Concepts
IDENTIFY CONSEQUENCES, C_j UNPLANNED EVENTS
–Physical
–Psychological
–Social
CONSEQUENCE ANALYSIS
–Magnitudes
–Distributions
MODELS OF SPECIFIC BEHAVIOUR
–Attitude-based
–Utility-based
–Statistic-based
MODELS OF GENERAL BEHAVIOUR
–Attitude-based
PROBABILITY ANALYSES, C AND E
–Distribution
–Uncertainty
FORMAL DECISION ANALYSIS
–Multi-Attribute
–Cost/Benefit
–Cost-Effectiveness
QUALITATIVE BACKGROUND INFORMATION
–Social
–Cultural
–Historical
–Political
ANALYSIS OF RISK MANAGEMENT STRATEGIES
–Systems Modifications
RISK MANAGEMENT

FIGURE 1

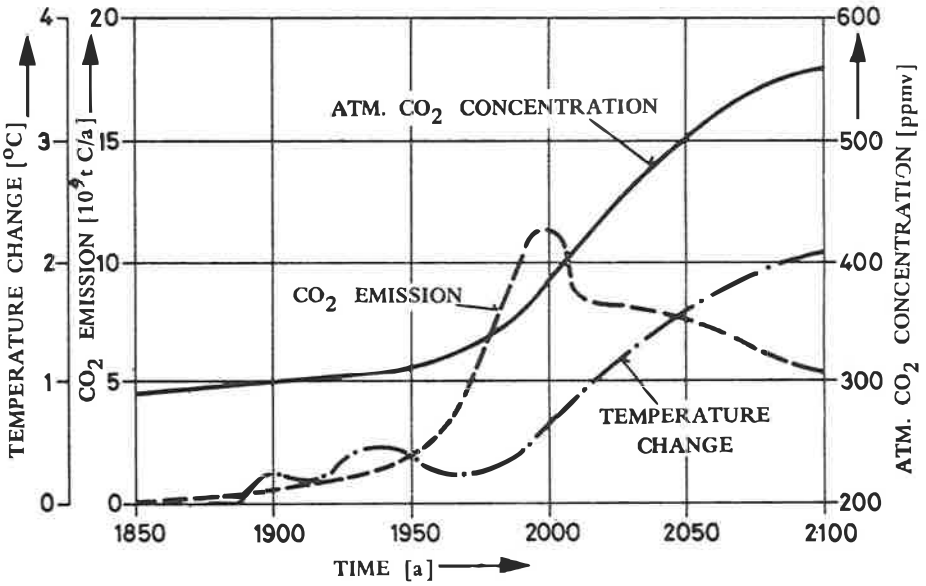


EXAMPLE OF A RISK ESTIMATION RESULT

UNPLANNED EVENTS

(AFTER RASMUSSEN)

FIGURE 2



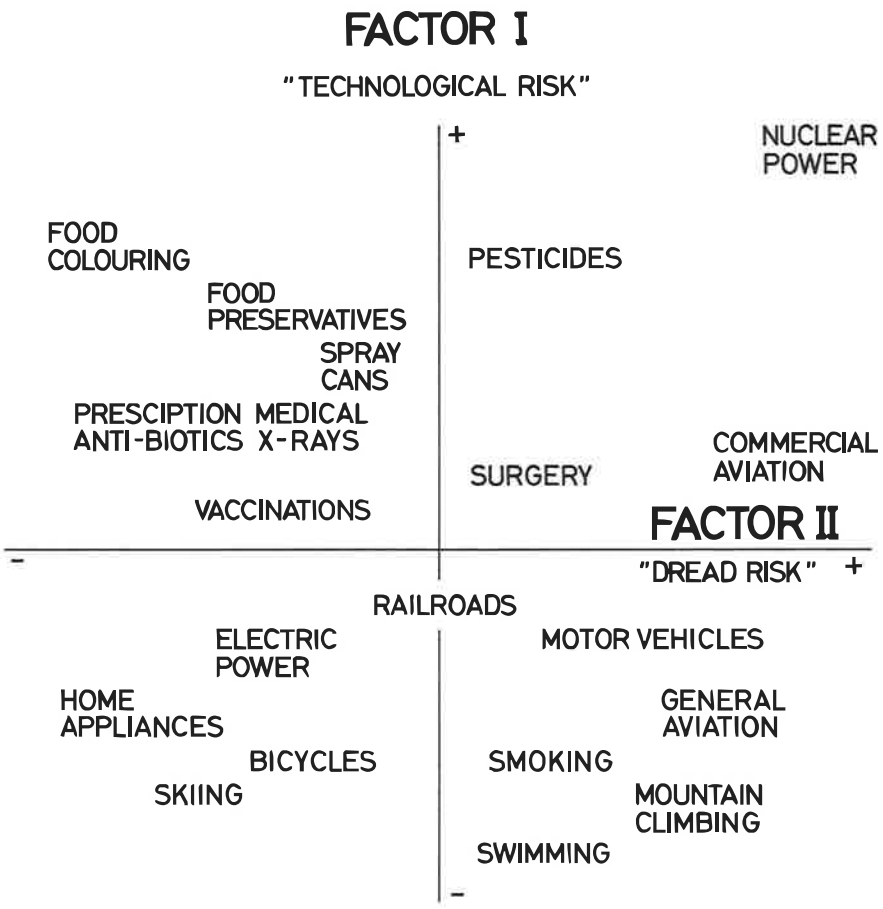
Simulation of the CO_2 burden to the atmosphere with regard to an optimistic equilibrium strategy.

EXAMPLE OF A RISK ESTIMATION RESULT

PLANNED OPERATIONS

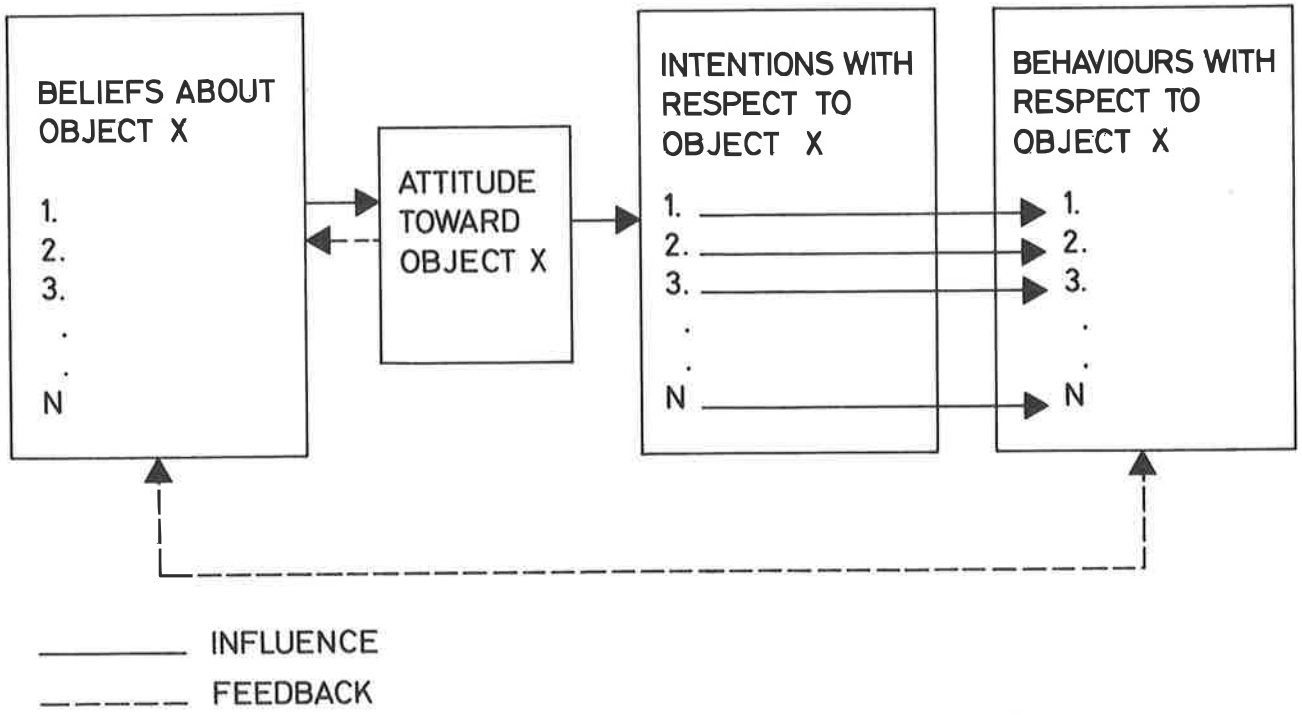
(AFTER NIEHAUS)

FIGURE 3



LOCATION OF RISK ITEMS IN A TWO - FACTOR PSYCHOLOGICAL SPACE

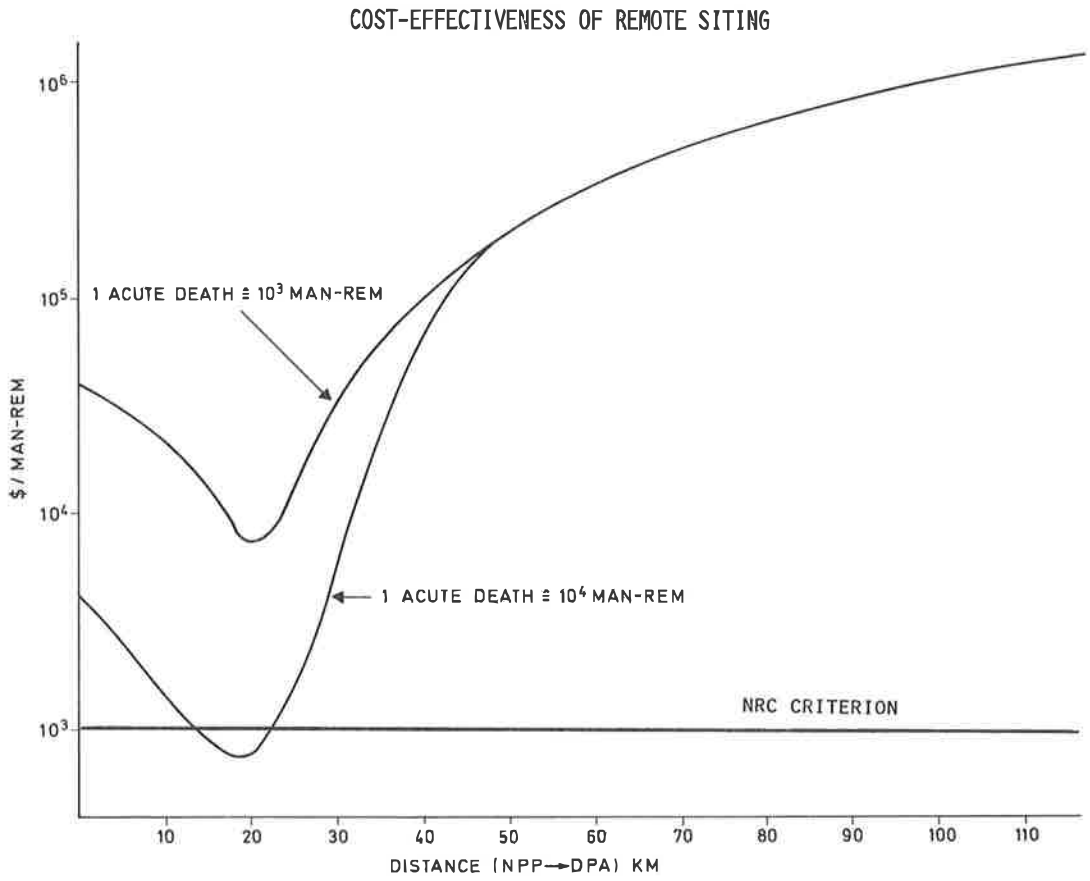
FIGURE 4



A Model of Attitude Formation
(after Fishbein)

FIGURE 5

FIGURE 6


COST-EFFECTIVENESS OF REMOTE SITING
$/ MAN-REM
10^6
10^5
10^4
10^3
1 ACUTE DEATH ≡ 10^3 MAN-REM
1 ACUTE DEATH ≡ 10^4 MAN-REM
NRC CRITERION
10
20
30
40
50
60
70
80
90
100
110
DISTANCE (NPP→DPA) KM

IMPORTANCE OF ATTITUDE DETERMINANTS - NUCLEAR POWER

DETERMINANT	TOTAL SAMPLE	
	Importance Rank	Average Importance $\overline{\lvert eb \rvert}$
creates noxious wastes	1	5.17
can be mis-used in a destructive way	2	5.03
can affect large numbers of people at the same time	3	5.00
provides good value for the money	4	4.47
provides benefits which are essential to society	5	4.27
enhances "quality of life"	6	3.70
consumes large quantities of natural resources	7	3.37
in the hands of big government or business	8	3.00
uses principles and processes which are difficult to conceptualize	9	2.77
presented a new and different mode of death	10	2.73
offers social benefits which are not highly visible	11	2.30
seldom seen or contacted in daily life	12	1.63

TABLE I

COGNITIVE STRUCTURE UNDERLYING ATTITUDES TOWARD NUCLEAR POWER

DETERMINANT	Average Attitude Contribution $\overline{eb}$ "pro"	"con"	Average Belief Strength $\overline{b}$ "pro"	"con"	Average Evaluation $\overline{e}$ "pro"	"con"
provides good value for the money	7.00	0.80**	2.80	0.30**	2.50	1.90
enhances "quality of life"	6.70	-0.50**	2.60	-0.50**	2.60	1.60**
provides benefits essential to society	5.80	0.90*	2.20	0.30*	2.70	2.60
can be mis-used in a destructive way	-4.30	-5.70	2.00	2.20	-2.30	-2.30
uses principles and processes difficult to conceptualize	-3.40	-2.00	2.80	2.50	-1.20	-0.80
creates noxious wastes	-2.70	-6.60	1.80	2.30	-1.70	-2.50*
can affect many people at the same time	-2.60	-5.30	1.90	2.60	-1.70	-2.70**
consumes large quantities of natural resources	2.50	0.90	-1.00	-0.30	-2.10	-2.10
in the hands of big government or business	1.20	-2.80*	2.90	2.60	-0.40	-1.00
presented a new and different mode of death	-1.20	-4.10	1.50	2.40	-1.10	-1.50
offers social benefits not highly visible	-0.70	1.00	1.60	0.90	0.00	0.30
seldom seen or contacted in daily life	0.10	-1.50	1.20	2.30	0.10	-0.50

* difference significant at 0.05 level

** difference significant at 0.01 level

TABLE II

AN EXAMPLE OF CUE UTILISATION

IN

DECISION MAKING

(AFTER WIGGINS, ET AL.)

CUES	JUDGE TYPE				
	I (45)	II (28)	III (53)	IV (10)	V (5)
1. HIGH SCHOOL RATING	.97 ***	.34 **	.45 ***	.61 ***	.38 ***
2. STATUS	.08	.08	.20	.05	.81 ***
3. SELF-SUPPORT	-.03	-.09	.07	.08	.03
4. ENGLISH EFFECTIVENESS	.16	.90 ***	.42 ***	.24 *	.32 **
5. RESPONSIBILITY	-.10	.04	.46 ***	-.01	.20
6. MOTHER'S EDUCATION	.05	.07	.15	.26 *	.12
7. STUDY HABITS	.00	.03	.46 ***	-.08	-.09
8. EMOTIONAL ANXIETY	.08	.09	.11	.05	.11
9. CREDIT HOURS	.23 *	.24 *	.24 *	.75 ***	.17
MULTIPLE CORRELATION	.99	.99	.98	.95	.97

* STATISTICAL SIGNIFICANCE < 5%

** STATISTICAL SIGNIFICANCE < 1%

*** STATISTICAL SIGNIFICANCE < 0.1%

TABLE III

LIFE VALUATION FOR PURPOSES OF COST-BENEFIT ANALYSIS

(AFTER LINNEROOTH)

APPROACHES	VALUES	LIMITATIONS
(1) **IMPLICIT VALUE**	$9,000 - $9,000,000	. ASSUMES PAST DECISIONS ARE OPTIONAL
(2) **HUMAN CAPITAL**	$100,000 - $400,000	. BASED SOLELY ON LIFETIME INCOME . IGNORES INDIVIDUAL PREFERENCES . DISCRIMINATES AGAINST UNPRODUCTIVE MEMBERS OF SOCIETY
(3) **INSURANCE PREMIUMS**	WIDE RANGE	. DOES NOT TAKE INTO ACCOUNT INDIVIDUAL'S INTEREST IN PROTECTING HIS OWN LIFE
(4) **COURT AWARDS**	~$250,000	BASED ON LOST EARNINGS
(5) **WILLINGNESS TO PAY**	$180,000 - $1,000,000	. DIFFICULT TO ESTIMATE . DEPENDS ON RISK SITUATION

SUMMARY

ALL MEASURES DEPEND TO SOME EXTENT ON THE LIFETIME EARNING POTENTIAL OF THE INDIVIDUALS AT RISK AND IGNORE PERCEPTION OF SERIOUSNESS.

CONCLUSION

CANNOT BE RIGOROUSLY DETERMINED. CHOOSE VALUE (SAY $300,000) WEIGHT ACCORDING TO: PERSONAL VARIABLES, THIRD PARTY INTERESTS AND PSYCHOLOGICAL FACTORS.

TABLE IV

A simple theory on the reliability of automatic protective systems

Ir. H. J. de Heer
DSM
Geleen
The Netherlands

Summary

The main issues with regard to automatic safety devices are: 1. confrontation of a failed state of the device with a demand on its function, and 2. unsolicited action. If a single safety device cannot attain the required reliability with respect to either one issue or both, two or more devices are arranged to form a protective system. The present theory covers both issues and the systems required to meet them. This is done without recourse to probability distribution functions. Instead, the concept of unavailability is made use of. The indispensability of regular testing is shown and the implications thereof are considered. Some thought is devoted to the limitations of this and other theories.

Introduction

An automatic safety device has the task of preventing a process variable from transgressing a predetermined limit, as is symbolically represented in Fig. 1. The following considerations are also valid for the type of device that detects the presence or absence of a condition and triggers off action accordingly. A flame-failure device belongs to that category.
Safety devices have a passive function. They are only called upon in the case of a limit-transgression, more generally called a demand. Consequently, a failed state is not revealed unless the device is tested on its functional capability, either by regular testing or, less comfortably, by a demand!
Safety devices can also act unsolicitedly. A loosened wire or a broken connection can shut down an entire plant. This kind of failure results in immediate action and therefore is selfrevealing. It is commonly called a spurious failure.

Failure rate

Failures are assumed to occur randomly in time and independent of other events. If, during t years, we have observed an event to occur n times, we can define a mean rate of occurrence:

$$r = \frac{n}{t} \tag{1}$$

If the events are failures, r is called the mean failure rate. The reciprocal is often used and is called the Mean Time Between Failure (incidence), commonly abbreviated to:

$$MTBF = \frac{1}{r} \tag{2}$$

In practice, r is an average from observations made on different but similar apparatus in different but similar situations since, as behoves proper safety devices, failures are rare events.

Unavailability

As we have seen, only the coincidence of a failed state and a demand will consitute a hazard. Clearly, not only the failure rate but also the duration of a failed state is of primary importance.

By regularly testing the device, a non-selfrevealing (dangerous) failure, if present, will be detected and remedied. A failed state can therefore exist no longer than the interval T between two tests. In the mean, the duration of a failed state will take on a value between zero and T.
Now imagine time as a long straight line, with a large number of regularly spaced markings on it, representing tests. Imagine failures to be irregularly and sparsely distributed along this line, with a duration varying from zero to T. This image can be likened to that of a long wall with narrow gates of varying width, dispersed sparsely and unevenly along its length. Suppose a blind insect is flying in a direction perpendicular to the wall, approaching a spot unknown to us. The probability of the insect flying through a gate instead of hitting the wall simply equals:

$$\Pr(\text{gate}) = \frac{\text{total width of all gates together}}{\text{total length of the wall}}, \text{ or, after some reflection}$$

$$\Pr(\text{gate}) = \frac{\text{mean width of the gates}}{\text{mean spacing of the gates}} \quad \text{(Law of Large Numbers)}$$

Accordingly, the probability of a failes state at a random moment equals:

$$\Pr(\text{failed state}) = \frac{\text{Mean Failed Time (MFT)}}{\text{Mean Time Between Failure (MTBF)}}$$

This instantaneous probability is called unavailability. If it is indicated by U and if the reciprocal of the MTBF, the mean failure rate, is to be called MFR, the fundamental truth found above can also be written as:

$$U = \text{MFT} \times \text{MFR} \tag{3}$$

often called Fractional Dead Time (FDT) in literature. German publications will call this Unverfügbarkeit or Relative Ausfallzeit.
We still have to assess which value between zero and T the MFT takes on. We will assume this to be T/2 since the occurence of a failure will show no preference for any moment in T whatsoever. Testing, a go-no-go procedure, will not influence this statement. Actually, it will bear slight correction (1) but that is very small and can be neglected for practical purposes.
Thus, if the MFT of a single safety device is denoten by t_u, we can write:

$$\text{MFT} = t_u = \frac{T}{2} \tag{4}$$

Substituting eqs. (2) and (4) into eq. (3) yields:

$$U = rt_u = \frac{rT}{2} \tag{5}$$

Hazard rate

A hazard is created as soon as a demand coincides with a failed state. We assume demands to occur randomly. We also assume them to have been recorded, e.g. from the number of times the safety device was required to act, and what we can therefore formulate a mean demand rate, in the manner shown by eq. (1). Since demands occur at random moments in time and since unavailability is defined as the probability of a failed state at a random moment in time, we can forthwith formulate a mean hazard rate. Applying the Law of Large Numbers, we postulate that the mean hazard rate h equals:

$$h = g.U \tag{6}$$

because only a fraction U.n. of a total number of n demands in a time t will be 'successful', i.e. will create a hazard. Since U.n. denotes the number of hazards, the hazard rate will be U.n/t, and with n/t = g we arrive at eq. (6). Combination of eqs. (5) and (6) yields:

$$h = g.r.t_u = g.r.\frac{T}{2} \qquad (7)$$

This, then, is the fundamental relation for the performance of a safety device with a mean failure rate r, in the face of a mean demand rate g, when tested at regular intervals T.

Redundancy, 1-from-2 system

Assume the safety device to have an MTBF of 10 yrs and that demands occur once a year on the average. That means 2 = 0.1 and g = 1. With monthly testing, T = 0.08 yrs approximately. This yields a hazard rate of h = 0.004 hazards a year and a Mean Time Between Hazards (MTBH) of 250 years.
If a particular hazard has grave consequences, this is unacceptable. In such cases, an MTBH of at least 10,000 yrs is considered adequate. This is not attainable with a single device. We then have to resort to redundant arrangements, such as symbolically presented in Fig. 2. The devices are arranged in such a way, that activation of either one or the other or both will trigger off relevant action. For example, two automatic pressure relief valves in the same steam line will function that way. Such arrangements are called 1-from-2 systems. These systems will only fail if both elements are in a failed state simultaneously.
We assume both elements to be tested regularly with an interval T. If the unavailabilities of the elements are U_1 and U_2, the probability of both elements being in a failed state at a random moment is given by:

$$U(1\text{-from-}2) = U_1.U_2 = U^2 \text{ if } U_1 = U_2 = U \qquad (8)$$

according to elementary probability theory. If this system is confronted with g demands a year, the hazard rate according to eq. (6) will be:

$$h(1\text{-from-}2) = g.U(1\text{-from-}2) \qquad (9)$$

Thus, the hazard rate of a 1-from-2 system is U times that of a single device. If U = 0.004 again, the hazard rate will be reduced 250 times and the MTBH will be 250 times as large, i.e. 62,500 years!

Selfrevealing (spurious) failures

In a 1-from-2 system, action in either element, be it functional or unsolicited, triggers off the system, and there are two devices to play that game! Therefore, if the spurious failure rate of a single device is called z (to discern it from r), we conclude:

$$a(1\text{-from-}2) = 2z \qquad (10)$$

The 2-from-2 system

We could also arrange two devices in the manner shown in Fig. 3. In that case, the system is only activated when both devices are activated (one AND the other). This means that if one and only one device fails, the whole system gets into a failed state. In proper logic: the system fails if one or the other or both devices are in a failed state.
If we assume both devices to be tested regularly and the unavailabilities to be U_1 and U_2 respectively, elementary probability theory has it that

$$U_{syst} = U_1 + U_2 - U_1U_2$$

Since U_1 and U_2 are small figures, the product U_1U_2 can be neglected. Therefore, if $U_1 = U_2 = U = rt_u$, we have:

$$U\ (2\text{-from-}2) = 2U = 2rt_u \qquad (11)$$

So this system is less safe than a single device, but it will reduce the spurious failure rate dramatically. If one device develops a spurious failure, the system does not react unless and until the other one also develops a spurious failure before the next proof-test. Hence, in analogy to the situation with dangerous (non-selfrevealing) failures, the first device to develop a spurious failure can be said to be in a failed state, i.e. unavailable, the unavailability in this case being $U_{sp} = zt_u$. In keeping with eq. (6) and the philosophy behind it, spurious failures of the other device, occurring at the same rate z, are only 'successful' in $z.U_{sp} = z^2t_u$ cases. This rate, however, only represents half the number of possible cases, because the devices are mutually interchangeable. So we can write:

$$z(2\text{-f-}2) = 2z.U_{sp} = 2z^2t_u \tag{12}$$

$$\text{MTBF}(2\text{-f-}2) = \frac{1}{z(2\text{-f-}2)} \tag{13}$$

If the MTBF of a single device is 10 yrs, the failure rate will be z = 0.1. Assuming T = 0.08 yrs, and therefore t_u = 0.04 yrs, the system failure rate will be 0.008 and the MTBF will be 1250 yrs. This is a great deal more than the 10 yrs of a single device. Conclusion: the 2-from-2 system can be applied in those cases where the safety would be more than adequately ensured by a single device, but the spurious failure rate of the latter would be prohibitive with regard to loss of production or other nuisance caused.

The 2-from-3 system

If one wants a high degree of protection and at the same time a very low spurious failure rate, a 2-from-3 system is indicated. The arrangement is symbolised in figure 4. As can be seen, the system only reacts if at least two of the three constituting devices are activated, be it by demands or by spurious failures. Also, the system will fail functionally if at least two elements are in a failed state. Hence, the system can cope equally well with both kinds of failures.
In Appendix 1 and Appendix 2 a general but still simple theory has been worked out for M-from-N systems, i.e. systems with N elements, at least M of which have to be activated to trigger off the system. By substituting 3 for N and 2 for M, the general equations yield the unavailability and the spurious failure rate of a 2-from-3 system. We will find:

$$h(2\text{-f-}3) = 3gU^2 = 3g(rt_u)^2 \qquad \text{if } rt_u \ll 1 \tag{14}$$

$$z(2\text{-f-}3) = 6z.zt_u = 6z^2t_u \qquad \text{if } zt_u \ll 1 \tag{15}$$

It is seen that the 2-from-3 system is less safe than the 1-from-2 system and less reliable than the 2-from-2 system, but unlike these two-channel systems, it improves both availability and reliability in relation to a single channel.

Systems of higher redundancy

The next symmetrical M-from-N system is the 3-from-5 system. To date, the author never has seen any in operation. If the results of Appendices 1 and 2 are applied, systems of higher redundancy appear to acquire disproportionally large coefficients (see also Appendix 4) because of the increasing number of combinations possible, so that the gain with respect to a 2-from-3 system is disappointing. The latter seems to be the optimum configuration. The difficulty and cost of realizing complex systems emphasises this statement.

Optimum proof-testing frequency

The act of proof-testing takes time. Since the safety device is taken out of commission

during that time, testing adds to the unavailability. If the average time needed for testing is called t_t, this will introduce an unavailability of t_t/T since the test will be carried out after every interval T. So the unavailability of a single device, formerly taken to be rT/2, turns out to be:

$$U = \frac{r(T-t_t)}{2} + \frac{t_t}{T} \tag{16}$$

Clearly, there is an optimum beyond which T must not be reduced because then U will increase again. The optimum for T can be found in the usual manner, by equalling the first derivative dU/dT to zero. This yields:

$$T_{min} = \sqrt{\frac{2t_t}{r}} \tag{17}$$

$$U_{min} = \sqrt{2rt_t} \qquad \text{if} \quad t_t \ll T \tag{18}$$

There is no point in shortening the testing interval beyond T_{min}.

Staggered testing

Staggered testing, as opposed to simultaneous testing, aims at shortening the MFT (Mean Failed Time) without reducing the test-interval T. It is only applicable to systems with two or more elements or channels, such as 1-from-2 and 2-from-3 systems.
Each separate channel will still be tested at intervals T, but the individual channels are tested consecutively, the testing times being evenly distributed over a time span T. If there are N channels, each channel will be tested a time T/N later than the previously tested one.
Fig. 5 schematically depicts the procedure for a 2-from-3 system. For clarity, each channel is drawn on a separate time axis. The tests of the channels are shifted over a time T/3.

Since a failure can persist no longer than T, i.e. up till the next test, the maximum duration of two coexisting failures will be 2T/3, whereas with simultaneous testing the maximum time of coexistence would be T (neglecting the testing time). Hence, with staggered testing, the period of coexistence can take all from 2T/3 to zero, whereas, with simultaneous testing, the limits are T and zero. Since all situations are equally probable, we conclude that the system will behave as if it were tested simultaneously but at intervals of 2T/3 instead of T. In that case, the MFT of a single channel, t_u, would be T/3 instead of T/2.
Now it can be shown (2) that an M-from-N system with simultaneous channel-testing has an MFT equal to:

$$\text{MFT(M-from-N)} = \frac{t_u}{N-M+1} \qquad \text{if} \quad rt_u \ll 1 \tag{19}$$

i.e. proportional to the MFT of a single channel. From the above, we conclude that staggered testing will reduce the MFT of a 2-from-3 system by a factor of 2/3 as compared with simultaneous testing.
Appendix 3 gives full details for M-from-N systems in general. The reduction of the MFT appears to be approximately equal to M/N. Since, for systems where the difference N-M is less than 2, the system failure rate will not be affected by staggered testing, one can conclude that the unavailability of the system is also reduced by M/N, see also eq. (3).
So, a 1-from-2 system finds its unavailability reduced by 1/2, whereas a 2-from-2 system does not benefit at all, as was to be expected.

Some other considerations

In some places in the foregoing, we introduced the condition: $rt_u \ll 1$, to simplify

mathematical relations without sacrificing mathematical severity and to promote practical applicability. However, there are two reasons for making this condition indispensable.
Firstly, remember that $t_u = T/2$. If rt_u would approach unity, the testing interval would become of the order of magnitude of the MTBF. No one in his right mind would choose this interval, because the probability of a failure occurring within every testing interval would then be quite high, which would render proof-testing ineffective.
Secondly, random failure incidence admits the possibility of more than one failure within t_u. In practice, this cannot happen, since a device once failed cannot fail again within t_u. So a large t_u would bring practice in conflict with the assumption of randomness.
Similar considerations are valid for the condition $gt_u \ll 1$, but here the reason is purely practical: t_u is the 'target' for demands! The higher the demand rate g, the smaller the target t_u should be.

An important aspect is the 'testability' of a protective system. One is apt to take it for granted that a channel or system can be proof-tested at intervals T, but how are we to perform a thorough check on a controlling device (valve etc.) all the way without causing an outage?
A solution to this problem will always be expensive, but should be considered with regard to all critical applications. It is advisable then to consider the controlling device separately.
A commendable solution is offered by STEWART (3). Fig. 6 shows such a solution with four valves. In this case, the valves are open during normal operation and are required to effect a shut-down in an emergency. Since the valves are taken up in parallel branches (A and B) of the feed-line, it is obvious that each branch can be tested separately without cutting off the main flow. If the failure rate of one valve equals r_V, the unavailability of two valves in series equals:

$$U_A = U_B = (r_V t_u)^2 = U_V^2 \tag{20}$$

if U_V is the unavailability of one valve. But the branches A and B are in parallel and, as such, operate as a 2-from-2 system: if one branch fails to close, shut-down cannot be effected. We know the unavailability of such a system from eq. (11). With eq. (20) we can write:

$$U_{syst} = 2(r_V t_u)^2 \tag{21}$$

The gain in relation to a single valve amounts to $1/2r_V t_u$. As we have seen, this can easily amount to a factor of 100 or more. However, if the availability of one single, regularly proof-tested shut-down valve would be more than adequate for the application at hand, we could consider the use of two valves in parallel, to provide the required testability. Although one looses a factor of 2 with respect to a single valve, one gains certainty about the condition of the shut-down system at each test. This could easily outdo the theoretical factor of 2. Alas, no data are available on this issue.

We will conclude these considerations with a warning. The apparent ease with which safety can be enhanced by redundancy might lure the user into a false sence of security. Note, however, that a demand rate cannot be lowered by redundant safety devices and that hazard is directly proportional to that rate! It can only be held down by proper (automatic) control of the relevant variables and this should never be neglected. Safety devices shall always be regarded as a last resort. Beyond them lays calamity.

Work of others

A number of authors, including the present one, did approach the problems in a different way. Notwithstanding a fair amount of literature available, there are relatively few publications which treat the present subject as such. For the basic theory used,

one is referred to books and magazines. Hence, as to self-sufficiency and applicability, the present paper might provide to someone's long felt need. Those who find it lacking in scientific standing are referred to APPLEBAUM (2). To this author's knowledge, it is the only paper existing in which an irrefutable scientific foundation is laid. His results confirm those of the present paper as well as those of previous work done by the present author (4).

It is curious to notice that an insight into the underlying principles, so effortlessly exposed in the preceding pages, was only gained in the relatively recent past, say, in the late sixties. Much of the credit for that must go to BOURNE and GREEN (5), who were the first to show the inherent relationship between failure rate, proof-testing, demand rate and hazard rate, as laid down in eqs. (6) and (9) of the present paper. The document (5) cited is a comprehensive treatise on the subject, based on previous work of the authors, which in turn was based on foundations laid in the inner sanctums of ICI. The results are used throughout the United Kingdom. With due respect for the work done, this author has a piece of criticism to offer. Owing to an erroneous approach to the assessment of the MFT, the authors had to go through some mathematical contortions to arrive at conclusions following effortlessly from straightforward reasoning. To arrive at the equivalent of eq. (6) of this paper, they used a (non-converging) series, as if this were an approximation instead of a fundamental truth. Their text is fraught with integrals which, as we have seen, can be dispensed with altogether. Moreover, their coefficients do not corroborate with APPLEBAUM's, a fact which refers them to the dock. The misery all springs from the statement that the probability of failure incidence is zero immediately after every test, and increases with a first order time-constant to a certain value immediately before the next test. This simply cannot be true. A proof-test as such does not alter the physical condition of a protective system, except perhaps for the worse (forgotten blocking valve !). It certainly does not improve that condition; one only observes that the device is free of failures. It is possible that the authors inadvertently borrowed from the so-called renewal theory, in which the problem of replacement is treated. Nevertheless, the results of BOURNE and GREEN are not far off the mark and, viewed in the light of the uncertainty of available statistical data, are undoubtedly applicable in practice, if not in theory. Notwithstanding that, the proper relations are given in Appendix 4.

LITERATURE

(1) SCHNEEWEISS, W. : On the mean duration of hidden faults in periodically checked systems,
SIEMENS AG, Karlsruhe, Germany, July 1975, manuscript, to be published in IEEE Transactions on Reliability.

(2) APPLEBAUM, S.P. : Steady state reliability of systems of mutually independent subsystems,
IEEE Transactions on Reliability, March 1965.

(3) STEWART, R.M. and HENSLEY, G. : High Integrity Protective Systems on Hazardous Chemical Plants,
United Kingdom Atomic Energy Authority, Document SRS/COLL/303/2, May 1971.

(4) DE HEER, H.J. : A basic theory on the probability of failure of safeguarding systems,
Proceeding of the First International Symposium on Loss Prevention and Safety Promotion, Delft, The Netherlands, May 1974.
Elseviers Scientific Publishing Company.

(5) BOURNE, A.J. and GREEN, A.E. : Safety assessment with reference to automatic protective systems for nuclear reactors,
Document AHSB (S) R 117 of the U.K. Atomic Energy Authority, Health and Safety Branch.

APPENDIX 1 : Unavailability of M-from-N protective systems

If the unavailability of a single device or channel equals U, the probability of finding k identical channels simultaneously in a failed state at a random moment in time will be U^k. If there are N channels, of which k are in a failed state and N-k intact, the availability of the latter equals $(1 - U)^{N-k}$. Hence, the probability to find N-k channels intact and k channels defective at any moment in time is given by the expression:

$$U^k . (1 - U)^{N-k}$$

which is valid for one particular group k out of N. For a random group k out of N, the expression must be multiplied by the number of combinations k-from-N :

$$\frac{N!}{(N-k)!\,k!} . U^k . (1 - U)^{N-k}$$

To incapacitate an M-from-N system, k must at least equal N-M+1 and can take discrete values up to N. Therefore, the instantaneous probability of a failed state of an M-from-N system, i.e. its unavailability, equals:

$$U(M\text{-f-}N) = \sum_{k=N-M+1}^{N} \frac{N!}{(N-k)!\,k!} . U^k . (1 - U)^{N-k}$$

In working out the results for a particular M and N, powers of an order higher than N-M+1 can be neglected if $U \ll 1$. This yields the formula used in practice:

$$U(M\text{-f-}N) \lesssim \frac{N!}{(N-M+1)!\,(M-1)!} . U^{N-M+1}$$

APPENDIX 2 : Unreliability of M-from-N protective systems

With regard to selfrevealing (spurious) failures, M channels have to be activated unsolicitedly to cause a selfrevealing system failure. Imagine a system on the brink of failure, which can be pictured as follows: One channel operational with certainty, and a subsystem of N-1 channels, M-1 of which are in an activated (i.e. failed) state and the remaining N-M channels are operational. Such a subsystem is not capable of coping with yet another channel failure and is, in that sense, unavailable. Therefore, we can formulate the unavailability of the subsystem:

$$\frac{(N-1)!}{(N-M)!\ (M-1)!} \cdot U^{M-1} \cdot (1-U)^{N-M}$$

i.e. the number of combinations M-1 out of N-1, times the unavailability of M-1 channels and the availability of N-M channels, with $U = zt_u$ being the unavailability (i.e. instantaneous probability of activated state) of a single channel. This unavailable subsystem is then confronted with the failure of the one channel assumed to be operational with certainty. However, one should realize that each of the N channels can play the part of the one channel, so that the unavailable subsystem is confronted with failures at a mean rate of Nz. To find the number of 'successful' confrontations, i.e. the system failure rate, one multiplies Nz by the unavailability calculated above. This yields the spurious failure rate of the system:

$$r_{sp}(M\text{-f-}N) = Nz \cdot \frac{(N-1)!}{(N-M)!\ (M-1)!} \cdot U^{M-1} \cdot (1-U)^{N-M}$$

Since N.(N-1)! equals N! and 1/(M-1)! can be written as M/M! , we can rewrite the above equation as:

$$r_{sp}(M\text{-f-}N) = \frac{N!}{(N-M)!\ M!} \cdot Mz \cdot (zt_u)^{M-1} \cdot (1-zt_u)^{N-M} \qquad \text{with } zt_u = U$$

In working out results for a particular M and N, powers of an order higher than M can be neglected if $zt_u \ll 1$. This yields the formula used in practice:

$$r_{sp}(M\text{-f-}N) \approx \frac{N!}{(N-M)!\ M!} \cdot Mz \cdot (zt_u)^{M-1}$$

Note: An expression for functional failure rates can be found in the same manner. Results are given in Appendix 4. However, they are of limited interest since they do not determine the hazard rate directly. For those who want to know, dividing the unavailability by the functional failure rate yields the system-MFT.

APPENDIX 3 : Staggered testing of M-from-N systems

The testing interval is divided into equal parts T/N. The N channels are tested consecutively, with a time-difference of T/N. The interval for each individual channel then remains T. For functional system failure, at least N-M+1 channels have to be in a failed state. With simultaneous testing, the maximum possible time of failure coexistence equals T. With staggered testing, such a maximum will occur when N-M+1 are distributed over consecutive channels (i.e. consecutive in the order of testing), since such a situation will show the smallest possible time-shift between the test preceding the incidence of the first failure and the test following the incidence of the last one. This minimum time-shift equals N-M parts of T/n, i.e. one less than the number of failed channels. The time left for coexistence then equals:

$$N.\frac{T}{N} - (N-M).\frac{T}{N} = \frac{M}{N} \cdot T$$

as against T in the case of simultaneous testing. There is a shortening effect, accounted for by a factor of M/N, as if the channels were tested simultaneously but at intervals of MT/N. If this had been the case, the MFT of each channel would have been

MT/2N, i.e. half the testing interval. Since the MFT of M-from-N systems is proportional to the MFT of the channels (2), one can conclude that staggered testing reduces the MFT of an M-from-N system by a factor of M/N.
Since one is interested in the influence on the unavailability of the system, i.e. the product of MFT and failure rate FR, it is necessary to investigate the possible influence of staggered testing on the FR. Now the assessment of the FR, according to the method of formulating a failed subsystem of N-M failed channels to be confronted with failure of yet another channel, boils down to:

FR(system) = U(subsystem) x FR(channel)

For the time of coexistence in the subsystem to be maximum, N-M failures have to be distributed over the same number of consecutive channels. The minimum time-shift then equals N-M-1 parts of T/N, leaving M+1 parts of T/N as the maximum time of coexistence. Therefore, the shortening effects on the unavailability of the subsystem amounts to a factor of (M+1)/N.
If N-M is large enough, the above subsystem can again be seen as a system with a subsystem, yielding yet another factor, this time equal to (M+2)/N. Now by a proces called complete induction, one finds a continued product:

$$\frac{\text{FR(staggered}}{\text{FR(simultaneous)}} = \prod_{k=1}^{N-M} \frac{M+k}{N}$$

Since we already found a factor of M/N for the MFT, the complete shortening effect of staggered testing is given by:

$$\frac{\text{U(staggered}}{\text{U(simultaneous)}} = \prod_{k=0}^{N-M} \frac{M+k}{N}$$

It should be noted that this expression is of rather academic interest, since for practical systems, with N-M = 1, the formula degenerates to M/N, and systems with a higher redundancy than 2-from-3 are unlikely to find practical application.

APPENDIX 4 : Unavailability and failure rates of M-from-N protective systems

For completeness, and because other authors produce similar tables, the following table gives the unavailability and the functional and spurious failure rates of a number of M-from-N systems. It should be remembered that r and z represent the functional and the spurious failure rate of a single channel respectively and that the parameter t_u represents the MFT of a single channel. All expressions are valid for $rt_u \ll 1$ and $zt_u \ll 1$ respectively. The error caused by simplification is small and on the safe side: complete expressions yield lower values than the simplified ones given. However, before application, the influence of the time needed for testing should be investigated, see eq. (16). Note that the coefficients increase with increasing complexity.
To obtain a hazard rate, the relevant expression for unavailability must be multiplied with the demand rate in question.

TABLE of simplified relations for M-from-N protective systems

System	Unavailability	Functional failure rate	Spurious failure rate
1-from-1 (single)	rt_u	r	z
1-from-2	$(rt_u)^2$	$2r^2t_u$	$2z$
1-from-N	$(rt_u)^N$	$Nr^Nt_u{}^{N-1}$	Nz
2-from-2	$2rt_u$	$2r$	$2z^2t_u$
2-from-3	$3(rt_u)^2$	$6r^2t_u$	$6z^2t_u$
2-from-4	$4(rt_u)^3$	$12r^3t_u{}^2$	$12z^2t_u$
3-from-4	$6(rt_u)^2$	$12r^2t_u$	$12z^3t_u{}^2$
3-from-5	$10(rt_u)^3$	$30r^3t_u{}^2$	$30z^3t_u{}^2$

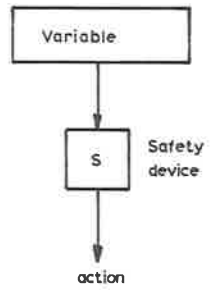


Fig.1 Single channel protective system

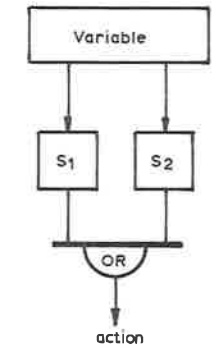


Fig.2 A 1-from-2 system
The system acts when one channel OR the other one, OR both are activated

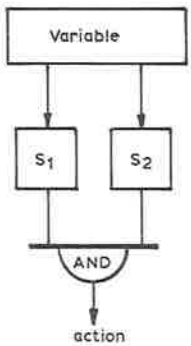


Fig.3 A2-from-2 system
Action only when both channels are activated.

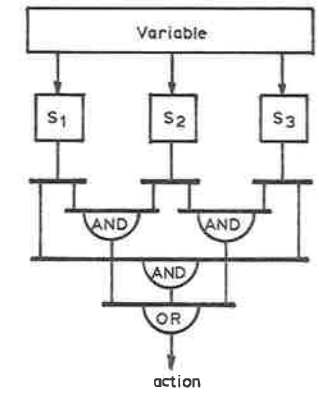


Fig.4 A 2-from-3 system

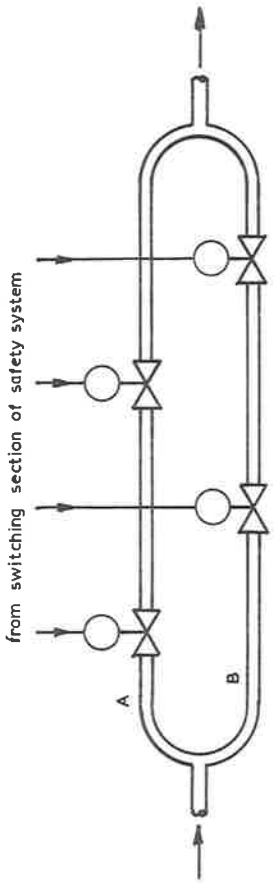


Fig.6 Shut-down system, allowing unrestricted testing.

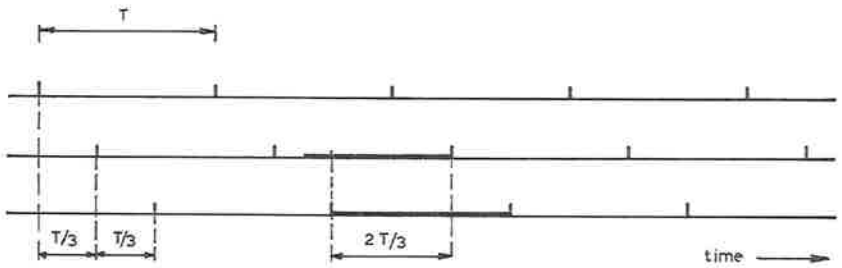


Fig.5 Staggered testing of a 2-from-3 system.
Worst case of failure incidence with maximum time of coexistence 2T/3

Risk Assessment & Risk Reduction in Industry

Mr. C.S. Windebank
The Insurance Technical Bureau
London
U.K.

Everything we do has a measure of hazard associated with it - crossing the road, visiting a sick friend, going out of doors in a storm; all human activity carries with it a chance of mishap - a chance of unplanned happenings working to our disadvantage. From the earliest age we learn to recognise these hazards, to assess them and to take appropriate action - i.e. to control them. The better at it we get - the longer we live.

I am not referring to adversity in a business venture - or even a bet - adversities which are so to speak wished on oneself. Here Dame Fortune smiles in one direction as she frowns in another. One man's losses become other people's gains. But superimposed on this is the hazard of loss to the individual (or corporation) which is at the same time a loss to the community as a whole. It works only in one direction. Engineers will recognise the general application of the laws of thermodynamics.

Industry as we know it today is a collection of human activities organised by a group of people we refer to generally as Management. It is management's job to do for the corporation what an individual does for himself and one of these jobs is to control the losses which can result from the hazards of the industrial operation.

These losses are of different kinds. Losses to life and limb; losses to property; losses to profits arising out of property losses; and losses to others resulting from the operation and reflecting liability onto the operator. These are not the only ones but they are as a rule the most important, and they can all be insured against. Loss of life, loss of profits and liability to others all relate in a very general way to loss of property. Most of what I have to say, therefore, will be with reference to property loss, but it can all be adapted to the other losses - more or less usefully.

Hazards stem from two basic sources - natural phenomena and human agency - or if you will, Acts of God and acts of man. If you take a broad look at industry losses you readily see that God doesn't act very often but when he does he acts on a grand scale. (Fig. 1) Acts of man are responsible for by far the greater number of losses. They may be divided into those due to present action and those imposed on us by action in the past. The misoperation of a valve would be present action whereas the failure of a flange bolt would be a result of someones mispractice perhaps two years ago. Each group can be sub-divided further - into planned and unplanned action. Planned action which leads to loss can be benign or malicious, i.e. action which is intended for the good (the calculated risk) or action which is intended to do harm (sabotage). Unplanned events can arise because we might be working outside the boundaries of human knowledge or because insufficient care was taken by the personnel involved. The last category would of course include failure to find out what other people knew about the hazards of the operation.

It is impossible to generalise about the numerical distribution of basic cause, but a few useful observations can be made. Here in Europe, natural phenomena account for a very small proportion of total industrial loss and even world-wide it is not a very important consideration, reflecting the fact that engineering design takes local conditions into account - and copes fairly well. Deliberate human action i.e. sabotage and the "calculated risk" on the other hand, account for a majority of losses throughout U.K. industry, both in terms of number and size. Sabotage is not a major factor in the more hazardous sectors of the process industry such as petrochemicals. The calculated risk (which of course is seldom calculated) is probably a more frequent cause of loss in all

industries than is often supposed.

Elimination of loss is of course impossible - this is why we tend today to avoid the well-established expression of "loss prevention". We speak now of hazard control or loss reduction. I prefer the term hazard control because it implies that we should be able to restrict the hazard within acceptable limits - which implies in turn that we must be able to measure it and determine the effect on it of loss reduction activities. It also implies that once we understand the nature of a hazard, control is merely a matter of expenditure.

How much should we spend? If we spend nothing we may lose the plant and be out of business. If we spend all our profits we may just as well be out of business anyway. Somewhere in between there must be an optimum. An optimum that depends on the cost of hazard reduction, the value of the benefits it brings, and the value of the benefits which would accrue if we spend the money for other useful purposes.

This is the sort of calculation that Industry Management is used to handling every day. Cost-benefit analysis and optimisation of return on investment are common activities with a growing number of sophisticated techniques to help in decision making. These same techniques can be used to help decide how to spend money on loss reduction. But to use them we need more precise quantification of cost and benefit than is at present possible.

Active protection measures are those designed to combat a hazardous event should it take place - the provision of alarms and fire fighting equipment for instance. Their cost both in terms of capital and operating expense is pretty well defined.

Passive protection measures are those built into the system to forestall the occurence of a hazardous event or to reduce its impact. A design modification which limits the amount of flammable liquid in process at any one time would be an example. A wide access road which separates process units and acts as a fire break would be another. The costing of such measures is usually difficult because they serve more than one purpose and invariably influence production economics.

Benefits are more difficult to express in precise financial terms than costs. Losses are sporadic in timing and variable in size. The benefits which result from loss reduction measures show eventually in a reduction of frequency and size of loss, but chance may distort the pattern of loss for some time both before and after the action. To make things more difficult still, losses in a particular industry or type of plant may be so infrequent as to make statistical comparisons of very low significance or even meaningless. In these awkward circumstances the decision-maker has to judge what the losses may be if he makes his investment, and set these against what they may be if he does not. The desirability of being able to assign values to these hypothetical losses is obvious.

The classical approach to hazard assessment has been the study of the loss history of the unit or "population" of units in question. The rate at which losses have been incurred in the past can be extrapolated into the future with due allowance being given to recognisable changes in and outside the system. However, technological change is so rapid today that extrapolation is no longer as reliable as it was. It was recognition of this fact that led U.K. insurers to set up the organisation I represent - The Insurance Technical Bureau. A few words about this organisation may be of interest.

U.K. insurers - like those of many other countries - have a long history of effort in the field of loss reduction and have taken many steps to encourage a technological approach to the subject. The early fire brigades were their creation and indeed they still subscribe towards the costs of the current brigades. They finance the operations of the Salvage Corps who complement fire brigade work in reducing losses from fire,

explosion and flood. They have originated and sponsor a number of organisations in the research and promotional fields in the longer term interest of loss control - the Fire Research Station and the Fire Protection Association for instance.

The Insurance Technical Bureau has a somewhat different mandate from any of these. It was set up about four years ago specifically to study and advise on the impact which changing technology might have on underwriting matters. It provides a technical interface between insurance and industry, but has no concern with individual insurance contracts. It is not a partisan organisation; its reports are general in nature and are made available to anyone who wants them.

It is what some would describe as a "public service organisation". It has in fact a lot in common with the T.B.B.S. here in the Netherlands, which has existed a good deal longer.

Its field of interest is potentially as broad as the field of insurance itself, but for the moment it is limiting its work to consideration of fire and explosion and toxic emissions.

A feature of the Insurance Technical Bureau is that its staff are drawn almost entirely from industry - and look at loss control from the industry viewpoint. They are concerned with the industrial process and with engineering and management, and are looking all the time for ways in which these can be moulded to control hazard and reduce loss - whether to life, property or profits.

As examples of their work I can quote a number of studies of the hazards of individual industries - industries which have particular characteristics from a potential loss viewpoint - e.g. very high value at risk (Aerospace and Electronics industries for instance) or a poor loss record (Paper industry for instance) or an impending big change in processing technology (Rubber industry for instance). They have pioneered a system of recommissioning electronic equipment which may have been damaged by fire - with a potential saving to the U.K. economy alone of many millions of £ sterling per year. They have looked closely at the hazards of particular aspects of petrochemical production and have made a deep study of the percussive vapour cloud explosion.

Such work as this provides a background to a continuing consultancy service available to all. It all involves hazard assessment which conventionally rests on the consideration of the historic loss picture. This has provided the basis for insurance operations throughout history. It has served very well where large numbers are concerned and the criterion of loss is clear-cut. Life insurance is the best example - the numbers to draw on are immense and the criterion of loss is a sure one. With the growing number of motor vehicles on the road, motor vehicle insurance is able to adopt similar actuarial techniques.

On the other hand, material losses in industry - although very heavy in money terms, are so diverse as to have made the application of actuarial techniques impractical up to the present. Losses are random and variable and often quite infrequent in an homogeneous population - such as for example a particular industry in a particular country. Fig. II shows the losses over the past several years of the U.K. Pharmaceutical industry. It is no use increasing the numbers by going back too far in history because of the changes, technological, corporate and social, which underly the experience and affect it. Nevertheless, for want of anything better, insurers speak of the "loss rate" over a limited period - say 5 years. This is the sum of losses over the period in an individual plant, or group of plants, averaged out per year and expressed as a fraction of the value at risk.

$$\text{Loss rate} = \frac{\text{Sum of losses}}{\text{number of years x value at risk}}$$

An equivalent function for industrial life statistics is called the fatal accident frequen-

cy rate.

Loss rate for a given population varies with time, according to the ebb and flow of the loss experience. If these fluctuations are large and infrequent, loss rate can vary considerably.

To avoid the variability surrounding loss rate, the I. T. B. have made use of a theoretical concept which represents what the loss rate would be if the experience with the plant or population under study could be enlarged infinitely. This is an "idealised" loss rate and is termed the 'h' factor. It is a numerical representation of the true hazard of the population. Whereas loss rate applies to a particular population and to a particular period of time, the 'h' factor is a fundamental property of the population.

The more experience there is to draw on, the closer loss rate will approximate to the 'h' factor. So when the population is large (e.g. if we are considering the losses by fire in domestic premises) the loss rate is close enough to the 'h' factor to be used as such. If we are considering say the losses by fire and explosion in hydrocrackers over the past decade, although we have a few dozen cases well recorded, they are superimposed on a commercial and technical background which has changed very widely as the number of plants in operation has increased, and as the design has evolved with experience and the application of fresh minds. The true hazard - as represented by the 'h' factor should in consequence show a steady reduction. The loss rate with the small number of incidents to draw on would show wide fluctuations, and, influenced by the ageing of the original plants, might give just the opposite impression.

The atomic energy people have had to meet this problem in the extreme. With nuclear power plants we just cannot afford to accumulate loss experience, so the 'h' factor - or some equivalent - must be synthesised from component parts, on each of which adequate experience may exist. This has stimulated the whole technology of reliability engineering into a fairly precise scientific study. Immense data banks of the reliability - or looked at the other way - the failure rate of mechanical and electrical components have been accumulated and can be used to calculate the reliability of plant involving a mass of such components.

It is possible that one day we shall have similar data banks on non-nuclear industrial processing equipment and some thought has been given to this. But as yet they do not exist and there are the problems already mentioned such as rapidly changing technology. To try to synthesise the failure rate of processing plant - such as a distillation column - from the atomic energy data would be expensive beyond the point of justification in most people's estimation.

Also we would need to take account of direct human action which accounts for such a large proportion of industry losses. And we would still have to bridge the gap between failure of plant and size of loss - which can range from the negligible to the disastrous.

These and other problems have led the I. T. B. to explore other ways of establishing the 'h' factor, and the rest of this paper will refer in general terms to a "down to earth" approach which shows some promise. It relies upon the use of a common sense combination of physical properties and abstract concepts which are easy to understand but impossible to define precisely.

The hazard of an industrial operation may be regarded as built of successive components. In broad terms we have the "inherent" hazard of the process, leading to the "intrinsic" hazard of the plant and finally to the "resultant" hazard of the operation. The terms are arbitrarily chosen to distinguish one from another.

The Inherent Hazard of the process is associated with the materials involved and the physical conditions to which they are subjected. One or two useful efforts have been

made in the past to quantify this concept insofar as fire and explosion are concerned. The work of Gretener in Switzerland and of the Dow Chemical Company are examples. They usually rate the heat content of the materials as a basic factor and introduce modifications to allow for other properties. The Bureau has found it better to keep to more abstract concepts and divides inherent hazard into considerations of -

containment
ignition
spread
effect

Containment refers in its broadest sense to the keeping apart of reactive materials - usually a combustible material and air. Containment is poor in the process of paper making because the process itself allows for the distribution of finished paper and worse still the waste all over the factory. The containment component will therefore be high. In a refinery however, the process provides for complete containment of the petroleum fractions within vessels and pipe lines and a zero containment component is aimed for, although of course, never quite achieved. Obviously high pressure processes and processes involving a lot of movement of materials are the more prone to loss of containment than shall we say static storage at atmospheric pressure, and the containment factor must reflect this.

Ignition covers a more physical concept - depending on the physical properties of the materials involved and the conditions to which they are subjected. Many methods of determining ease of ignition exist. Records of industrial fires help in assessing this component.

Spread is a function of the availability of flammable materials and their rate of heat release (rather than their heat of combustion). It would be quite high for nuts and bolts stored in wooden boxes but very low for the same stock stored in steel trays.

Effect of fire or explosion is not always 100% in the affected areas. Remote contact with the smoke from a fire may make food unsaleable whereas a water cooled or concrete clad structure may take an hour of flame impingement without appreciable harm. The factor should reflect these differences as accurately as the methods of assessment permit.

A plant when built to operate the process can be considered to have an intrinsic hazard which depends on the inherent hazard of the process and the skill and care (or lack of skill and care) which the engineers and constructors have put into the design and erection. Factors which contribute to the engineering influence on hazard can be put into such categories as

layout
engineering design
electrical zoning
instrumentation

Each of these can be sub-divided further if the attention to detail is considered worthwhile.

Thirdly the intrinsic hazard of the plant as so constructed is modified for better or worse by the skill and care applied to its operation (i. e. by the management systems adopted) to yield the resultant hazard of the whole operation. The factors which we can identify as contributing to this influence may be grouped under -

Policy and Organisation
Awareness
Procedures

Protection
Personnel

and again each group can be sub-divided at will.

It is the resultant hazard which counts. Although we think in terms of damage to or loss of a plant - it is the hazard of the operation which determines the chances of these losses occuring.

This crude analysis provides at the least a check list of factors which need to be taken into account in assessing the hazards of an industrial operation. But if we can put numerical values to each of the factors and find a way of combining them we can aspire to the idea of creating a model of industrial hazard which can provide us with a numerical value for the 'h' factor itself.

This is not easy - as pointed out earlier, good information experience is hard to come by. But one of the advantages of factorising is that we can use the experience of a wider range of industry to get ideas on the value for a single component; for instance every firm has a paint shop, many companies have a computer room and a lot of companies use flammable solvents. The experience from many different plants and industries can be used to arrive at figures with, hopefully, some degree of statistical significance.

Also we need not rely completely on experience - or historic loss information. A knowledge of the technology, comparison of one system with another, a lot of common sense and a growing amount of fundamental scientific fact, can all be used to help deduce a value for each hazard component.

This approach is basically very simple - which is to the good. There is of course a great deal of subjective judgment involved, and room for differences in view between different people, - which is not so good. But the more the 'h' factor is broken down into separately rated component parts the less will be the effect of personal judgment on the overall value. Occasional "fixed points" such as unusually complete and valid loss history can help control the persistent optimist or the persistent pessimist - and avoid a bias creeping in.

If the engineering/construction, and management conform to "good average practice" - i.e. they have no impact, positive or negative, on the net hazard of the process, the factors for engineering and management become unity and the inherent hazard of the process then becomes the 'h' factor of the operation. Bad engineering and bad management can increase these factors above 1,0. increasing the resultant hazard correspondingly. Good engineering and good management can reduce them.

In this way step by step a model of the hazards of an operation can be assembled. By careful definition of the components themselves the arithmetic can and should be kept as simple as possible.

You will note that I have confined my analysis to factors of human origin. Natural causes can be treated similarly - and fed into the model at appropriate places. Indeed today we are accumulating a great deal of understanding of natural phenomena and they are becoming more predictable and their hazards more manageable as a consequence, much more so than for human beings. Weather observation - with the satellites playing an important part - means that hurricanes and typhoons do not arrive unannounced. Our growing understanding of plate tectonics means that we can develop some idea of the location and timing and intensity of earthquakes and volcanoes. Of course, this increasing knowledge helps the engineer to design to accommodate the exceptional stresses his plant may have to encounter, and if this is done well the engineering component will compensate very largely for the additions to process hazard which natural phenomena introduce.

Any individual or preferably a group should, over a period of time, be able to construct a model along the above lines and use it to advantage. It would be presumptuous at this early stage to try to produce a general model for all industrial loss, but it is not necessary to go this far for use to be made of the concept. Most management decisions concern differentials - for instance the marginal effect on losses of a modification to plant or procedure. Usually one finds that differences in hazard can be estimated much more precisely and with more general agreement, than the resultant hazard itself. Fig. III. examines a simple case of a paper warehouse in the U.K. for which management is considering expenditure on sprinklers. Using the approach described above for process hazard estimation, one can deduce an 'h' factor for sizeable warehouses of 0.19% for sprinklered premises and 0.77% for unsprinklered. A calculation of payback time is quite simple - about $2\frac{1}{2}$ years in this case.

Had we used the loss rate information for this calculation we might have got a false indication for a number of reasons, the most important of which is that the loss data for sprinklered premises are very heavily associated with newer premises whereas those for unsprinklered premises are almost entirely for older installations - so sprinklers apart we would not be comparing like with like. The greater influence of chance on the loss rate has already been mentioned.

Similarly, one can compare one process with another, one plant with another, and one operation with another where process and plant are virtually identical. This last exercise will convince most people that the biggest differences between the hazards of different operations are those introduced by operating management. A consideration of the number, variety and importance of the factors contributing to this, can lead to the conclusion that orders of magnitude can exist between the 'h' factors (and, therefore, the losses which are to be expected) of identical plants operated by different people.

Why should the operation component introduce so much more variation than the process or engineering factors? It is perhaps worth noting that in spite of the great deal of attention given to management studies over the last half century it is only during the past decade or so that mathematical approaches to management have been tried. Management is still far from being a rigorous scientific discipline with well-established codes of practice, standards and techniques. Unless or until management becomes a strict discipline, the process and engineering components to hazard will be much easier to define and control, even though we may be relying on rather abstract unscientific concepts to measure them.

CAUSES OF LOSS IN INDUSTRY

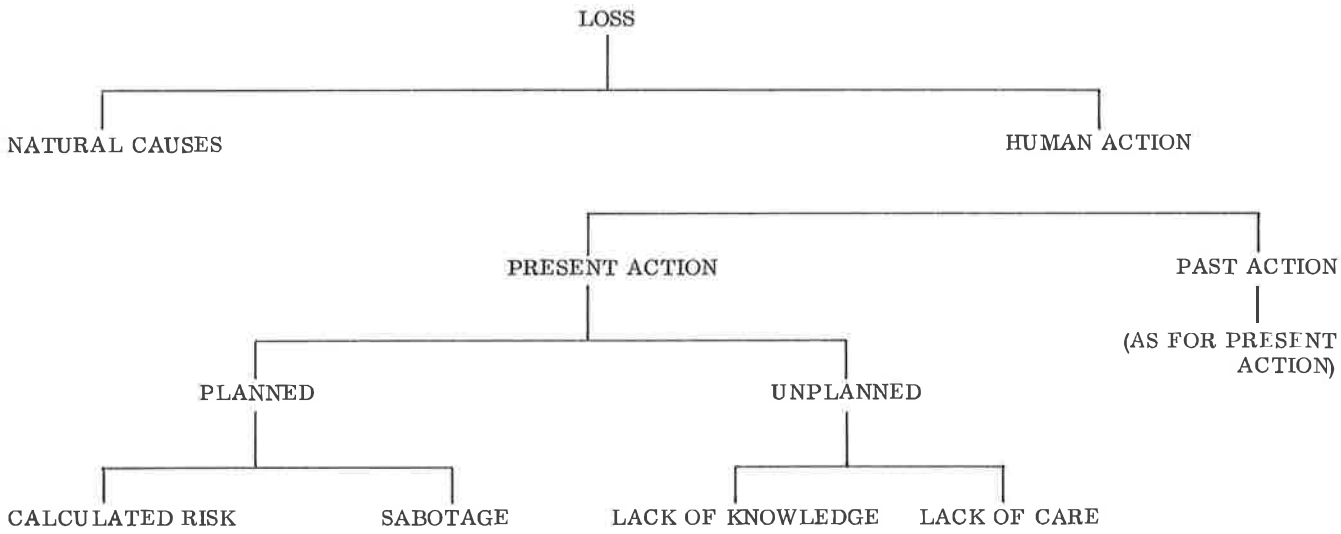


FIG. I

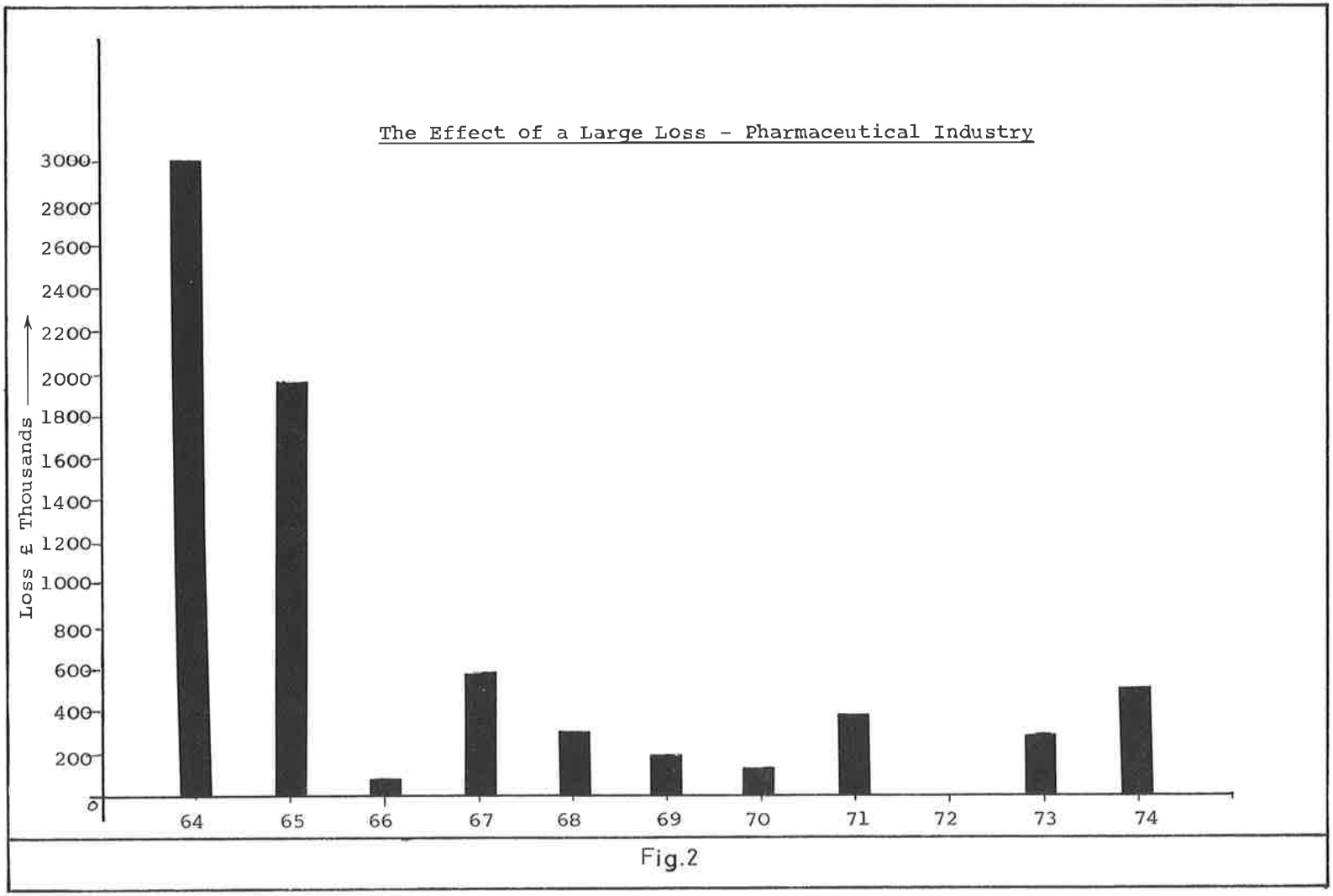

The Effect of a Large Loss - Pharmaceutical Industry
Loss £ Thousands
3000
2800
2600
2400
2200
2000
1800
1600
1400
1200
1000
800
600
400
200
0
64
65
66
67
68
69
70
71
72
73
74

Fig.2

WAREHOUSE FOR PAPER MILL

AREA		10 000 m^2
VALUE :	BUILDING	£ 1.15M.
	CONTENTS	£ 3.78M.
	TOTAL	£ 4.93M.

'h' FACTOR (UNSPRINKLERED) EQUIVALENT ANNUAL LOSS	0.77%	£ 38,000
'h' FACTOR (SPRINKLERED) EQUIVALENT ANNUAL LOSS	0.19%	£ 9,500
DIFFERENCE		£ 28,500
MAINTENANCE		£ 2,000
PAYOFF		£ 26,500
COST OF SPRINKLER INSTALLATION :		£ 65,000

FIG. III

The boy with his thumb in the dike

Ir. W. van der Kleij
Rijkswaterstaat
The Hague
The Netherlands

The boy with his thumb in the dike ..... that was Hans Brinkers, a little boy from Spaarndam near Haarlem. With his thumb he plugged up a small hole in the dike and so prevented a dike-burst and the inundation of his village. He even got a statue, which can be seen in Spaarndam. It is a remarkable story and it sounds so typically Dutch. Alas for modern romantics, it is wholly untypical of Dutch conditions. Dikes don't spring leaks like water mains and everything we know about dike-bursts indicates a quite different mechanism of failure. Our country has seen many dam-bursts, and most occured not because the dike had a small hole in it, but because it was too low. Dikes are constructed of earth - or nowadays ususally sand - and topped with a solid layer of clay as a facing. On the outer side it is strengthened with stones, or more up to date, with asphalt, to prevent the waves from damaging the earth core. The inner slope is strengthened by a good turf mat only. To such a dike nothing much can happen, unless it is too low. Then the waves may overtop it, or a whole layer of water may submerge it. Most dikes are not proof against that. The inner slope softens, lumps of earth start to slip down, and the dike becomes more and more eroded on the inner side until it crumples away and bursts, with the usual disastrous consequences. So much for Hans Brinkers.

Dikes in the Netherlands are in two main groups: sea-walls and dikes along rivers and canals. Sea-walls have to withstand high water-levels for short times only, but nearly always these levels are accompanied by heavy waves. On the contrary, river dikes should be able to withstand high water levels for long times, but here wave action is not so important. These different claims result in differences in design. Sea-walls are narrow but tall, as to prevent waves overtopping the dike. River dikes are lower but more heavily built, as they should not soften under high river-levels for long times. These differences in design can be seen clearly in the landscape. It should be pointed out, however, that for both categories of dikes, water level is the most important criterion.

Our forefathers knew that just as well as we do. They always made their dikes higher than the highest water-level they had experienced. Actually this was a rather bad method, as from time to time a water-level became higher than its predecessor with catastrophic results. Nowadays we think that we have better methods for the determination of the height of a dike, as modern mathematics has given us the possibility of ascertaining for every water-level the probability of this occurence. Accordingly the theme of my paper is: for which water-level do we design our dikes?
I realise that this is not 'risk-analysis' in the accepted sense of the word, it is more the determination of a planned load. All the same, it may be of interest for those who practise risk-analysis, for it is a good example of a "consciously accepted quantified risk". Living in a low-lying country is hazardous, but with modern techniques we can make the risk as small as we consider acceptable.
There are, of course, a number of other methods for the reduction of flood hazards. For example, we can simply go away and settle elsewhere. Or we can build artificial mounds and live on those. Our forefathers did this, and these dwelling mounds, called 'terps' in Dutch, are still to be found in the north of the country. Lastly we can evacuate the population in times of danger. There is nearly unanimous agreement that this is by far the worst solution. There are great organisational problems, and although these can be overcome, this is a distinct disadvantage. Furthermore, it means that the population in the low-lying parts of the country will have to live constantly with the idea that at any moment they can be ordered to leave their homes and belongings. It also means

that one has to rely heavily on wheather forecasts, and although these forecasts and gale warnings have become far more accurate in recent years, there is a clear possibility that the public will not accept that.
All these methods also have the disadvantage of conceding ground. That is the crux of the matter. The Netherlands have a particularly favourable location in Europe, and therefore are worth preserving. This is the reason why our forefathers did not leave the country, but enclosed it with dikes.
As I said, nowadays dikes are designed to withstand a water-level that has a certain probability of occurence. This means the acceptance of a 'conciously quantified risk', as still higher water-levels, which have a still lower probability than the accepted one, will cause a dike-burst. The techniques for calculating the probability of occurence of certain water-levels became available between the two World Wars. The famous physicist and mathematician Prof. Dr. H. A. Lorentz did the pioneering work, and as the calculating techniques were refined, the mathematicians began to suspect that at least some of the Dutch dikes might be too low to offer a reasonable degree of security.
Then the gale of 1953 caused a national disaster. Large areas of the country were flooded and nearly 2000 people drowned, and it became painfully clear that the mathematicians had been right. The government immediately installed a Committee, soon to be know as the Delta Committee, to draw up recommandations for the best way to safeguard the Netherlands against future floods. The Delta Committee wisely decided to use all available knowledge, including the results of the probabilistic investigations. Its final report appeared in 1958 and contained the recommendation to strengthen the Dutch coastal defences in such a way that a storm surge with a specific probability of occurence could be withstood. In its report, the Delta Committee stated: "Whatever storm-surge level is adopted as the basis for construction, it will always have to be borne in mind that absolute security is not guaranteed."
The government adopted the report and incorporated it in an Act: the Delta Act. From the point of view of risk-analysis, this was a rather important development:

a. For the first time, it was officially acknowledged that an absolute safeguard could not be provided. "Zero probability" cannot be reached.
b. Probability of inundation is regarded as a basic hazard of life in the Netherlands. In the event of a disaster the question of who is guilty can and should be left out of consideration.
c. All citizens are to be protected in the same way, there will be no arbitrary preferential treatment.

Since the passing of the Delta Act, the primary water defences of the Netherlands have been redesigned and reconstructed to withstand water levels which have specific probabilities of being exeeded. These probabilities are:

a. 10^{-4} per year for the 'Heart of Holland'. This is the mid-western region of the country where the large cities lie. It is one of the most densely populated parts of the world and therefore the risk has been put very low. (10^{-4} per year means that in any year the probability that a storm-surge occurs greater than the one for which the dike is designed, is as slight as 1 in 10,000).
b. For the other regions in the Netherlands a lower standard has been accepted: a probability of occurence of $2.5\ 10^{-4}$ per year.
c. For the dikes along the major rivers a still greater risk is deemed acceptable: $3.3\ 10^{-4}$ per year.

These standards involve a quantified risk, which can be lowered if we think that necessary, but can never be put at zero. In this respect the design of modern Dutch dikes is the first instance in the world of the adoption of a risk-analysis method.
The quantified risks that have been accepted in the Delta Act are such that nearly all Dutch dikes have to be redesigned, reconstructed and strengthened - a vast undertaking on which the Dutch are still engaged. Only in 1990 all dikes in the Netherlands will be up to the standards laid down in the Delta Act. The next questions is, of course, how such a quantified risk is determined. This is a very difficult question. In Holland, we are confronted with it again, now that a committee is considering whether the standard

for river dikes - $3.3\ 10^{-4}$ per year - is on the high side or not. For a number of examples have shown that strengthening of river dikes also results in a serious assault on the landscape.
One thing should be made absolutely clear: nothing is to be gained from a comparison with other risks. We know that the population runs many risks, on the road for instance. We also know roughly for a number of risks their probabilities of occurence. But we do not know to which extent these risks have been socially accepted. As Dr. Otway pointed out in his paper, social acceptance is not influenced only by the risk of occurence, but seems to depend on a number of determinants. At the moment we are rather ignorant about the whole process of social acceptance, so comparisons between risks are not very useful.
Another good reason for not comparing risks is a psychological one: an evil is so easily excused by pointing out another one!
But the main reason why every comparison comes to naught is that flood disasters simply cannot be compared with other calamities. They involve not only the loss of human lives, but also of possessions, land and cattle, and worse of all, they totally disrupt society.
So in the Netherlands floods are regarded and treated as catastrophes. In 1962 Tuindorp Oostzaan was suddenly inundated, by fresh water luckily. No human lives were lost, the dike that had been breached, was repaired easily and the water could be pumped away fairly quickly. Yet this simple flood was regarded as a national disaster. Sometimes, feelings are facts!
To determine admissible risks a large measure of common sense is of course needed. But nowadays common sense can be supplemented by modern techniques of analysis, such as cost-benefit analysis, risk analysis and policy analysis. With these techniques one can weigh the advantages of excluding a certain risk against the sacrifices the community has to make to that end. Of course, this is far easier said than done, as a number of factors have to be weighed against one another. Some can be measured, others however, are imponderables, and they pose the most difficulties.

Measurable factors are:
1. The cost of raising the dikes - this can be calculated rather easily.
2. The damage caused by the disaster. That is already far more difficult to calculate precisely. One might start with the 'maximum credible accident', by taking a specific region that has been inundated and then calculating the total value of all goods destroyed. These include houses, buildings, fittings and fixtures, cars, machines, plants and so on.
   Then there is the loss of production. Furthermore, inundations, especially those by salt water, also damage the soil, and for this an estimate has to be included in the total damage.

Calculations on the basis of the 'maximum credible accident' are extremely complex, but give a good indication of the total value of the goods that can be destroyed. They have been done for several regions in the Netherlands.
However, the method has its drawbacks too. In addition to their economic value, buildings or goods may have an historical or sentimental value, and that never can be equated to a sum of money. Secondly, the damages due to social disruption - disruption of traffic or the breakdown of electricity supply - are very difficult or even impossible to quantify.

Then there are the imponderable factors. I would like to mention only a few:
Loss of human life. Efforts have been made to calculate the value of human beings. This started centuries ago; Sir William Petty calculated the value of King Charles II's total estate in 1669, by arbitrarily adjudging to every inhabitant of Great Britain a value of £ 69.
In more recent times another Englishman tried to calculate the damages to society caused by traffic accidents. His approach was to calculate the mean value of the total expected production of a human being. In his scheme, new born boys were worth their

weight in gold, but girls far less. Pensioners had to be given a negative value. This, of course, is clear idiocy and we shall not dwell any longer on it. The value of human being fortunately cannot be expressed in terms of money.

Grief and social upheaval, the misery of not having a roof over one's head and of being made homeless. Also, there may be anxiety and a feeling of insecurity, even when nothing happens. That are psychological factors that, however, should never be neglected.

The concern for scenic values, which is a rather recent phenomenon. In the course of history, Dutch dikes have become part of the landscape. Dikes are the boundary between land and water and they often are one of the most beautiful elements in a rather flat landscape. In the past, they often were the safest places for settlement. Whole villages stretch alongside Dutch dikes, and some dikes are heavily built upon. Raising of river dikes spoils what has grown in centuries. Careful planning can limit the damage to scenic values, but it cannot prevented completely. It is not surprising that many in Holland protest against the raising of river dikes and query whether the safety gained is compensated by the scenic values lost.

This boils down to the accepted fact that it never is possible, even with modern techniques of analysis, to weigh all advantages of raising dikes against all sacrifices that have to be made. Yet, this has to be done if one wants to arrive at a standard for a quantified risk.

The Delta Committee tried to do exactly that. They invoked the assistance of the Mathematical Centre at Amsterdam and constructed a mathematical model, which left out all imponderable factors. Then, a method of calculation was developed that in its basic principles is still applied today. The model is based on the 'total discounted disaster damage expectation'. The idea is to calculate the compensation a hypothetical insurance company would have to pay for the damage a flood may cause.
This model results in a rather simple formula:

$$R = W.p.\ (1 + \frac{1}{d - g}).$$

R = the total amount of compensation that may have to be paid
W = the value of all damages and losses that will be claimed
p = the probability of a disaster (in the Heart of Holland 10^{-4} per year)
d = the discount rate
g = the growth rate of the economy.

This formula is not ideal, and we realise that. The chief culprits are the discount rate and the growth rate of the economy. How high should we put these rates? Some think that for the discount rate 4% would be reasonable, but others prefer a different value. The growth rate too, is rather troublesome. Some years ago 4 to 5 % seemed a good value, but today 2% would be nearer to reality. This would be not so bad if small changes in the growth rate and the discount rate did not have such marked effects on the outcome of the calculations. So nowadays we perform the calculations with a number of different values for those two rates.
As I mentioned earlier, the Delta Committee left all imponderable factors out of consideration. And yet it was found that the original choice of 10^{-4} for the Heart of Holland, which had been based partly on emotional considerations, was borne out by the calculations. The calculations showed that the proposed raising of the dikes paid for itself, certainly when - in an attempt to include the imponderables - the results of the calculations are doubled.
The Delta Committee's method has been used with satisfactory results for river dikes too. In consequence, we in the Netherlands have at the moment a considerable store of data about the costs of raising dikes and the value of goods present in the polders. Recently, there have been new developments. Today we would not tackle the problem

the way the Delta Committee did, we would use policy analysis instead - which, of course, was not available in 1953. Policy analysis was used for the first time when we had to decide upon the best solution for closing the Eastern Scheldt. We got important help from the Rand Corporation of Santa Monica, USA. The method can be defined as a "quantified survey of the long-term social advantages and disadvantages of alternative policy measures". Although this is quite a mouthful, policy analysis has proved to be a very valuable aid in deciding on complex problems.

In policy analysis you start with a number of alternatives for raising the height of a dike - for instance probabilities for the occurence of a disaster of 3.3×10^{-4}, 5×10^{-4} or 10^{-3}. Then you quantify all factors involved as far as possible, and preferably in money. Examples are the costs of constructing or raising the dike and the expected disaster damage, calculated according to the method I have just described.

Wherever possible, the imponderable factors are quantified, for instance in number of people protected, in hectares of countryside affected or in numbers of trees and houses lost.

Two courses are now open. The first is to use the 'weighing figure' method. A group of experts - they may be engineers, economists or ecologists - allots a certain figure to each factor. These are averaged, giving a certain score for each alternative. Usually however, the method does not work very well as experts are apt to disagree, something which causes a number of problems.

So usually the second course is adopted: the 'score-card' method. For every aspect, a score card is made which contains columns for the different variants. In the columns we can fill in numbers, or terms such as 'many' or 'few', or even colours - green for the highest, red for the lowest score and white for those in between. There may be score cards for such aspects as safety, the economy or nature preservation. We summarize on a total score card and there we can enter plus or minus signs in the columns.

Carrying out a policy analysis requires a tremendous amount of work, but it certainly is worth the trouble. Policy analysis is a great help in coming to a decision, but it is not more that that: the choice always remains difficult.

We used this method to come to a decision about the best way to close of the Eastern Scheldt and the committee now engaged in considering whether the standard for the river dikes should be changed, also uses this method.

One meets quite a number of other problems, mostly of a technical nature, when trying lay down standards. A major one is that, when calculating statistical frequencies of water levels, one has to extrapolate rather far. A storm with a frequency of 10^{-4} per year, fortunately has not occured up till now, but one has to extrapolate to that frequency, and in doing so one introduces a number of inaccuracies.

Then we have to reckon with the fact that small differences in water-levels give rise to large differences in statistical frequencies. For example, a water-level of five metres above N. A. P. (Amsterdam ordnance datum) at the Hook of Holland has a statistical frequency of 10^{-4} per year, but lowering the water-level to 4.80 metres above N. A. P. raises the frequency to $2\ 10^{-4}$, a doubling of the frequency for a difference of a mere 20 centimetres. And dike building is not a very precise construction technique, as differences in height of 10 centimetres are not unusual.

With river dikes one has similar problems.

Another thing is that we do not know exactly when a dike will give way. The ideal situation would occur if we could construct the dike in such a way that it will burst at a water-level somewhat higher than that it has been calculated to withstand. But that is impossible, because our present knowledge of soil mechanics is not good enough. So we assume that the dike will burst when more than 2% of the 'significant' waves go over its top. This is an empirical figure, and it is not very accurate. Modern dike probably can withstand more, but just how much more?

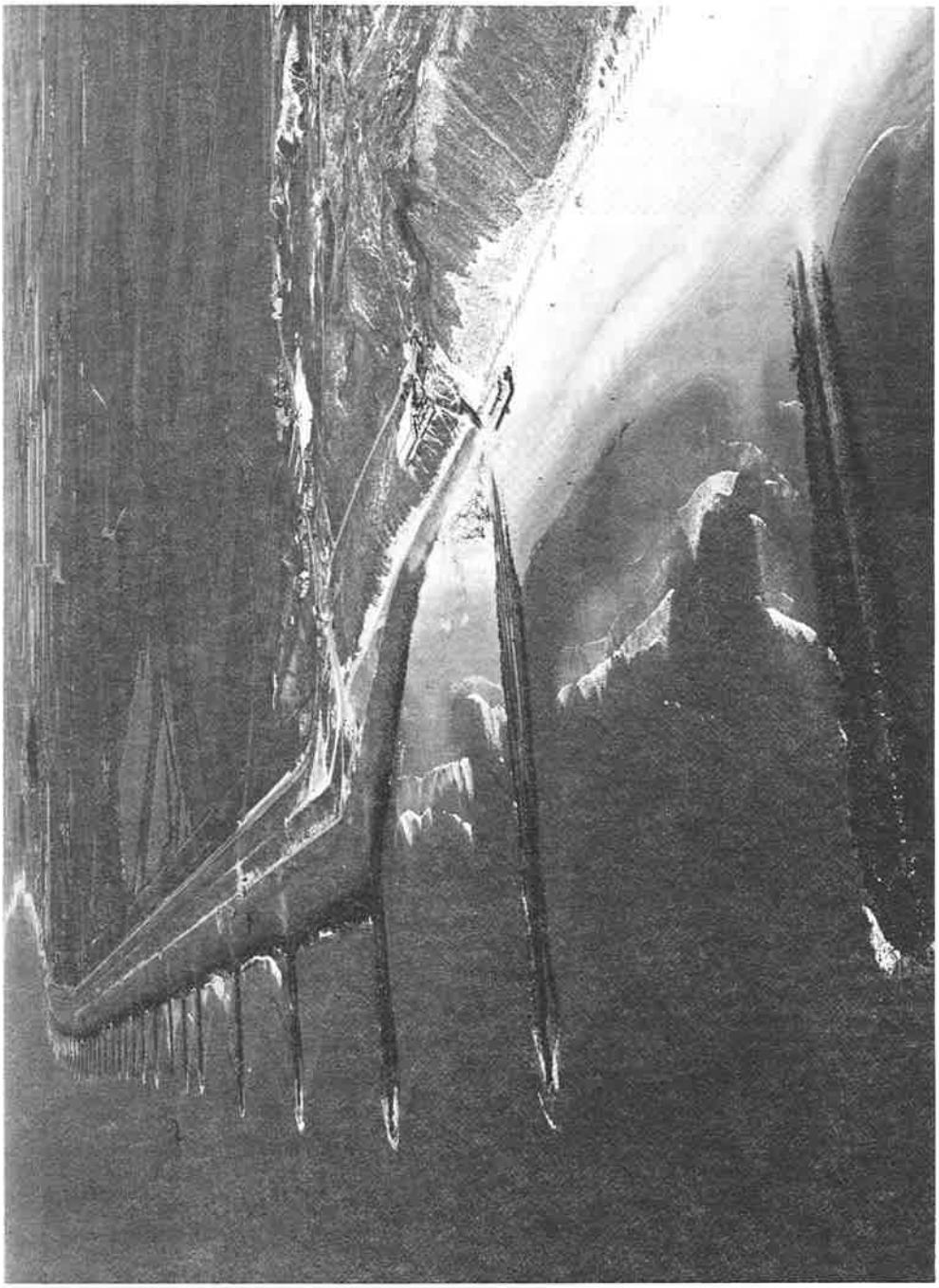
With river dikes, the problems are even more difficult. These dikes usually burst, either because they soften, or because water seeps through. The latter is called 'piping', and in such a case a small boy with a fat thumb might sometimes be able to help!

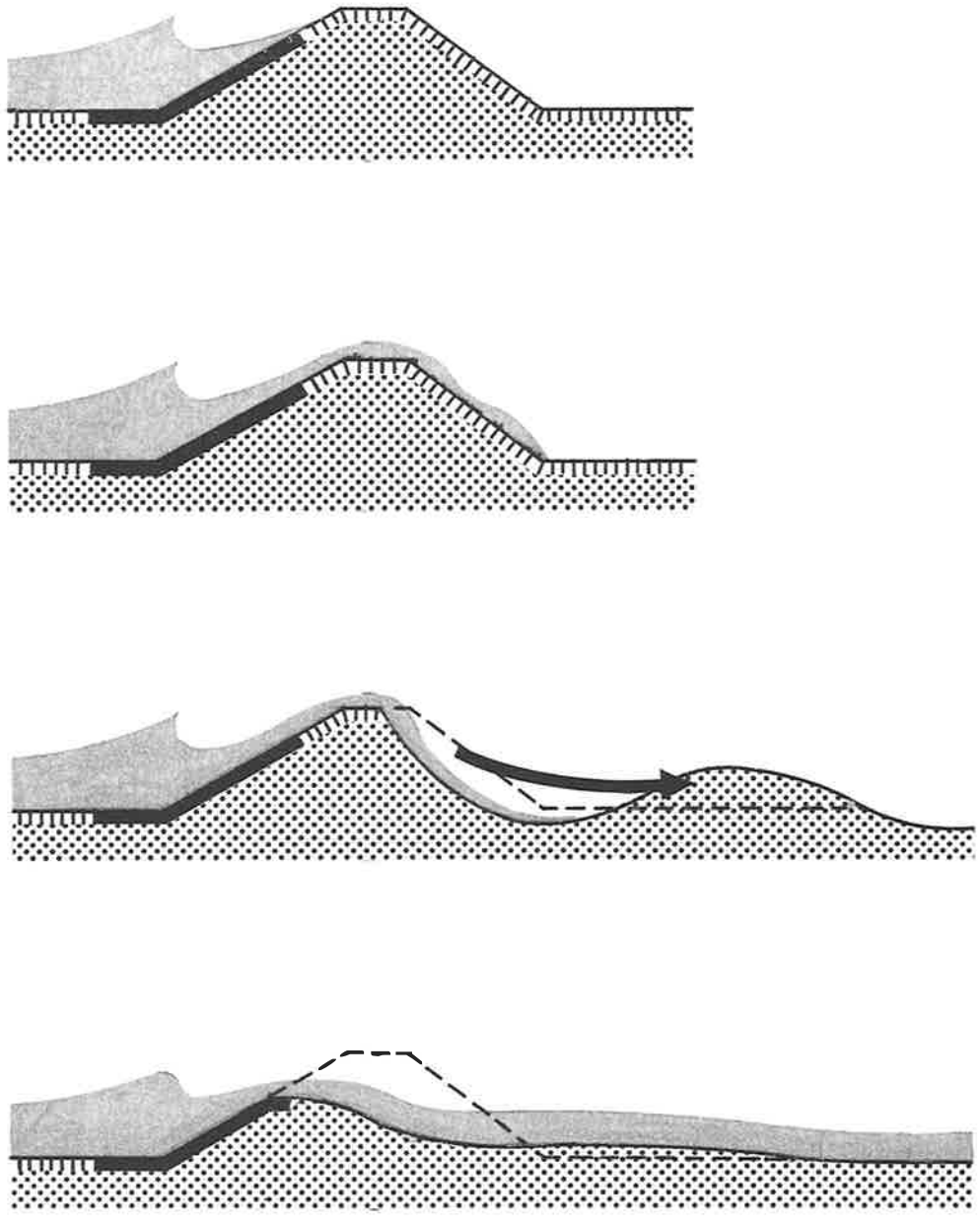
Then, we should not forget that dikes may burst owing to causes other than water: acts of war, a burst in a water main or a gas pipe, or a tree being uprooted in a storm.

These are all extra risks, and whenever possible we try to keep them at a level where their probability of occurence is at least lower than that on which the dike was calculated.
We still have much to learn, even about techniques. So we resort to a practical approach, the Dutch are rather good at that.
In summary I would like to stress five points:

1. Our aim is to safeguard our country by dikes that offer a high degree of security. Absolute protection, however, cannot be provided. There remains a conciously accepted quantified risk.
2. To determine the magnitude of that risk, we can use policy analyses - or, if you like, cost-benefit analyses or risk analyses. In these analyses the advantages of excluding a specific risk are weighed against the sacrifices the community is prepared to make.
3. The methods we employ are not perfect. There are many imponderables, and there are technical problems too. However, we arrive at good results.
4. The analyses are an aid in coming to a final decision. This final decision is a matter of policy.
5. Finally, it is of the utmost importance that the population fully accepts the choice made.

In final analysis, it is the habitability of our country which is at stake and which is worth preserving.





Application of Risk Analysis to Environmental Protection

Mr. W. D. Rowe, Ph. D.
United States Environmental Protection Agency
Washington
U. S. A.

Introduction

All activities of man as part of his narural environment involve risks. Many of these risks are undertaken voluntarily to achieve some beneficial return or are unavoidable. Coversely, some risks are imposed inequitable by one part of society on others. When these latter imposed risks involve health and the environment, regulation to ameliorate these inequities is required in most societies.
Amelioration of inequitably imposed risks does not imply no risk, but rather an acceptable level of risk which certain parts of society accept for the benefit of society as a whole. In order to address this problem, a basic understanding of the process of how societal risks are imposed and may be controlled is desirable.
This process of risk assessment is a relatively new discipline of developing importance as society becomes more cognizant of risk inequitably imposed upon them by technological activities of man. The term risk assessment is used to describe the total process of risk analysis and amelioration of risks. The process may be divided into two parts: (1) the determination of levels of risks, and (2) the social evaluation of risks. Risk determination consists of risk (hazard) identification and risk estimation. This latter area is the most familiar area since it involves the classical methods for determining the levels of risk as well as newer techniques for modeling risk. Risk evaluation involves acceptance of risk aversion as alternatives to imposed risks. Risk acceptance involves determinations of acceptable levels of societal risk while risk aversion involves steps to avoid risks.
The relationship of these aspects of risk assessment is shown diagrammatically in Figure 1.
Hazard identification is particularly of interest at this time since technology has progressed to the level that many new risks are either irreversible or are of global proportions. Hazard identification is open-ended, but up to now little attention has been given to identifying even major types of risk prior to their imposition.

Risk Identification

Assuming that we can define a "hazard"* in the general context of "a potential threat to man, his environment, and his well-being," the manner in which new hazards are perceived and identified is a major consideration in coping with them. Estimation of the changes in levels of man-originated and naturally-occurring hazards over time involves both the measured changes in levels of risk and the manner in which the perception of new risks takes place. The first area involves screening and monitoring to identify new risks, while the latter one is a social and cultural response of an aware population, and they are not mutually independent.

New risks are identified by at least three different processes:
1. The risk is new and did not previously exist.
2. The magnitude of an existing risk has changed.
3. The magnitude of the perception of an existing risk has changed.

Of course, all three processes may occur simultaneously.

---

* "Hazard" and "risk" may be used interchangeably with this definition. Alternatively, the "hazard" may imply the existence of a threat; and "risk is the potential occurrence of the threat.

A new risk is defined as one that did not previously exist. It is almost always a risk originated by man (as opposed to the new identification of an existing risk), usually as a result of a new technology, often where nature has no natural defense mechanism. Schumacher says it concisely:

> Our scientists and technologists have learned to compound substances unknown to nature. Against many of them, nature is virtually defenceless. There are no natural agents to attack and break them down. It is as if aborigines were suddenly attacked with machine-gun fire; their bows and arrows are of no avail. These substances, unknown to nature, owe their almost magical effectiveness precisely to nature's defencelessness.*

The second process involves existing risks which are newly perceived. These may occur because the hazard was previously unidentified, a sudden change in magnitude of the hazards occurs, or a slow change in hazard magnitude crosses some threshold of concern. Schumacher continues in this vein:

> . . . and that accounts also for their dangerous ecological impact. It is only in the last twenty years or so that they have made their appearance in bulk. Because they have no natural enemies, they tend to accumulate, and the long-term consequences of this accumulation are in many cases known to be extremely dangerous, and in other cases totally unpredictable.*

The third process involves the changing perception of society towards existing risks that may or may not be changing in an objective sense. This may occur when a more dominant risk is eliminated or reduced (e.g., the reduction of contagious diseases has made chronic ones of greater concern), or when there is a transfer of concern from one part of society to another through mass media and other communication modes, or when the hazards become a threat to particular individuals or groups, as opposed to statistical risks to the population at large.

In the latter case the process may be considered as a possible threat to the "status quo" of those who feel satisfied with their status quo.** However, the threat or perceived threat is to a hierarchy of possible types of risk.

Based upon the manner in which risks are identified and the types of risks involved, a morphological approach to screening for hazards can be constructed. Such a morphological structure is shown in Figure 2. The vertical column uses the processes involved in perceiving new risks as entires, whereas the horizontal row across the top uses an array of different types of risks. These latter include risks to: health and life, resulting in pain, disability, and premature death; the environment on a local or global basis, resulting in both reversible and irreversible effects; the economic well-being of groups and individuals; the social well-being of groups; and changes in the status quo of individuals. A third dimension might well be the types of systems that cause risks, such as:

> Chemicals - including drugs and pesticides
> Energy - including fossil and nuclear fuels
> Transportation - hazards to people and environment
> Construction - including fire and earthquake hazards
> Waste products - organic and inorganic
> Materials - ferrous, non-ferrous, plastics, etc.
> Etc.

The idea of the morphology is that each intersection can be studied on its own to determine if significant risks exist in that area. The necessity to examine each intersection analytically provides some possibility that areas not previously covered are brought into focus. The degree of detail in each scale and the level of aggregation are important factors in determining the scope of coverage and the practicality of the screening process.

---

* E.F. Schumacher. Small is Beautiful. New York: Harper Colophon, 1975, p. 17.

** See W.D. Rowe, "An Anatomy of Risk," Chapter 11, for a more detailed discussion of this idea.

Most of the effort in risk identification in the United States is presently focused on two major areas: (1) screening chemicals for toxicity and carcinogenesis, and (2) identifying technological threats to geochemical systems. In the first area the newly enacted Toxic Substances Control Act authorizes the Environmental Protection Agency (EPA) to obtain from industry data on the production, use, health effects, and other matters concerning chemical substances and mixtures. If warranted, EPA may regulate the manufacture, processing, distribution in commerce, use, and disposal of a chemical substance or mixture. Pesticides, tobacco, nuclear material, firearms and ammunition, food, food additives, drugs, and cosmetics are exempted from the Act. These products are currently regulated under other laws.

Testing of Chemicals

EPA may require manufacturers or processors of potentially harmful chemicals to conduct tests on chemicals. Testing may be directed to evaluating the characteristics of a chemical, such as persistence or acute toxicity, or to clarifying its health and environmental effects, including carcinogenic, mutagenic, behavioral, and synergistic effects. Before requiring testing, EPA must set forth the need for such testing in terms of expectation of unreasonable risk.

Premarket Notification

Manufacturers of new chemical substances must give EPA 90 days notice before the manufacture of the chemicals. Any chemical which is not listed on an inventory of existing chemicals to be published by EPA by November 1977 will be considered "new" for purposes of the premarket notice requirement.

Regulation of Hazardous Chemical Substances and Mixtures

EPA may prohibit or limit the manufacturing, processing, distribution in commerce, use, or disposal of a chemical substance or mixture if it finds that these activities or any combination of them presents or will present an unreasonable risk of injury to health or the environment. Labelling may be required for a chemical or any article containing the chemical. A manufacturer may be required to make and keep records of the processes used in manufacturing a chemical and to conduct tests to assure compliance with any regulatory requirements. Further, EPA may require a manufacturer to give notice of any unreasonable risk of injury presented by his chemical to those who purchase or may be exposed to that substance. A manufacturer may also be required to replace or repurchase a substance which presents an unreasonable risk. Essentially this act is similar in many ways to the Federal Food and Drug Act, but is extended to all materials.
Studies of various kinds are underway to identify threats to geochemical systems such as fluorocarbon gases and high altitude jet travel affecting the ozone layer of the earth's atmosphere, thermal and carbon dioxide loading of the earth's climatology, and tracing the fate of toxic materials through the environment.

Risk Estimation

The process of risk estimation is basically a five step process, as shown in Figure 3. First, as shown in the upper left hand corner, there is a causative event or events which, when properly defined, can have a probability of event occurence associated with it. When such an event occurs, there are a number of possible outcomes which likewise can be defined and the probability of the resultant outcome(s) also determined to varying degree.
As such, the causative event and the outcome do not involve risk since exposure to people, the environment, or institutions has not yet been taken into account. Thus, the combination of causative events and outcomes by itself is limited to experiments, statistical design of experiments, and hypothesis testing. Experiments are carried out

and outcomes observed to determine the behavior between the causative events and the outcomes. If such experiments involve exposure to people or the environment, then there are risks involved in conducting the experiments as well as testing the hypothesis. The third step in Figure 3 extends in the area of risk through the exposure pathway. Various exposure pathways can be defined explicitly. The probability of the various exposure pathways and resultant exposures can also be determined. Each exposure results in an array of possible consequences which also can be explicitly defined and the probability of consequence occurrence determined, as shown in the fourth step. However, risk determination does not end with definition of the consequence, but must also consider the value of the consequence to those people affected.

It is the consequence value to those affected which determines, along with the probability of occurrence, behavior in response to risks. Thus, the process of risk determination involves two basic steps: (1) a probability determination, and (2) consequence value determination which covers the areas as shown by the brackets at the right hand side of thw Figure. There is an overlap at Step 4, Consequences.

The probability of a consequence is a function of the probabilities of the causative event, the outcome, and the exposure pathway. This is shown in the lower left hand corner in equation 1. The value of the consequence is a function of the definition of the consequence and the probability of consequence occurrence as shown in equation 2. Risk then is a function of the probability of the consequence and the value of the consequence to the risk taker. However, the concept of risk is more complicated than the use of "expected risk" found by multiplying the risk consequence value by the probability of occurrence. The degree of knowledge of each of these parameters must be properly understood.

The probability of an occurrence of an event may be determined by direct measurement of repeated trials. When the number of trials is large, we can refer to the estimate of probability as being objective since it represents an empirical estimation. At the other extreme, if we only have estimates made from one or a few trials or totally by conjecture, the probability estimate is subjective. These definitions follow the classical ones of objective and subjective probability. In the subjective case Baysnian approaches to conditional probability and use of a priori information are useful. In between these two extremes, there is another area which I have called synthesized probability. In this case the probability of an event is not directly measured, but it is modelled and estimated from similar objective probabilistic systems which are expected to act in a corresponding manner. For example, the Rasmussen Study* on reactor safety is an estimate of synthesized probabilities where the estimates are not actually measured, but are computed from tests on parts of the system and synthesized into a total model.

A consequence which is directly observable and measurable and the value of that consequence expressed explicitly is an objective consequence value. For example, the accounting value of the payoffs of a gambling establishment as far as the house is concerned is an example of objective consequence value. The other extreme is subjective consequences where the value of a consequence to a particular risk agent is completely dependent upon the risk agent's value system and situation. In between these two extremes, there is a level which I call "observable" consequence value. Here the measured, behavioral response of groups in society to objective or subjective consequences can be ascertained through study of their behavior.

A matrix of the nature of probability and the nature of consequence as discussed above is shown in Figure 4. The probability nature is shown in the left hand column and the consequence nature along the top. The combination of probability and consequence defines risk. For the objective probability-objective consequence case, as shown in the upper left hand box, we have the area of objective risk. This is the area where most classical studies of risk have taken place. They are the easiest to define and the easiest to work with. As we move towards synthesized probability or observable consequences, we have areas which are called "modelled" risk. Here the model is not directly observable, but the correspondence of the model to reality determines its useful-

---

* Reactor Safety Study-WASH 1400. Nuclear Regulatory Commission.

ness. The modelling may be developed through the probability estimate by the use of synthesized probability, it may be through the valuation because of the use of observable consequences, or it may be through both synthesized probability and observable consequences as shown in the central box. All other risk areas are shown as subjective, either because of subjective estimates or subjective valuation or a combination of both.

The classical area of science involving experiments and making empirical measurements deal primarily with objective risk. In the last few years, the idea of synthesized probabilities has developed extensively and in the behavioral sciences the treatment of observable consequences as opposed to objective ones have been of major importance. However, as we look towards decision makin in society, it is the subjective risk area which is the reality. People make their decisions on subjective risk estimates, not upon what is objective. In other words, the emotional aspects often are what drive people, not the objective scientific knowledge. As an example, the use of expected value reactors and the fuel cycle usually results in lower estimates for accidents. While this may or may not be true, such results are anti-intuitive in terms of present behavior.

If the subjective risk estimates are the reality, the only way to make them closer to the objective risk measures is to educate people to the objective risks or to make the subjective estimates and valuations more explicit and visible so people understand them better.

The difference between objective and subjective behavior is well known to psychologists. Considerable study has looked into the objective and subjective probabilities for reward and punishment as behavioral models. The objective probability for reward or punishment involves the actual value of reward or punishment. For example, the punishment for speeding on a certain portion of road may be loss of licence and a high value fine. But at a given time, if there are no enforcement officers on that highway, the objective probability of punishment is zero. However, speed is often governed on these roads by the subjective probability of punishment in that the absence of knowledge of the placement of law enforcement officers involves some expectation that there might be one to observe your speeding. So behavior is generally based upon the subjective assessment of reward and punishment.

The subjective nature of consequence valuation implies a considerable variability in such measures. There are a variety of factors which can affect assignment of value to a consequence. A list of these is shown in Figure 5.

The purpose of such classification of risk factors is to provide means of comparing different types of risks and risk behavior under different conditions. Studies of each of these factors can provide considerable insight into individual and societal behavior toward risk acceptance.

Risk Evaluation

Man is naturally risk aversive. However, he is willing to take risks to achieve specific benefits when such choice is under his direct control. However, when the risk is imposed by man or nature without direct benefit, risk aversive action dominates. The fact that society is more concerned with adverse consequences than benefits is obvious from consideration of the content of news media, a reflection of society's news preferences. Disaster and disagreeable news far outweigh the achievements and beneficial events.

The risk aversive nature of society, coupled with increasing awareness of new risks resulting from side effects of new technology, has focused increased attention upon technological risk in recent years. Such awareness and concern are probably irreversible since the knowledge base for technology assessment and risk identification is available to all aspects of society. Consideration of societal risk in all technological decisions is rapidly becoming accepted, and increased regulatory attention is focused on risk assessment. A methodological approach to assure reasonable perspective in assessing risk is necessary if the regulatory apparatus is to work in a visible way. Purely voluntary risks need not and probably should not be regulated by government.

This is the case where only direct gains and direct losses to a risk agent are involved.* Unfortunately, there are relatively few conditions for which voluntary risks occur. There is usually some indirect risk imposed upon others who neither directly nor indirectly share in the gains. For example, the act of suicide has a consequence not only to the individual involved, but to his survivors, his insurance company, his creditors, etc. Further, the benefit of the act to the individual involved, if it may be thought of as a benefit in the form of relieving oneself of problems of living, is situational and, in some cases, irrational. Both the State and the Church have laws, regulations, and moral codes which attempt to make this act as unattractive as possible. Thus, government is involved in regulating voluntary as well as involuntary risks to some extent. This occurs when indirect losses associated with a voluntary risk condition affect significant numbers of the population of identifiable recipients indirectly; regulatory action to ameliorate the risk inequity becomes necessary. Thus, the purpose of a risk assessment methodology is not to balance direct gains and losses, but to ameliorate inequities in balancing indirect gains and losses. Risk assessment is only used after a favorable balance of direct gains and direct losses has been made, and involves consideration of involuntary risks. Thus, a risk assessment methodology is neither a cost-benefit analysis nor a substitute for such analysis. Its purpose, recognizing that some levels of risk always exist, is to determine when imposed risks on segments of a society are low enough to be acceptable. There is little question that the balancing of indirect gains to society against imposed risks is a requirement in risk acceptance. Higher levels of risks may be acceptable under these conditions; and moreover, total societal equity is rarely achieved in practice.

The Formulation of Methodology for Risk Evaluation

Risk assessment involves both risk determination and risk evaluation. A methodology for risk evaluation assumes that risks have been previously quantified or may be quantified by other efforts as a prerequisite for risk evaluation.

A methodology for risk acceptance involves four distinct steps, as shown in Figure 6. The direct gain-loss analysis involves a comparison of direct gains against direct losses, and represents a classical cost-benefit analysis usually made by an individual or institution undertaking a project or program. The individual or institution receives the benefits and accepts costs, and makes an analysis that is primarily an economic one. Voluntary risks are taken to achieve specific results.

If the balance is negative, the motivation for going ahead with the project or program disappears. It will probably be dropped unless the balance is changed or new factors, such as subsidization, are introduced. A favorable balance will provide incentive for the program. Institutional barriers involving legal constraints, taxes and related incentives, and public opinion are factors which are not always quantifiable.

The responsibility for carrying out this analysis is that of the individual or institution, private or governmental, undertaking the project for direct gain. It is an open-ended analysis since additional direct costs from subsequent steps will affect the balance, and new factors must be accounted for as they occur. Such a process is dynamic; and the sponsor will continuously review his position through its completion, perhaps only for economic reasons.

The indirect societal gains of a proposed activity must be balanced against the indirect societal losses of the activity. Risks are one aspect of the societal losses. This balance is the type of overall cost-benefit analysis sought in environmental impact statements under the National Environmental Policy Act of 1969 and is a goal of technology assessment activities. These balances must be made on at least three different levels of impact: (1) local balance, (2) national balance, and (3) world balance, and often result in qualitative value judgments as opposed to numerical balances.

At the governmental level, a sponsoring agency is usually responsible for the prepara-

---

* The terms "gains" and "losses" are used in place of "benefits" and "costs" since the latter two terms mean different things to different people.

tion of such analyses and they become part of the public domain.

Cost-Effectiveness of Risk Reduction

Since society is generally risk aversive, it is necessary that for a given indirect gain (benefit) the risk in obtaining it be minimized to the extent feasible, even for favorable indirect gainloss balances. The costs of risk reduction and in part direct costs must be factored back into the direct and indirect gain-loss analysis.
The key question in the risk aversion process is when is the risk reduction low enough. In considering the direct gain-loss analysis, the concept of "as low-as-practicable" limit consideration. One definition for obtaining an "as low-as-practicable" limit is when the incremental cost per risk averted is such that a very large expenditure must be made for a relatively small decrease in risk as compared to previous risk reduction steps. This implies a relative risk for the particular activity in question.
The "as low-as-practicable" concept limit is thus arbitrary as is that for risk acceptance. Some other reference is required to determine when cost-effectiveness of risk reduction has reached an acceptable level. The development of such a reference, based upon acceptable levels of inequitably imposed risk, is the basis for a methodology of risk evaluation. Up to this step, the three preceding steps are well-described by present practice.

Reconciling Identified Risk Inequities

When the overall indirect gain-loss analysis is made and is favorable, various inequities may still exist for specific value groups. Those who assume the risks may not always receive the benefits or the risk may not be evenly distributed among the benefit recipients. If this condition occurs, the risk must be identified and the nature and type of risk must be ascertained. One alternative approach is to compare these risks against the level of risk that society is experiencing for similar types of risks,* i. e., a set of societal risk references. This approach involves a societal value judgement of how much additional risk should society assume to obtain indirect benefits. Since risk references are static and generally historic, dynamic risk aversive behavior must also be considered in establishing the risk references. This involves the systemic degree of control that the new project includes to assure that risks will be properly controlled in the future.
Another approach involves risk balancing. The risks of the new program must be balanced against similar indirect benefits to derive a net risk. For example, the life extending aspects of radiation therapy may be balanced against the increased somatic risk of cancer induction by the therapy. The net risk which results from such balancing is risk to be evaluated, and may be negative (a probable gain). If all net risks of each type are negative or zero, there is no risk inequity; and a risk acceptance comparison is not necessary. Risks can only be balanced if measured on the same measurement scale. This is not possible very often and risk balancing is of limited application. It should be used when feasible.
Basically, a methodology prescribed for risk evaluation is a method for reconciliation of inequities based upon acceptable levels of risk in the form of risk references or other external criteria after the initial three steps are implemented. The process is illustrated graphically in Figure 7.

Conclusions

The determination and achievement of acceptable levels of risk inequity for each aspect of risk in a new technological undertaking is the key to resolving many of society's most perplexing problems. Safety aspects of nuclear energy and liquid natural gas

---

* Note activities causing risk are not compared. The risks of activities are compared with similar risks in society, independent of source.

transport, toxicity of chemicals and industrial by-products, threats to climatology, and the impact of release of uncontrollable genetically manipulated material are but a few of the kinds of problems that may be addressed in this manner.

The author has developed several "strawman" methodologies for determination of acceptable levels of inequitable risk. These methods are in the form of existence theorems. That is, the methods themselves may or may not be good methods, but as existing methods they show that it is possible to develop and apply them effectively. There is insufficient opportunity to illustrate these methods here and I must refer those who have further interest to my book "An Anatomy of Risk," which is to be published by John Wiley & Sons in July of 1977. It addresses in detail the whole area of risk assessment and application to decision processes.

FIGURE 1

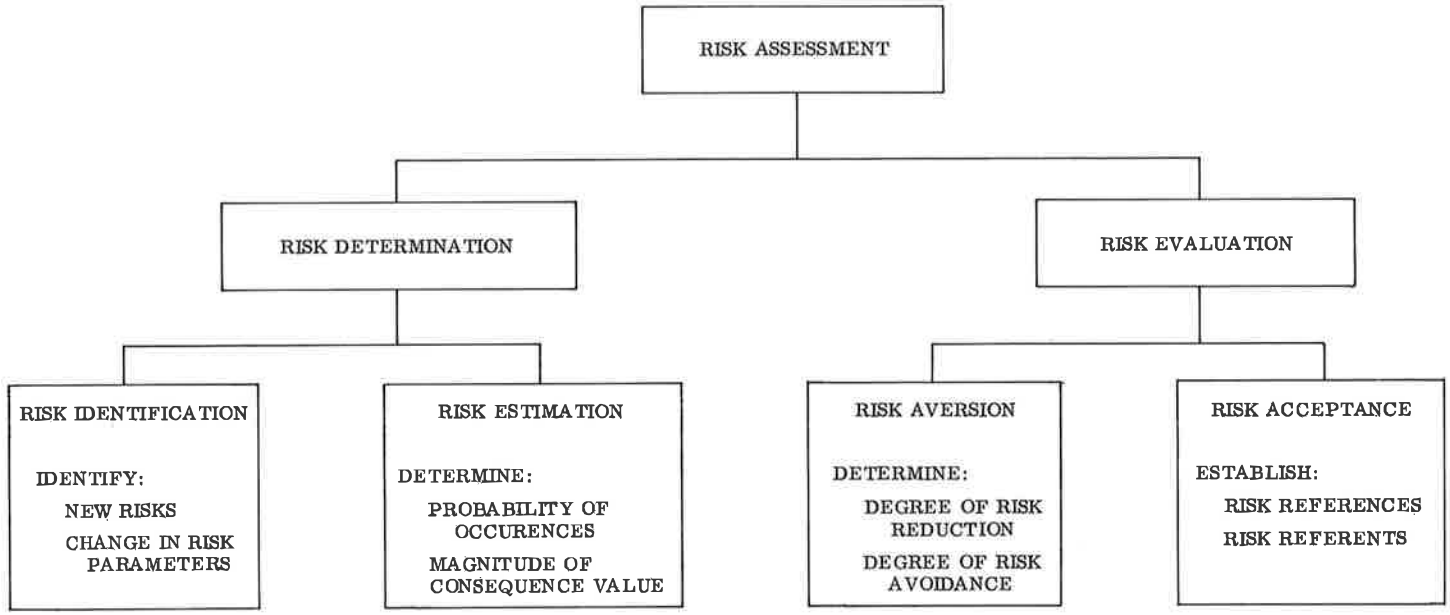

RISK ASSESSMENT
RISK DETERMINATION
RISK EVALUATION
RISK IDENTIFICATION
IDENTIFY:
NEW RISKS
CHANGE IN RISK PARAMETERS
RISK ESTIMATION
DETERMINE:
PROBABILITY OF OCCURENCES
MAGNITUDE OF CONSEQUENCE VALUE
RISK AVERSION
DETERMINE:
DEGREE OF RISK REDUCTION
DEGREE OF RISK AVOIDANCE
RISK ACCEPTANCE
ESTABLISH:
RISK REFERENCES
RISK REFERENTS

FIGURE 2

SCREENING MORPHOLOGY FOR HAZARD IDENTIFICATION

TYPE OF RISK / METHOD OF RISK PERCEPTION	Health and Premature Death				Environment				Economic Well-Being				Social Well-Being			Change In Status Quo		
					Scope		Effect		Group		Individual		Group			Individual		
	Acute	Chronic	Intergenerational	Genetic Pool	Local	Global	Reversible	Irreversible	Inequitable Distribution	Depression-Inflation	Loss of Income	Material vs. Other Goals	Loss of Prestige	Changes In Style of Living: Form	Changes In Style of Living: Magnitude	Degree of Satisfaction	Magnitude of Threat	Fight or Flee Response
1. NEW RISK a. Natural Defense b. No Natural Defense																		
2. EXISTING RISK-NEWLY IDENTIFIED a. Previously Unknown b. Sudden Change in objective magnitude c. Slow Change in Objective Magnitude Across Threshold of Concern																		
3. EXISTING RISK-CHANGE IN PERCEPTION OF RISK a. Dominant Risk Eliminated or Reduced b. Transfer of Concern from others c. Risk Agents Become Identifiable																		

FIGURE 3

PROCESS OF RISK ESTIMATION

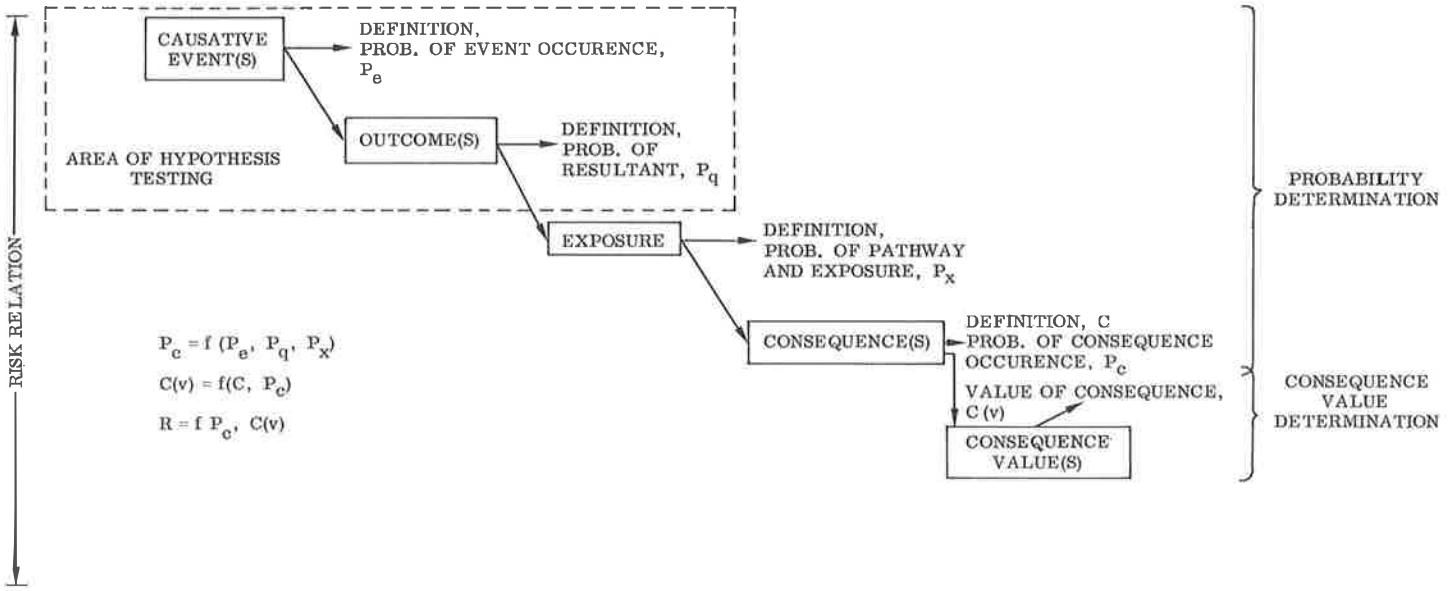


FIGURE 4

THE SUBJECTIVE AND OBJECTIVE NATURE OF RISKS FROM THE NATURE OF PROBABILITY AND CONSEQUENCES MEASURES

	CONSEQUENCE NATURE		
PROBABILITY NATURE	OBJECTIVE CONSEQUENCE — EVENT DESCRIPTION WHICH IS DIRECTLY OBSERVABLE AND MEASURABLE	OBSERVABLE CONSEQUENCE — MEASURED BEHAVIORAL RESPONSE OF GROUPS TO OBJECTIVE OR SUBJECTIVE CONSEQUENCES	SUBJECTIVE CONSEQUENCE — VALUE OF A CONSEQUENCE TO A PARTICULAR RISK AGENT
OBJECTIVE PROBABILITY- MEASURED BY REPEATED TRIALS	OBJECTIVE RISK	MODELLED* RISK (VALUATION)	SUBJECTIVE RISK (VALUATION)
SYNTHESIZED PROBABILITY- MODELLED FROM SIMILAR OBJECTIVE PROBABILISTIC SYSTEMS, BUT NOT MEASURED	MODELLED* RISK (ESTIMATE)	MODELLED RISK	SUBJECTIVE RISK
SUBJECTIVE PROBABILITY- ESTIMATED FROM FEW TRIALS OR THROUGH CONJECTURE	SUBJECTIVE RISK (ESTIMATE)	SUBJECTIVE RISK (ESTIMATE)	SUBJECTIVE RISK

* DEPENDING ON CORRESPONDENCE OF THE MODEL TO REALITY, THE MODELLED RISK IS CLOSER TO OR FURTHER FROM OBJECTIVE RISK, BUT NEVER REACHES OBJECTIVE RISK COMPLETELY.

FIGURE 5

FACTORS IN RISK VALUATION

1. FACTORS INVOLVING TYPES OF CONSEQUENCES
   - A. VOLUNTARY AND INVOLUNTARY RISKS
     - (1) EQUITY AND INEQUITY
     - (2) KNOWLEDGE
     - (3) AVOIDABILITY AND ALTERNATIVES
     - (4) IMPOSITION - EXOGENOUS AND ENDOGENOUS
   - B. DISCOUNTING IN TIME
   - C. SPECIAL DISTRIBUTION AND DISCOUNTING OF RISKS
   - D. CONTROLLABILITY OF RISK
     - (1) PERCEIVED DEGREE OF CONTROL
     - (2) SYSTEMIC CONTROL OF RISK
2. FACTORS INVOLVING THE MAGNITUDE OF PROBABILITY OF OCCURENCE OF A CONSEQUENCE
   - A. LOW PROBABILITY LEVELS AND THRESHOLDS
   - B. SPATIAL DISTRIBUTION OF RISKS AND HIGH PROBABILITY LEVELS
   - C. INDIVIDUAL RISK ACCEPTANCE AND PROPENSITY FOR RISK TAKING
3. FACTORS INVOLVING NATURE OF CONSEQUENCES
   - A. HIERARCHY OF NEED FULFILLMENT
   - B. COMMON VS CATASTROPHIC RISKS
   - C. SPECIAL SITUATIONS
     - (1) MILITARY VS PEACETIME
     - (2) LIFE-SAVING FUNCTIONS

FIGURE 6

STEPS IN ESTABLISHING AN ACCEPTABLE LEVEL OF SOCIETAL RISK

(1) Direct gain-loss analysis

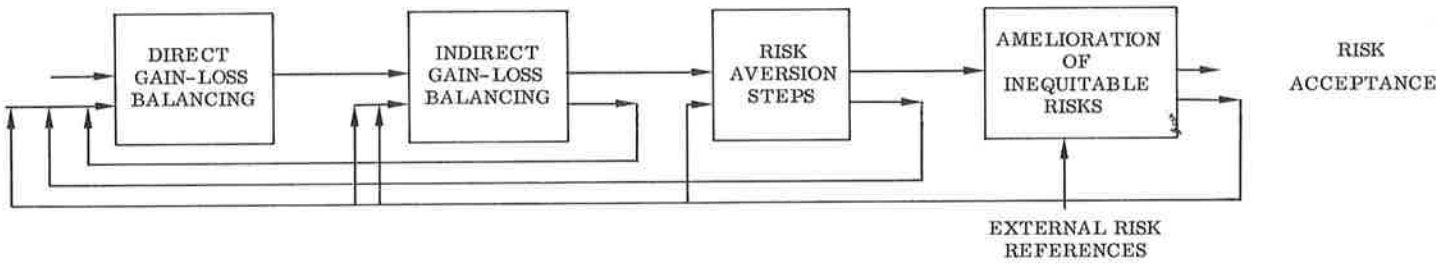
(2) Indirect gain-loss analysis

(3) Cost-effectiveness of risk-reduction

(4) Reconciliation of risk inequities

FIGURE 7

RISK EVALUATION PROCESS



Loss Prevention in the Process Industries

Mr. T.A. Kantyka
Imperial Chemical Industries Limited
London
U.K.

Introduction

Since the second world war the chemical and process industry has been expanding at a rate considerably higher than the rest of the industry. Many new products appeared on the market, new processes have been introduced and whole new industries have been created. The highly competitive nature of the industry has been responsible for a striking advance in technology, an increase in the size of plants and inventory and an increase in the complexity of the processes. This in turn contributed to the rise in the potential hazard of fire and explosion.

In parallel, although sometimes lagging behind these developments, the industry has taken steps to reduce and control hazards and to improve the general standard of safety. In fact, the safety record of the process industry compares favourable with other industries and the number of injuries and fatalities is small compared with those caused by accidents on the roads or at home. However, society, which has undoubtedly benefited from the technological progress in improved living standard, increasingly questions and challenges this progress and its consequences. A single disaster like Flixborough precipitates a disproportionate reaction, a reaction which is natural and genuine, but often based on ignorance. Chemical industry is regarded with suspicion and its image is heavily tarnished. Yet we must not dismiss lightly public opinion and concern. The First Report of the Major Hazard Committee of UK's Health and Safety Commission points out that this concern must bear heavily in assessment of what the highest acceptable risk should be.

The theme of this conference is risk analysis and my paper does not properly belong to the programme as it does not contribute directly to the subject. However, I feel it has a considerable bearing on it in that it shows how the overall level of risk could be reduced. In my paper I shall describe how the more enlightened and progressive companies in the process industry responded to the post-war developments and the consequent increase in potential hazard by evolving a new approach to safety.

Loss Prevention Concept

Historically, the responsibility for safety in chemical factories rested with specially appointed people, often called safety officers who were invariably a part of personnel function and who often acted as welfare officers. They were rarely sufficiently qualified to participate in technical discussions, or to understand the safety implications of complex processes and plants. If their advice was sought it was often as an afterthought when the plant design was completed. Equally, accidents were investigated and where possible corrective action was taken, but accident reports were treated as confidential documents to be filed in the archives.

During the last decade a much more positive approach to safety has slowly evolved. This is referred to as Loss Prevention and the emphasis is on prevention. Loss prevention extends over all the activities which are likely to affect safety and involves all the people in the working environment, payroll, staff and management and not only those specially appointed for this purpose. It implies that each individual has responsibility for safety in his sphere of activities.

Loss prevention philosophy can best be illustrated by considering a project for the

manufacture of some product which involves process development, design, construction, operation and maintenance.

Process Design

Hazardous processes are often protected by controls, trip systems and other protective devices to prevent the development of a dangerous condition, or to minimise its consequences, should it arise. If this is not possible, or if we are not entirely satisfied with the effectiveness of the protective measures employed, we encase the plant within blast walls. A more sensible approach would be to tackle the cause of the hazard and to design the hazard out of the process, or to reduce its magnitude by process modification.

The development of a chemical process in the laboratory offers the first and the best opportunity of reducing, or even eliminating hazard at its source. There are numerous practical examples which illustrate this. Reference 1 describes the development of a continuous process for the manufacture of nitroclycerine where safe operation of the highly dangerous process was ensured by the design of a special reactor operating at higher temperature and hence at a faster rate but containing only some 5 Kg of material compared with 200 Kg in previous designs and 1,000 Kg in the old batch process. Reference 2 shows how detailed examination of the formaldehyde process has eliminated the need for a complex safety control system and made the process intrinsically safe.

To develop an inherently safe process it is essential to have comprehensive process data. In particular it is necessary to:

a. identify all components and impurities

b. determine relevant physical and chemical properties

c. establish reaction mechanisms and determine kinetic and thermal data for all the reactions likely to occur

d. identify toxic, flammable and explosive hazards

e. explore the operating conditions well outside the normal operating range of concentration, temperature and pressure

The above information is a minimum requirement necessary not only for a design of a safe plan also for a design of a plant that works and performs efficiently.

An interesting case history is described in Ref. 3 of an explosion in a plant distilling crude chloromethylaniline which killed 3 operators and injured several others. A lengthy laboratory investigation was carried out after the accident to establish the cause of the accident an investigation that should have been carried out before full scale operation of the process was undertaken.

Plant Design

During the plant design stage equipment in which the process is to be carried out is specified and selected. This phase of the project offers another opportunity to reduce the risk of plant failure. The design engineers must be aware of the responsibility they carry for the plant safety. They must ensure that the design is sound and that measures are taken to deal adequately with any hazards which have been identified during the process development stage. Skilful design can often reduce hazard and eliminate the need for complex control and protective system. The design aspects which have an important bearing on the overall plant safety are as follows:

1. Reactor System Design

Reactors are a major source of hazard in a chemical plant, particularly when they carry out exothermic reactions, or contain large amounts of flammable material at elevated temperature and pressure. The design should provide for the removal of the maximum amount of heat which can be generated in the reactor under any operating conditions to which the reactor is likely to be exposed. In addition, the thermal stability of the reactor should be analysed over a wide range of conditions outside the normal operating level. In this connection, reactors operating under adiabatic conditions are inherently safer since a runaway reaction is less likely to occur. It must be emphasised again that a design of a safe reactor system can be undertaken only if comprehensive and accurate data are available on physical properties and kinetics.

2. Reliability of Equipment

The key to reducing hazards is the reliability of equipment.
Reliability of equipment affects plant availability and is directly related to plant safety and performance. Any failure of equipment however insignificant may lead to a serious accident. The most vulnerable items are moving parts eg. pumps, compressors, centrifuges, but equally important are valves, flanges etc. which can cause leaks and spills. The designer must take great care that he follows the recognised engineering standards and that he uses the right materials of construction.

Reliability engineering, which is a quantitative technique for assessing the probability of plant failure and which has been pioneered by the nuclear and aerospace industries is being increasingly applied in the chemical industry. The main limitation is the availability of data. Although data banks exist, they cover mainly electrical and electronic components. More extensive data particularly on larger equipment is necessary before this technique could be generally applied in the design of more reliable plants.

3. Plant Layout

It is necessary to provide space and access for firefighting and to subdivide the plant into sections so as to minimise the material loss and reduce risk of injury to personnel.

4. Inventory

The general principle to follow when handling toxic or flammable materials is to reduce the plant inventory to the minimum, particularly when the material is at elevated temperature or pressure, rather than rely on containment of the materials within the plant by good design, or by control systems such as emergency isolation. Containment should always be a feature of good design, but by minimising the quantity of hazardous material present in the plant the extent and the consequences of an accident are directly reduced.

In the earlier section on process design it has been shown how the safety of the reactor for the manufacture of nitroglycerine has been achieved by minimising the quantity of the reactants in the system. Generally, continuous reactors, especially tubular reactors have significantly lower volume and should be considered in preference to other types. Large inventories of boiling liquids are normally present in distillation columns and other methods of separation should be examined. Alternatively by a judicial choice of column internals and reboiler design the hold up of materials in the system could be reduced.

5. Control and Protective Systems

The high degree of reliability demanded from new, large and complex plants calls for sophisticated control and protective systems. In the past, plants have been equiped with alarms and trips. Many new plants operate closer to their safe limits and conventional controls are inadequate for safe operation. In such cases fully automatic controls should be installed to eliminate human invention. Duplication, or the use of elaborate multivoting control systems, whereby the chance of a plant closure by a spurious fault in a control circuit is minimised, may be necessary.

There are effective techniques available for the examination of plant in the design stage, or in operation, which are designed to help in identifying hazards and reducing risk of accidental failure. For instance, Hazard and Operability study is being successfully applied by many companies in the chemical industry.

Plant Protection

Careful attention to process and plant design will reduce the risk of fire and explosion but will not eliminate it completely. There will always remain a residual risk due to unexpected failure of equipment, or human failure. Most fires start as small fires and if they are undetected or not extinguished early enough, they can rapidly become major conflagrations. We cannot rely entirely on fire services, they are not available immediately and a delay of a few minutes may be crucial. As a result, there is a growing need for a comprehensive leak and fire detection system to monitor unattended areas and to trigger alarms. Similarly, the availability of effective fire protection and fire fighting systems, which can be brought into operation, either automatically or by operating personnel without delay is of immense importance in preventing, or minimising damage.

Human Aspect

Modern plants rely to a large extent on automatic control and operation but cannot entirely dispense with people to operate and maintain the plants. People are liable to make mistakes and this fact must be taken into account in the design of chemical plants. The reliability of plants is, therefore, the sum total of the reliability of hardware and personnel.

Records indicate that half of all the accidents occurring in industry are attributed to thoughtlessness, negligence, inadeqaute instructions, lack of motivation and involvement, insufficient training, unsatisfactory systems of working and communications, inadequate inspection, supervision and bad management.

Management

The attitude of management is of primary importance. Unless management is fully committed and motivated to safety and loss prevention it cannot exercise influence or expect the employees to respond. Apart from legal responsibility to safeguard the health and welfare of the employees and public, as well as reasonably practicable, the management has also responsibility to shareholders and customers. Any accident leading to interruption of process is an interruption in business with losses arising from higher cost of production, loss of sales and profits. For these reasons management must include loss prevention as an essential function of its business. Loss prevention must underline all management activities if it wishes to manage its business successfully and profitably.

Procedures and Systems

These include clearly laid out formal rules and routines for the control and mainte-

nance of plants. These should cover operating instructions for normal operation, shut-down and start up, clearance certificates, permits to plant modifications, control and access to installations. These must be strictly followed and management must ensure that through training, operators and maintenance personnel have sufficient knowledge and understanding of these procedures and of their importance in maintaining safety of plants. Particular attention should be given to unusual occurrences, disturbances and deviations from normal operating conditions, so that operators are in a position to take appropriate action. To prevent complacency, management should institute a system of inspections and safety audits to check the effectiveness of the safety systems and practices.

Hazard and Operability Studies

As already mentioned Hazard and Operability Study is a very useful technique which is increasingly applied in industry to ensure that hazards are minimised in all industrial activities. This is a comprehensive method of checking the safety of plant in a systematic manner. (Ref. 4). In many companies Hazard and Operability Study is applied to all new projects and all process and plant modifications. The following summary describes the pertinent studies carried out at the various project stages:

Project Stage	Details of Study
1. Feasibility evaluation	- Identify major hazards and inherent process risks (toxic, explosive)
2. Process design	- Systematic quantitative analysis of hazards and definition of measures to reduce them
3. Engineering design	- Formal examination of engineering diagrams with quantitative hazard analysis to ensure above measures have been implemented
4. Construction	- Systematic check that hardware (as constructed) and operating instructions are as intended in design
5. Operation	- Post start-up review of all departures from design affecting safety, operating difficulties, equipment failures with hazard implications Plant modifications and changes in operating procedures or conditions checked for effect on plant safety

Total Loss Control

It has been demonstrated that there is a direct relationship between major accidents, minor accidents and "near misses". The often-quoted relationship is 1:30:300. This means that it is not possible to eliminate major accidents without taking care of the minor ones. In the past, safety campaigns were concentrated on major accidents, which either killed people or damaged property. Little attention was paid to the "near misses" and yet a purge on these and other bad practices which are responsible for them would reduce the risk of major accidents. Some companies have adopted the concept of Total Loss Control and have demonstrated remarkable reduction in accident frequency by monitoring and investigating minor accidents and "near misses". The examination of "near misses" can often prove as valuable in improving safety as inquiries into accidents. In addition, Total Loss Control is also worthwhile in an economic sense by reducing material losses.

Summary

The principle of Loss Prevention in the process industry as outlined in the paper is applicable generally to other industries. There are two messages the paper aims to convey. Firstly, that safety can be achieved more effectively by the application of the concept of intrinsic safety, that is by designing hazards out of the plants, rather than by control protections. Secondly, that safety concerns everyone in the working environment and does not rest only with personnel specially appointed for this purpose. Every individual has a contribution to make to the overall safety of the enterprise and the role of good management is to foster this idea and to ensure that employees recognise and accept this responsibility. This should not be regarded as an additional burden but as a way of life.

REFERENCES

1. N. A. R. Bell, "Loss Prevention in the Manufacture of Nitroglycerine", I. Chem. E. Symposium Series No. 34, "Major Loss Prevention in the Process Industries", 1971, p. 50

2. R. G. Pickles, "Hazard Reduction in the Formaldehyde Process", I. Chem. E. Symposium Series No. 34, "Major Loss Prevention in the Process Industries", 1971, p. 57

3. T. Kotoyori et al., "Explosion During Distillation of 4-Chloro-2-Methylaniline", Journal of Hazardous Materials 1, 1975/76, p. 253

4. H. G. Lawley, "Operability Studies and Hazard Analysis", Chemical Engineering Progress, 1974, Vol. 70, No. 4, p. 45

Managerial Aspects of Risk Analysis - The Contribution of the Expert to Disasters

Mr. J.E. Bannister
Managing Director Keith Shipton Developments
London
U.K.

The management of risk is a topic of increasing interest to senior management and all of those concerned with the management of future uncertainty.

Modern systems show increasing vulnerability to risk, partly by reason of size and concentration, partly by changes in technology, resulting in more critical operating conditions, partly by changes in the social climate which business operates and partly by the reaction to increasing environmental impact.

In the last 20 years, important advances have been made in the assessment of risk, especially in hazard analysis and reliability studies to calculate the mechanical uncertainty in items of plant and equipment. In terms of the possibility of mechanical failure, most of the studies have been of value but we have continued to experience the occasional catastrophic failure or "near miss" in situations which cast doubt on the reliability of the over-all concept of risk assessment.

It has been pointed out that many of these failures or near failures arise from what is called "human error" and the picture is sometimes presented of the reliability of science compared with the unreliability of man. However, it is my submission that we need to design mechanical, electronic and chemical systems to take into account the most important factor in the environment in which these inanimate systems operate - man (and woman) in all his (her) complexity, both as a positive and a negative factor in any given situation.

Before examining the relationship between the expert and the remainder of the community, one should acknowledge that among the arbitrary characteristics of mankind that offend the susceptibilities of the expert is that proportionately more attention is paid to the occasional technological failure which causes say 20 or more deaths compared with the unending stream of road accidents, resulting in the death of about 1,000 people a day throughout the world and the maiming of a much larger number each day.

When combined with some of the other consequences of the private motor car such as a complete transformation in the character and shape of many of our finest cities, the problem of safe unobstrusive private transport is one of the major problems facing mankind today and successful solution of this problem would appear to require tackling on a macro-economic basis. Perhaps the most promising approach has been that of a US epidemologist who has suggested that we approach the road accident problem as an epidemic problem and deal with it in terms of prevention by improving the vehicle and the environment within which it operates (the road surface and surroundings), instead of trying to reform the driver.

It will probably not be acceptable within the framework of this conference for me to take the road accident situation as a major disaster and it is therefore necessary for me to deal with the problems of catastrophic technological failure, a subject of considerable concern and even morbid fascination to newspaper readers.

It is one of the features of modern society that we have placed increasing emphasis and dependence on the role of the expert. Beginning as an adviser to management and government, we have reached the situation where frequently the expert's views are not a guide to policy making but the basis of the actual policy itself. The most critical area is the interface between expert and decision maker. Whenever an expert makes an

assessment of future uncertainty, he has of necessity, whilst using quite sophisticated techniques in some cases, to make a number of subjective assumptions. It is therefore most important that those who rely on the work of experts have at least a broad understanding of the techniques that they are using and their reliability, as well as a clear understanding of the subjective assumptions that the expert has used.

One of the most interesting and important studies in recent years was the reactor safety study prepared by the US Nuclear Regulatory Commission in 1975. This was a most detailed, technical and mathematical study but the most widely used version of the report is a 12-page executive summary. To be quite fair, one should state that part of one of those pages is given over to a description of the techniques used in performing the study. The central technique was the use of what is called event trees and fault trees. To quote from the report:

> "Event trees were used in this study to define thousands of potential accident paths which were examined to determine their likelihood of occurrence and the amount of radioactivity that they might release.
>
> "Fault trees were used to determine the likelihood of failure on the various systems identified in the event-tree accident paths. A fault tree starts with the definition of an undesired event, such as the failure of a system to operate, and then determine, using engineering and mathematical logic, the ways in which the system can fail. Using data covering (1) the failure of components such as pumps, pipes and values; (2) the likelihood of operator errors; (3) the likelihood of maintenance errors, it is possible to estimate the likelihood of system failure, even where no data on total systems failure exists."

The first three pages of the report contain three charts showing fatalities due to man-caused events and frequency of fatalities due to natural events, together with the frequency of property damage due to natural and man-caused events. For anyone not used to such graphs, and presumably this includes most politicians and other decision makers, attention is naturally diverted to a small table on page 3 which sets out the average risk of fatality by various causes. A range of accidents is described starting from motor vehicles with 55,791 fatalities each year, producing an annual individual chance of death in one in 4,000, down to tornadoes producing 91 fatalities with an individual chance per year of one in 2,500,000. The last line covers the risk of fatality from nuclear reactor accidents assuming 100 plants and describes the risk as one in 5 billion per year.

To the observer who believes in experts and has no independent means of verifying figures, this would seem a most reassuring figure. However, what is particularly astonishing is that the report was prepared after an incident in a US atomic power station which can be described as a very near miss.

The official reoprt on this accident is a very lengthy one running to several volumes and I propose to rely on a brief extract from "The Sixth Report of the Royal Commission on Environmental Pollution" published in Britain in September 1976 as follows:

"There are those who believe that technical solutions can be found which will ensure that the risk of serious accidents are reduced to acceptable and negligible levels. There are others who believe that the potential hazards are so great and the possibility of human error in devising safeguards to cover every contingency so inescapable, that an acceptable level of safety cannot be guaranteed. It is hard to see that these views can be reconciled a priori. The contacts we have had with the nuclear industry during our study leave us in no doubt that the most diligent attention is given to safety and the design, construction and operation of reactors. It is, however, a fact of everyday experience, that all eventualities cannot be foreseen, even when the most stringent precautions are taken. A commonly quoted incident in this context is the fire in a lunar

module which killed three American astronauts in 1966 and which occurred because of the high inflammability of materials in a pressurised oxygen atmosphere. This had not be appriciated in spite of the immense resources devoted to safety in the project. A more directly relevant incident is one that occurred in 1975 at Brown's Ferry nuclear power station in the USA, involving fire in the cable room beneath the reactor control room. The fire was started by the flame of a candle which was being used by work-men to detect air leaks through cable openings. The emergency core cooling systems on one reactor were put out of action by the fire and very serious consequences were very narrowly averted. The risk of fire in the inflammable cables was realised by some of the staff and had been brought to the attention of the management but no action had been taken. No doubt the risk of fire from any cause should have been foreseen during design and no doubt it will be covered in future, but the question arises of what other unforeseen risks may exist. Certainly, it is clear that the unexpected hazards are not necessarily only the small ones."

If we regard the whole operation of the chemical, nuclear, or other potentially hazardous plant and its relationship with the human and other environment surrounding it as a total system, it is not too difficult to see that we are faced with a very complex problem of analysis, if we are going to predict the possibility of disaster and take all reasonable steps to avoid such a disaster, including an ultimate evaluation of whether the risk is acceptable. However, the tendency has grown in recent years for reliance to be placed on individual or small groups of experts, frequently from the same discipline to provide us with guidance on what is essentially a multidisciplinary problem. It would be too facile to blame the experts for their situation; we also need to point a finger at those managements who are too ready to delegate their responsibility for effective decision taking. Instead of balancing all the factors on the best possible information available to them, such managements rely on reports presented by experts, and see their own role as the relatively narrow one of accepting or rejecting such a report.

Now that is rather a sweeping statement and it cannot be said to apply to all of management. There are many companies where careful balancing of the information and the non-delegation of executive authority has ensured standards of operation and effectiveness of very high standards. Unfortunately there are many other managements where such standards do not exist and from time to time we are faced with a catastrophic system failure that subsequent examination shows could have been avoided by the operation of proper systems of management and control.

It should be recognised that the executive role of the expert is a very recent phenomenon. If we go back 60 or 70 years we find a situation where general management in industrial enterprises had a very clear over-all understanding of what was involved and the role of any ancillary staff was confined to the collection and summarisation of facts. The increasing complexity of science from an academic point of view and industry from a more practical point of view has led to the rapid advance of specialisation. The claim put forward that it is impossible for one man to understand and be master of all the knowledge that is required in the operation of science and industry is of course a valid one. Unfortunately, the development of specialist disciplines in universities and technical institutes and the parallel development of specialist functions in business has had two negative consequences:

(1) The chief executive or managing director has begun to delegate effective responsibility and to rely on the expert, not as a presenter of facts on which a decision may be made, but as someone who effectively makes the decision which the chief executive rubber stamps.

(2) The creation of powerful spheres of influence in the different disciplines and functions where the necessarily one-sided view that the particular discipline or function can have of an over-all system or event or activity is enthusiastically and aggressively presented as the only possible view with an equally aggressive state-

ment of the years of study or experience that the particular individual or individuals have devoted to a particular problem.

It is my view that the development of such narrow thinking has directly contributed to a number of disastrous errors in various fields. One might illustrate the social failures of high-rise flats, the building failures associated with the use of high alumina cement, failures in individual makes of motor cars that have led to mass recall, or the series of events that have led to some of the world's most serious air disasters.

In each of these cases the expert had his way and catastrophe ensued. In each of these cases we see an arbitary exercise of power by the expert and a reluctance of those who should properly be making the decisions to exercise balanced judgment. Although the examples I have quoted, with the exception of the use of high-rise flats, have had relatively narrow direct implications in terms of economic loss, the same argument can be applied to the decisions of experts in the field of government, where the demise of the generalist and the rejection of the need to consider many different views has led to increasing social conflict and unrest. We can see developing today the beginnings of a revolt against the arrogance of expertise run riot and the presumption that someone else knows better what is good for us as individuals.

In earlier times, the conflict was resolved in a simple and summary way by the arbitary exercise of power by one or a small group of individuals. Although such a system is unacceptable today, we should note that the individuals concerned were not frightened of taking decisions, exercising authority or facing the consequences.

Today such an approach is unthinkable but we are creating an informed population through the use of modern methods of education and a dissemination of knowledge and information. As a practising consultant I constantly find that the man who is nonexpert but has thought in a much wider way about the problem and faces the practical consequences of failure day by day, makes a wider and more objective contribution than the man whose years of training and devotion to a single aspect of the study have unfortunately made him relatively narrow minded.

This is probably a dangerous thing to say to a gathering of what must be devoted, well trained and highly-skilled experts, but I do feel the urgent need to balance the narrow-minded application of expertise with that most underrated of all human qualities, common sense.

In saying this, I am arguing for the value of expertise rather than experts. In particular, for trying to see a problem from many points of view and to examine the contradictions implicit in a particular problem or situation, so that we see the negative as well as the positive effects, or if we are pessimists, the other way around, we see the positive as well as the negative effects. This argues for a multi-disciplinary view and I think it is one of the contributions that good risk management has to make to improving the quality of life.

Having questioned the role of experts, I ought to emphasise that I do not see risk management or risk management consultants as super scientists or super experts that can eradicate or reduce the harmful effects of unbalanced use of expertise. Essentially risk management consists of using a variety of techniques from other disciplines to identify, measure and economically control the risks that threaten us, whether in business or government. The contribution of risk management is in terms of system, philosophy and method, rather than arbitary discipline or technique.

It is perhaps a reflection on the underconfidence that pervades many elements of society today, that experts feel the need to defend their arbitary view to the last, instead of welcoming constructive criticism that will help to exapnd their own knowledge, improve the quality of their own contribution and above all, to give a better and more effective lasting solution.

Essentially I am advocating a wider view of managing the risks implicit in many of today's activities. In particular that:

1. each of the disciplines or functions represented in any new major project should be required to give their assessment of the major vulnerabilities including the source of likely threats (from inside and outside the company);

2. each statement of vulnerabilities should be subject to comment by other disciplines or functions;

3. any major differences of opinion should be resolved;

4. special attention should be paid to human behavioural aspects;

5. general management should be required to endorse or reject or modify a combined statement of vulnerabilities and threats.

Such steps are already taken by some major companies who also carefully analyse malfunctions and incidents so as to prevent a repetition or avoid more serious consequences. The best plants, the best airlines and the best shipping companies have loss records considerably better than their worst competitors. The range of experience over a period of years would largely eliminate the incidence of risk and differences of 20 to one in loss experience between worst and best indicate the potential for improvement.

It cannot be stated that a wider multi-disciplinary approach will prevent all accidents but we can note from many accident investigations that the most prevalent factor is a failure to take into account normal human behaviour. Perhaps the biggest danger of the expert is the false sense of security given to others.

If we want safe operations, we need a level of awareness and alertness. To keep in mind the question "what happens if", rather than rely on someone else's statement "that it is impossible to ...". The expert has a special role in interpretation and guidance, in training but he should not feel that he can take sole responsibility. If he must state that this operation is completely safe or that a possible loss cannot occur, at the very least he must give his reasons and in terms that are understandable to those who are "non-expert".

May I conclude with one general observation on risk. A great deal of risk management thinking and writing is in terms of eliminating the risk. If one thinks in terms of preventing air crashes, preventing road fatalities, preventing industrial accidents, this must be a logical aim but if we see some risk as implicit in all human activity, whether at work or at play, we are faced with the dilemma that the only way to eliminate risk is to do nothing at all and even then, we might be caught by an earthquake. I see the role of risk management in helping us to understand and manage risk in today's society. This must include the deployment of various types of expertise but it also includes the balance of various opinions and perhaps the most important expression in risk management is that of "trade-off". By trade-off I mean balancing the positive and negative effects of an economic activity or decision or an expenditure. The whole concept of trade-off implies that life is constantly changing and that all of our activities and all of our decisions take place against an environment of quite complex human and non-human systems. When we intervene in those systems, we create changes which are for the better or for the worse. The contribution of risk analysis is to help us make better solutions, to improve our trade-off and to try and limit the negative effects and particularly to limit or if possible eliminate the catastrophically dangerous effects of our activity. The man who designed the control systems for that particular atomic power station did not take into account the possibility of a workman using a candle to look for air leaks. That example illustrates the vulnerability of experts and the contribution that they unwittingly make to disasters.

Risk Assessment of a Liquefied Natural Gas Terminal

Mr. J. T. Kopecek
Science Applications, Inc.
El Segundo, Ca.
USA

Introduction

SAI has completed LNG terminal risk assessment studies for both commercial and United States Government agencies. The analyses have included potential impacts on all phases of the delivery and storage operations. This paper presents an overview of the methodology developed and used in the SAI risk assessments. Particular results of the studies are not presented since they vary significantly with proposed terminal location. Individual results are available, however, on a requested basis.

Assessment Overview

The basic approach used by SAI in the development of a methodology for LNG risk assessment was to logically define the major elements in an LNG importation system. These elements define the potential initiating events. The elements of the LNG system are the ships used to transport the LNG, the loading and unloading terminals, and the storage facilities.

The initiating events that could lead to LNG spills include normal operations, natural events (winds, earthquakes, etc.), ship-ship collisions, and other man induced events such as aircraft and/or missile impact. Clearly, these initiating events will assume varying importance due to the location of the LNG system operations and facilities. This overview of the LNG system elements and the key initiating events are presented in Figure 1.

The next phase in the methodology was, for each of the system elements and initiating events, to perform the sequence of analyses similar to that described in Figure 2 for ship collisions. The probabilities for each of the LNG system elements and initiating events can be combined according to basic probability laws to provide a single number for estimates of LNG risk. Although very intimately coupled, the methodology can be reduced to the following specific tasks that must be performed:

- Accident Definition
- Consequence Analyses
- LNG Facility Element Penetration
- Physical Characteristics of an LNG Spill

Each of these tasks will be described in detail in the following paragraphs of this section.

Initiating Eevents

Normal Operations

Normal operations, defined as operations internal to the LNG plant or ship, are analyzed to determine equipment failure and other events which could individually or in combination result in a significant LNG spill.

The approach to estimate the potential LNG spills due to "business as usual" required two types of analyses as described in Figure 3. The first was a fault tree approach which combines basic fracture and failure paths and the second was fracture mechanics

to determine the physical extent to which failures would develop (due to fatigue or critical crack lengths at operating conditions).

Fault tree analysis is a methodology that serves to systematically and logically combine component failure modes and other events (e.g., operator errors) which can individually or in combination result in system failure and/or LNG leakage. The fault trees are used to analyze the following major systems:

- Tanker
- LNG transfer system
- Storage tanks
- Vaporizer system

Elementary stress analyses of the tank for both static and cyclic loadings were conducted. Critical crack lengths (i.e., cracks that would result in fast fracture) were calculated using conservative assumptions (e.g., regions of lowest roughness). Typical results show that the critical crack lengths were several times larger than the wall thickness. Thus, any subcritically growing part-through crack would become a through crack before it became a critical crack. The final step is to calculate the LNG leak rates through a critical crack based on basic fluid dynamics.

Basic fracture mechanics principles (e.g., ASTM, Section XI) were applied to the fatigue analysis of the LNG tank where it was assumed that existing part-through cracks would propagate, under cyclic loading (over 20 years) to produce a through crack and therefore a leak. The analysis was also applied to initial surface defects. Typically, it was found that the initial flow size would be large relative to the capabilities of inspection procedures to identify these cracks. Even if a crack did escape detection, the crack would not grow to a critical crack size within the period of time in which the tank was to be operable.

Similar calculations were conducted for the ship tanks.

Natural Events

The natural events of interest include severe winds, tornadoes, storm waves, tsunamis, earthquakes and meteorites. A summary of the approach used for each of these events along with the major conclusions are presented in Figure 4.

To a large extent (for severe winds, tornadoes, strong winds, tsunamis, and meteorites) the approach used the historical incidence as a basis to identify event characteristics (frequency, etc.) and LNG system vulnerabilities from which the probability of an LNG spill was estimated as well as recommended design changes that would further reduce the potential impact.

Ship Collisions, Ramming, Groundings

The possibility of an LNG ship tank spill can occur through groundings, rammings with fixed objects, and when a loaded LNG ship is struck by another ship. In regions studied by SAI to date, groundings have been judged not to be severe enough to result in an LNG spill. Rammings have also not resulted in predicted LNG spills and therefore are not discussed in this paper.

The methodology used in the ship collision analysis for harbor accidents has been shown in Figure 2. Initially, a data base was established from the U.S. Coast Guard (available for the last six years) for major U.S. port areas for analysis and application to the particular region of interest. SAI has analyzed the port areas of Los Angeles, Long Beach, Boston, New York, Tampa, the Mississippi River Delta, and Galveston. The data base was carefully screened to identify those collisions which

would be similar to an LNG tanker being struck by another ship capable of penetrating the hull. The result was that there were seven collisions in the seven ports for 554,400 transits recorded over the six year period of ships greater that 1000 tons.

Following the establishment of the data base, SAI develeoped a ship collision model to estimate the probability of shipping accidents in the future based on these statistics of the past and to account for changes in the volume and characteristics of ships. This model embodies the various elements which are factors in ship collisions, such as speed, length and width of ship, number of ship transits, and the geography of the site in question. These parameters were estimated for the various operating sites of interest. Much of the data was common and could be derived from the existing data base. For example, empirical representation for the distribution of the draft by type of ship and the relationships between displacements, beam and length of various classes of ships are available. This information was used to characterize traffic in other areas than in which the data was obtained. The collision model was calibrated with analyses to predict the probability of collision in the seven port areas described above. The model was conservative (i.e., predicted higher ship collision probabilities), but was generally in agreement with the observations at the seven port areas as well.

Another key consideration in the analysis was the cargo tank rupture probability. The study used the theoretical method of V. U. Minorsky (Ref. 1) that relates the structural resistance of deformation of the colliding ships to the effective kinetic energy of the collision. The analysis accounts for such parameters as the mass of the striking ships, the hydrodynamic mass of the struck ship, the relative velocity and orientation. The data base was examined to determine the distribution of the parameter of the speed of the colliding ship as well as the angle of incidence. Both were assumed to be uniform.

Also addressed in the SAI analyses were questions relating to the effect of operating restrictions. It was concluded that these would only serve to improve the probability of a ship collision as calculated based on the above approach and model.

Aircraft and Missile Operations

The approach used to estimate the probability of an LNG accident due to an aircraft crash is presented in Figure 5.

To carry out this analysis it was necessary to establish the history of crashes of air carrier (both general and military aviation) to provide a reasonable basis for developing a predictive model. There is an extensive data basis available on aircraft crash data from the National Transportation Safety Board (NTSE). This data base was searched to provide data for:

- Determining the probability of an aircraft crash per square mile per aircraft operation for air carrier, general aviation and military aviation as a function of distance from an airport up to five miles.
- Determining the residual aircraft crashes for air carrier, general aviation, and military aviation operations that occur beyond the five-mile radius about airports.
- Determining the validity of using fatal accidents as the index of those accidents which threaten LNG facilities.
- Eliminating general aviation and air carrier aircraft statistics that do not engender risk to commercial installations.
- Determining the aircraft crash statistics for the region in comparison to the National statistics.

- Determining general aviation accidents represented by aircraft greater than 12,500 lbs in weight and the accidents for aircraft of 12,500 lbs or less in weight.

A Model for LNG Installations

Nearly 50 percent of all aviation accidents occur within a five-mile zone about airports. Beyond five miles, the accidents are considered random in nature and not directly related to the problems of errors made during takeoffs and landings. The symmetrical bivariate Gaussian distribution approximates the established statistics for accidents within the five-mile zone about a given airport and is termed the near field. Beyond the five-mile zone, the accidents occur in a random manner and this region is termed the far field.

The penetration analyses conducted for both aircraft and missile hazards is applied to both storage and ship tanks and pipelines used to transfer LNG.

For the storage tanks and tankships, a worst-case impact was chosen to insure that penetration would yield an upper bound on the penetration probabilities. This was accomplished by choosing impact points which maximize the normal component of velocity over the surface being considered.

An important simplifying assumption regarding the impacting aircraft is that they are non-deforming. It follows, therefore, that the aircraft does not change mass and shape subsequent to initial impact. The actual aircraft under consideration will most likely undergo considerable deformation upon impact; and, therefore, they will absorb a certain amount of energy. Nevertheless, it has been assumed in this analysis that this energy is expended in the barrier (target) material itself. These assumptions give rise to conservative penetration predictions.

Failure due to pipeline impact were also considered. The effective areas of the pipelines were estimated to determine the impact probability. Next, the energy required to sever the pipe is compared with the kinetic energy of the impacting aircraft.

The considerations required here are, of course, similar to those required for missile impact analyses.

Consequence Analysis

The preceding sections described the potential events that could lead to a spill. A crucial question that must also be addressed is, given that a spill occurred what would be the consequences that could be expected. The approach taken was as follows:

- Define the location and size of the spill based on the analyses described in the previous section. This led to various scenarios for subsequent analyses.
- Predict the dispersion of the LNG vapor cloud resulting from the various scenarios accounting for the prevailing meteorological conditions, the vaporization rates and terrain.
- Analyze the characteristics of LNG ignition, the nature of ignition sources and the probability of ignition associated with the various scenarios.
- Determine the thermal radiation fields around the LNG plume and pool fires assuming that ignition occurs.

Each of these aspects will be described in detail below.

This methodology is shown schematically in Figure 2 which includes its relationship

to other parts of the study.

Spill Scenarios

The spill scenarios considered must be defined in terms of the initiating events previously described. For example, a single full storage tank would release approximately 88,000 m^3 of LNG and a single tank from an LNG ship would release 25,000 to 37,500 m^3 of LNG. SAI has completed the following cases.

- 37,500 m^3 instantaneous spill on water from failure of a single ship tank.
- 75,000 m^3 instantaneous spill on water from failure of two ship tanks.
- 88,000 m^3 instantaneous spill on land due to failure of a single storage tank.
- 176,000 m^3 instantaneous spill on land due to failure of two storage tanks.
- 352,000 m^3 instantaneous spill on land due to failure of four storage tanks.

Each of these spill conditions was analyzed in terms of meteorological effects including wind speed and direction, atmospheric stability, relative humidity, LNG spill rate and volume, and site topography.

LNG Vapor Plume Dispersion

The meteorological conditions at the site must be defined. This includes specifying the atmospheric stability class and the regional climatology. Regional data sources can be consulted (NOAA-EDS, NCC; USAF; National Weather Science). Thus usually provides the necessary data to characterize the wind speed and direction stabilities, expected flow patterns and topographical considerations that would have an impact on LNG cloud dispersion. This is standard meteorological analyses that are also conducted routinely for air pollution analyses.

The next key technical consideration are the spill and vapor source rates for unconfined spills on land and water and confined spills on land. Existing data correlations are available and generally accepted by the technical community for prediction of evaporation rates. Variables considered include LNG spread rates, minimum pool thickness, evaporation rate, ice formation, effects of wind and convection on evaporation rates, and effect of solar radiation.

The basic information on the vaporization rates were necessary to provide key input data for prediction of the dispersion of natural gas. Additional considerations necessary were a quantitative method to describe the physical phenomena by which air is entrained in the negatively buoyant plume and modification of the local atmospheric stability due to the LNG cloud density.

The main features which constitute the development and subsequent dispersion of an LNG vapor cloud are as follows (see Figure 6): LNG is lighter than water and insoluable in water and will rapidly spread over its surface, or comparably, land. As it does, it will absorb heat from the underlying surface and vaporize. As the LNG spreads, the rate of vapor generation increases because there is more surface over which heat can be transferred. The vapor cloud grows in size until the liquid pool breaks up. The diameter of the vapor cloud will be much greater than its height, since vertical spreading will be inhibited by the higher density of the vapor cloud. Although methane vapor is colorless, the cloud will appear white due to condensation and/or freezing of water vapor entrained from a water surface or condensed from the atmosphere.

The initial bulk temperature of newly vaporized methane is approximately 112°K. At that temperature and at atmospheric pressure, methane vapor is approximately 40 percent more dense than ambient air. Consequently, there is no tendency for the cloud to rise. Experimental data (2) indicate that the vapor cloud continues to spread radially, and there is very little vertical dispersion. Entrainment of air increases the cloud temperature, but calculations show that, generally, the density of the mixture remains above that of the diluting air. In instances where the heat input from the surface of the water and/or heat input from the condensing and freezing water vapor is significant, the vapor cloud can become neutrally buoyant. In theory, it is possible for an LNG cloud to become buoyant; however, this has not been observed experimentally, with the possible exception of one test (No. 16) discussed in Reference 2.

As the cloud moves downwind, it is further diluted by turbulent mixing with ambient air. In the absence of ignition, this process continues until the entire contents of the cloud are mixed to concentrations below the lower flammability limit and the methane is dispersed in the atmosphere.

To assist the evaluation of these phenomena, numerical methods are required. These methods assume that a vapor source rate exists which has been calculated using the methods outlined in the above paragraphs. The results of the dispersion calculation is a distribution of methane concentration as a function of position and time. These events involve a complicated interaction between fluid dynamics and turbulent diffusion. The formulation employed characterized by a unified treatment of the fluid dynamic system consisting of methane vapor and ambient air. In order to carry out this analysis it was necessary to use numerical simulation of the fluid dynamic equations, which are described in detail in Reference 3. The calculations performed using these codes were validated with experimental data to make direct comparison between predicted and experimental results. It was demonstrated that the techniques could produce quite accurately the characteristics of LNG spills.

It is of interest to demonstrate the results of these analyses as shown in Figure 7 which gives the concentration profiles of methane for various atmospheric wind conditions and time after an instantaneous spill on water. These results are used to define the region or extent of the 37,500 m^3 LNG "Lower Flammable Limit (LFL)".

Ignition Probabilities

Having defined the dynamic characteristics of the vapor cloud, the ignition probabilities must be addressed. This is an area of great uncertainty due to the fact that a flammable LNG vapor/air mixture may be ignited by a vast number of sources (open flames, arcing, switches, discharges, etc.). It was reasoned that in the average or typical accident case that there will be immediate ignition upon impact. Nevertheless, the possibility remains that immediate ignition will not occur.

In order to give recognition to the possibility that a major spill could occur without immediate ignition, the probability of immediate ignition is postulated for SAI studies as nine out of ten, but only in the case of a penetration by ship, aircraft or missile. The approach taken by SAI, then, is to assume a 90% probability for immediate ignition in the event of ship, aircraft or missile impact; a 10% probability for plume spread in such cases prior to ignition; and a 100% probability of such spread in the event of ruptures that are internally generated or caused by earthquakes or meteorites. These assumptions are thought to represent a conservative means of arriving at fatality probabilities related to hypothetical plume ignition. Individual sources on land have been assumed to havea 1% probability of igniting a plume passing over them.

Thermal Radiation

The next key issue that must be addressed is the thermal radiation that may result

from ignition of LNG spills, and a determination of the spatial region within which fatalities may occur beyond that area occupied by the plume or pool fire.

Two general problems must be analyzed - the first is the effect of ignition and flame propagation through the plume (plume fire), and the second is the effect of a stationary fire attached to the vaporizing liquid pool (pool fire). Models have been developed for the thermal output and flame geometry for premixed (both fuel-lean and fuel-rich) fires. By premixed it is meant that portion of the plume which has already been dispersed and mixed to the molecular level by atmospheric mixing. A methodology was developed for the analysis of the pool fire hazard which included the general geometric relationships for calculating thermal radiation fluxes on to receiver surfaces located outside of the fire. Conservative thermal exposure criteria have been selected for fatalities which were then integrated in a straight-forward manner to provide the estimate for fatalities based on the regional or local population distribution. The effects of burning on local wind fields must also be addressed.

Risk Evaluation

The final assessment of risks are determined as the probability of fatality per year per person and compared in several ways to the fatalities that could result from other causes. The risk determination requires that a summary analysis be conducted which includes the following elements:

1. The initiating event probabilities and spill zones independently identified.

2. The surrounding population and source distribution for each spill zone be individually analyzed.

3. The probability of all expected meteorological conditions be accounted for.

The expected fatalities for each possible accident, site, and condition are calculated in a time dependent manner (see Figure 8) and the overall risk is obtained by summing all independent events.

SAI has chosen to present the contours of the estimated fatalities per year (Figure 9). A second approach is to present the cumulative probability that a given number of fatalities would occur within a year. This can be compared with other fatalities that could result from either natural or man made events.

REFERENCES

1. Minorsky, V. U., "An Analysis of Ship Collisions with Reference to Protection of Nuclear Power Plants", Journal of Ship Research, The Society of Naval Architects and Marine Engineers, Vol. 3., No. 2, October 1959.

2. "LNG Safety Program Interim Report on Phase II Work", American Gas Association Project IS-3-1, July 1974.

3. "LNG Terminal Risk Assessment Study for Los Angeles, California", Science Applications, Inc., Report No. SAI-75-614-LJ, December 1975.

INITIATING EVENTS AND ASSOCIATED PROBABILITIES

- NORMAL OPERATIONS OF THE TERMINAL
- NATURAL EVENTS (WINDSTORMS, EARTHQUAKES, ETC.)
- SHIP COLLISIONS
- AIRCRAFT IMPACTS
- MISSILE IMPACTS

FIGURE 1. OVERVIEW OF LNG SYSTEM ELEMENTS AND INITIATING EVENTS

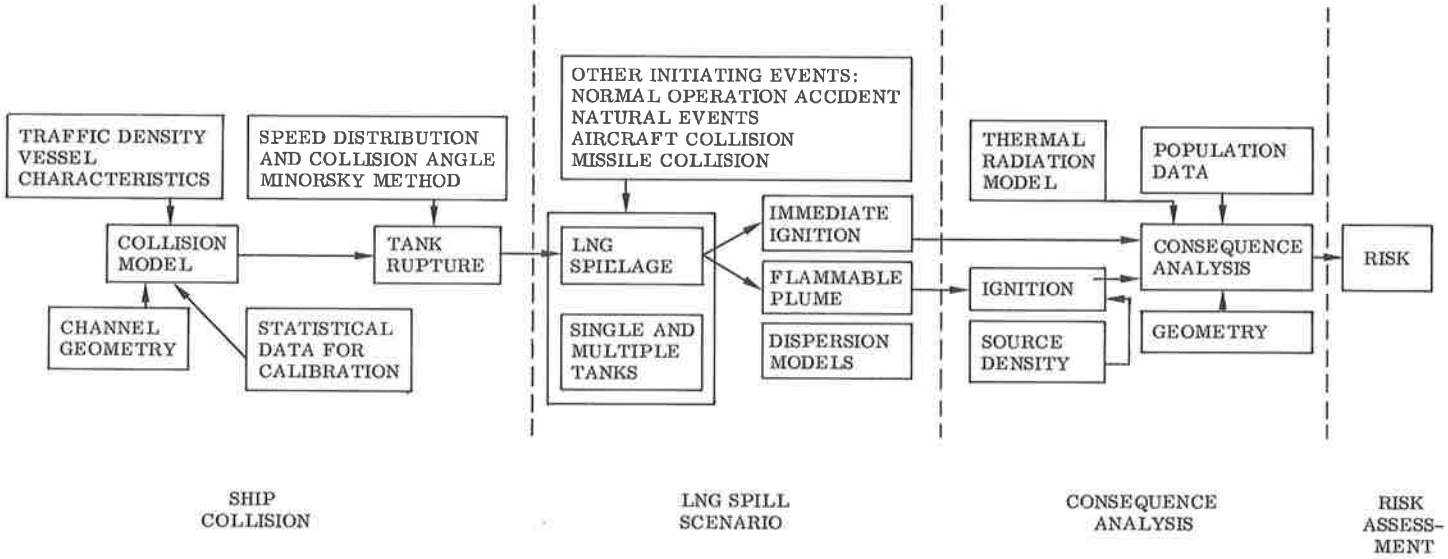


FIGURE 2. METHODOLOGY OVERVIEW FOR LNG RISK ASSESSMENT FOR SHIP COLLISIONS AS AN INITIATING EVENT

METHODOLOGY FOR LEAKS UNDER NORMAL OPERATIONS

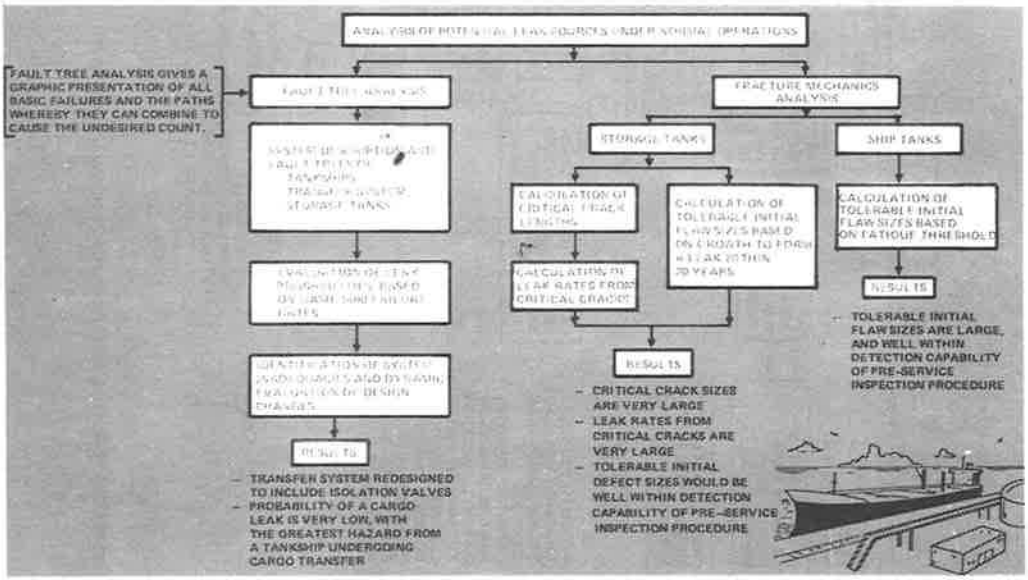


FIGURE 3

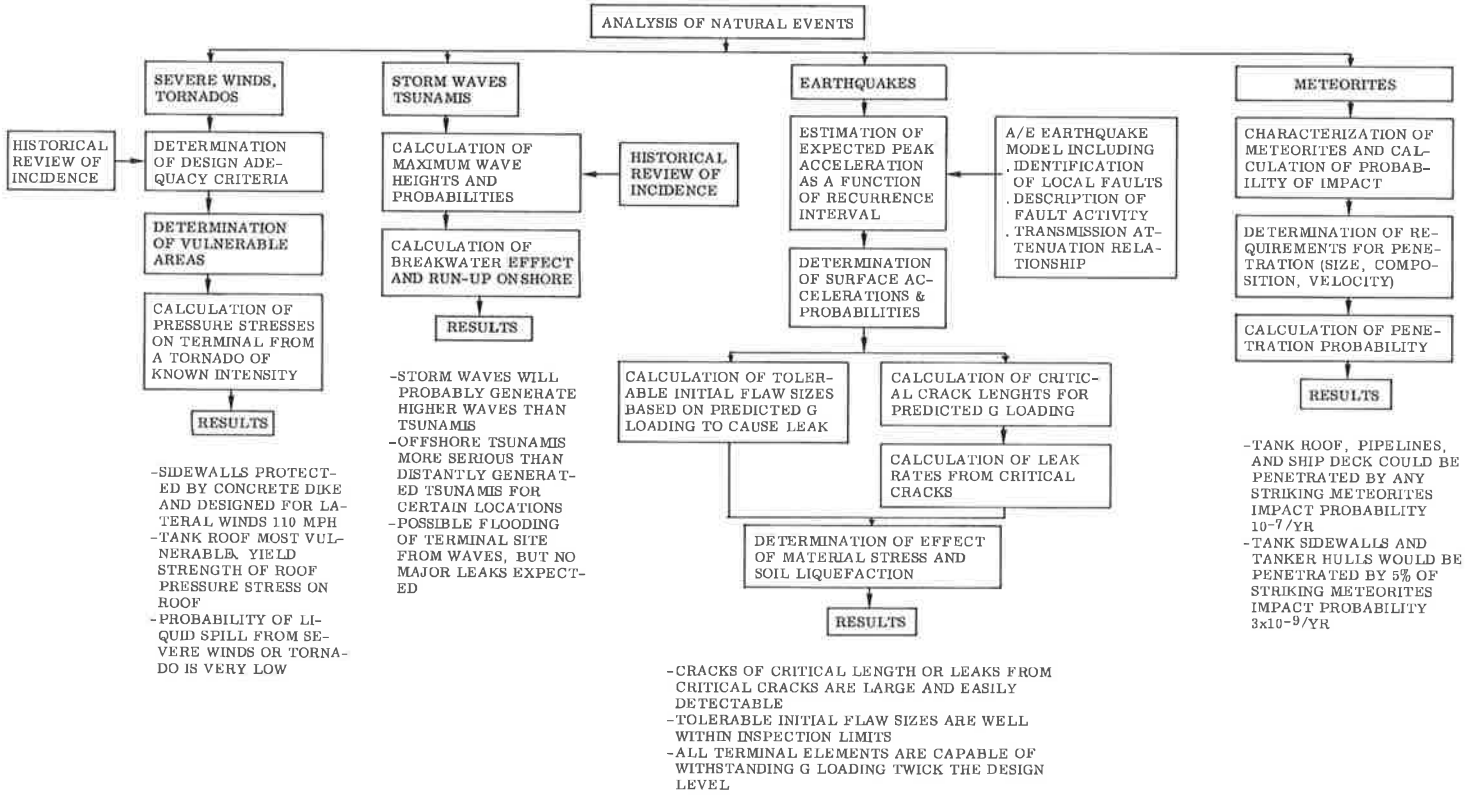


FIGURE 4. METHODOLOGY FOR ESTIMATING POTENTIAL LNG SPILLS DUE TO NORMAL OPERATIONS

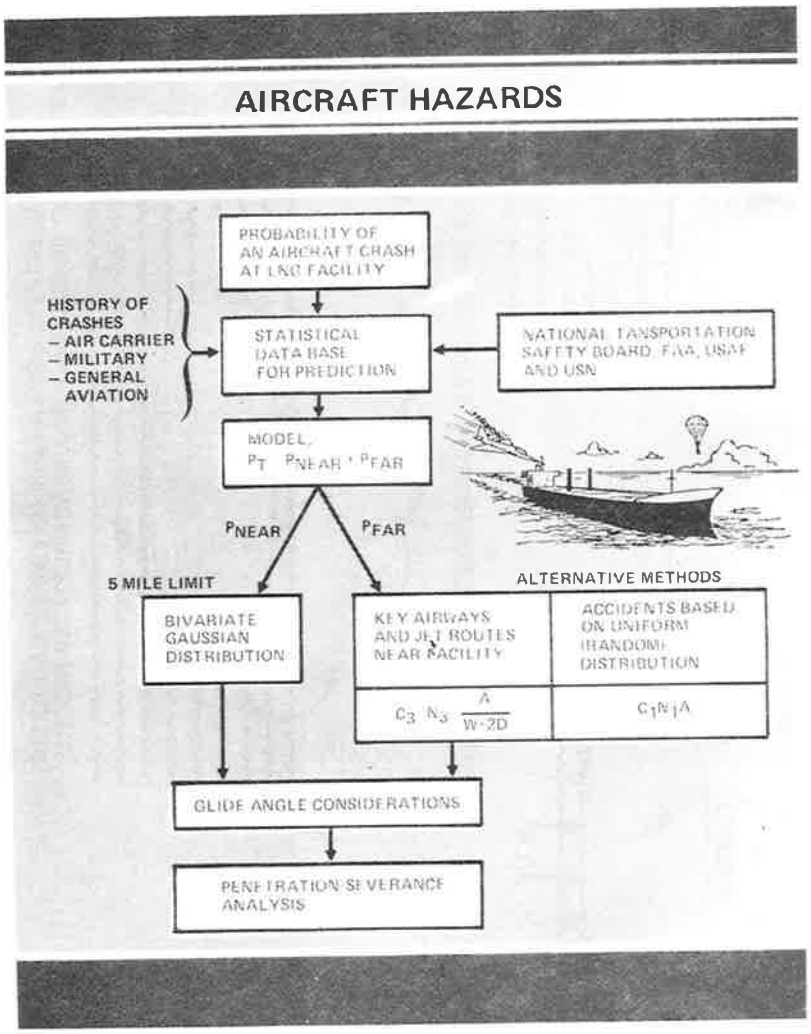
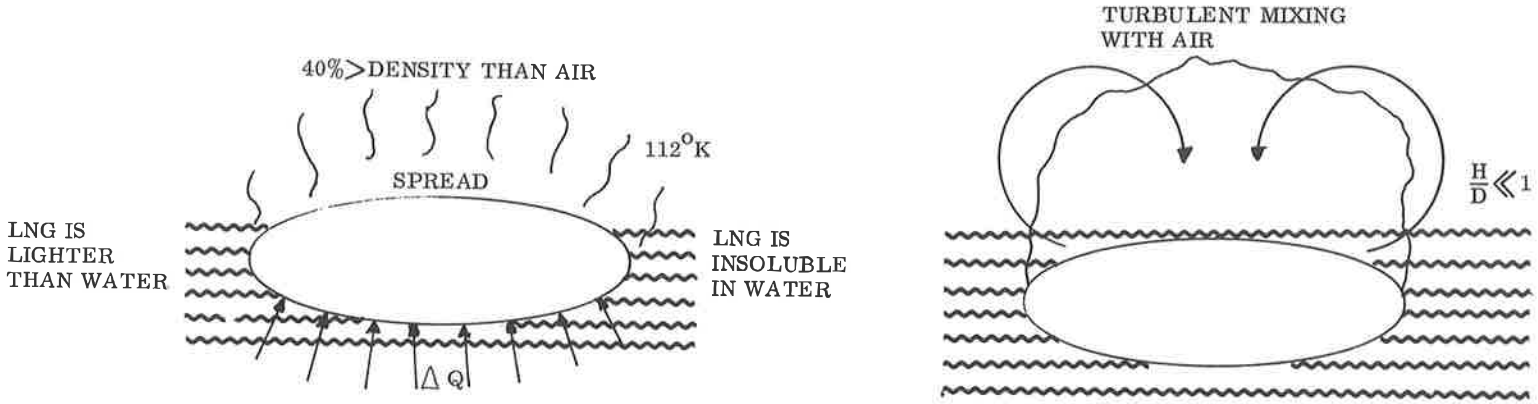
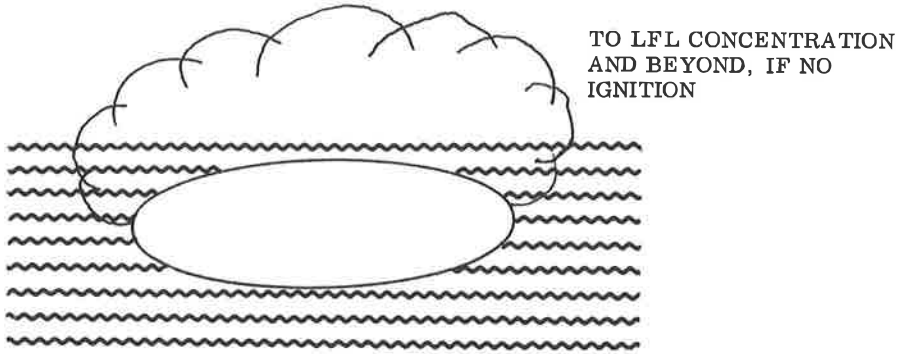

AIRCRAFT HAZARDS
PROBABILITY OF AN AIRCRAFT CRASH AT LNG FACILITY
HISTORY OF CRASHES
– AIR CARRIER
– MILITARY
– GENERAL AVIATION
STATISTICAL DATA BASE FOR PREDICTION
NATIONAL TANSPORTATION SAFETY BOARD, FAA, USAF AND USN
MODEL,
P_T P_{NEAR} ' P_{FAR}
P_{NEAR}
P_{FAR}
5 MILE LIMIT
ALTERNATIVE METHODS
BIVARIATE GAUSSIAN DISTRIBUTION
KEY AIRWAYS AND JET ROUTES NEAR FACILITY
ACCIDENTS BASED ON UNIFORM (RANDOM) DISTRIBUTION
$C_3 N_3 \frac{A}{W \cdot 2D}$
$C_1 N_1 A$
GLIDE ANGLE CONSIDERATIONS
PENETRATION SEVERANCE ANALYSIS

FIGURE 5



WHITE CLOUD-CONDENSATION/FREEZING OF WATER



. NUMERICAL TECHNIQUES FOR ANALYSIS OF COMPLICATED INTERACTION BETWEEN FLUID DYNAMICS AND TURBULENT DIFFUSION

. SLICE, SIGMET

FIGURE 6. PHYSICAL PROCESSES IN AN LNG SPILL

CONCENTRATION ISOPLETHS FOR AN INSTANTANEOUS SPILL OF 37,500 m^3 OF LNG ON WATER WITH A 7m/sec WIND

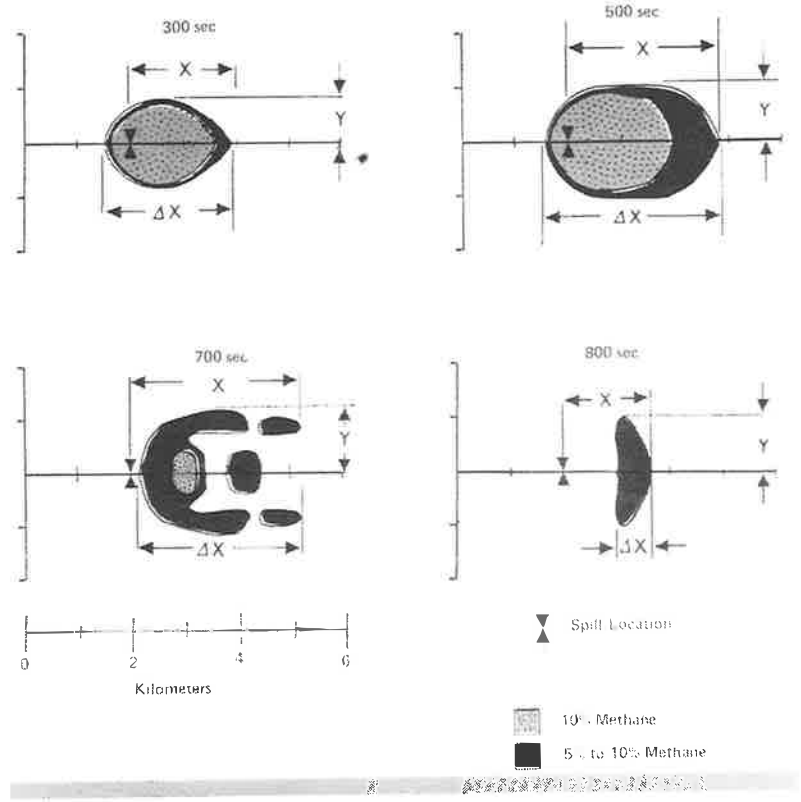
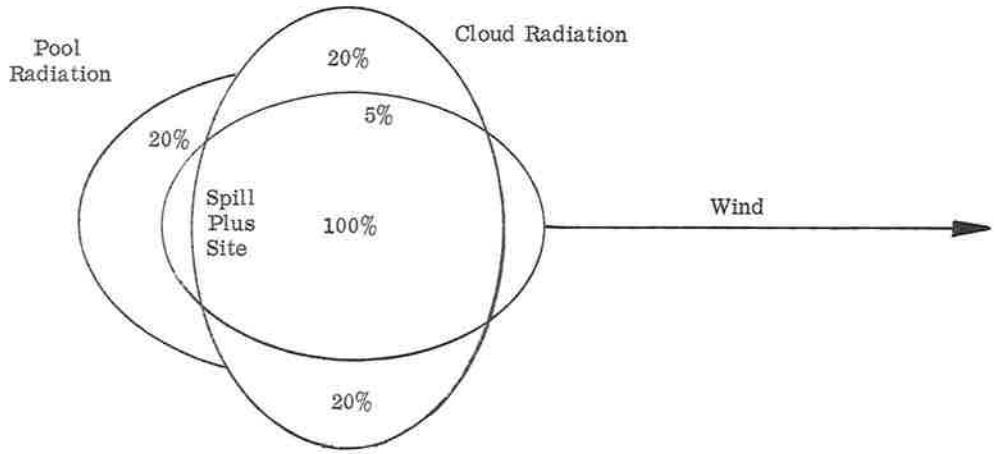


FIGURE 7



Percent expected falatilies assumed within

a. Flammable plume area 100%

b. Cloud fire radiation area 20% (from cloud region C_ 10%)

c. Pool fire radiation area 20%

FIGURE 8. FATALITIES DUE TO IGNITION AT A GIVEN TIME FROM SPILL

LOS ANGELES, CALIFORNIA

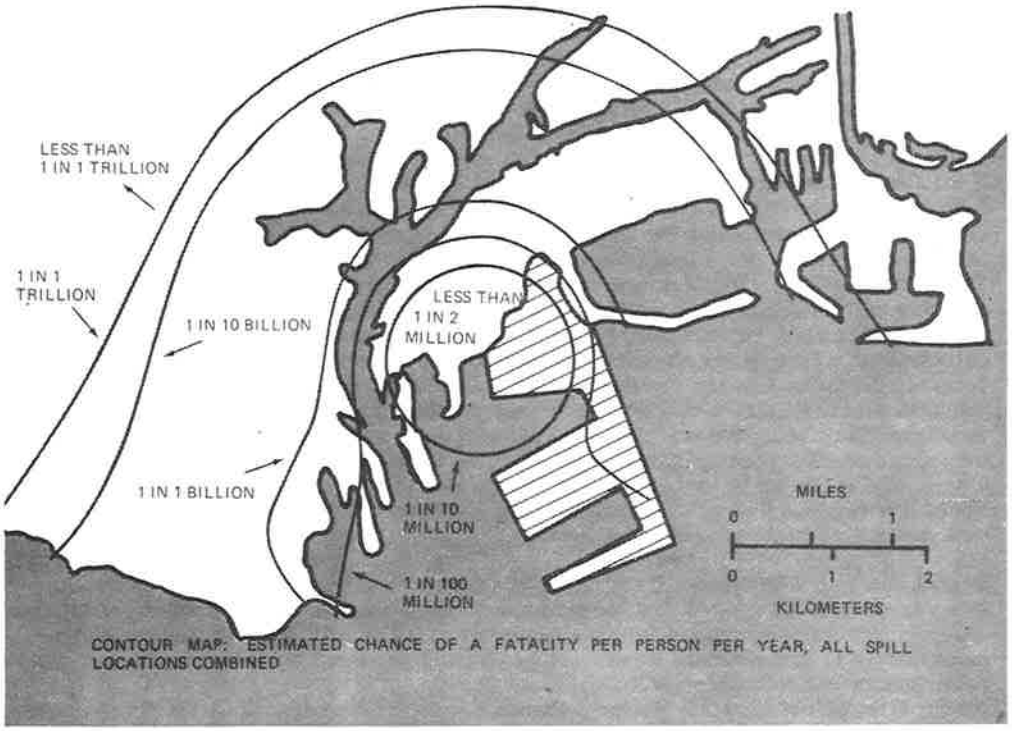


FIGURE 9

Case study: A chlorine destruction unit

Ir. M. Vis van Heemst
AKZO Engineering BV
Arnhem
The Netherlands

As a result of some major accidents in the recent past, such as Flixborough, DSM and Seveso, the chemical industry is searching for more effective approaches to safety. One of these approaches, which is new for a large part of the chemical industry, is 'quantitative risk analysis', also known as 'hazard assessment'. Today, many chemical companies are exploring the possibilities of this technique, and since about one year AKZO is one of them. Why did we join?
We did not join simply because our competitors were investigating hazard assessment, but because, after a serious study, we concluded that one of the main advantages of risk analysis is the possibility of giving more structure to the important decisions that have to be taken about safety investments. Up till now safety usually has been looked at in a rather subjective and qualitative way. Risks were and are weighed intuitively, and therefore there is a heavy personal element in many decisions about safety. We think that risks and hazards should be assessed in a more quantitative way and that in the long run, when tools and techniques have been developed further, this approach will lead to greater safety of industrial installations for the same outlay of money.
If we assume that Risk (R) is some function of Probability (P) and Effect (E) - R = f (P,E) - then we can say that ways for calculating effects have been deeply studied in recent years, in particular the dispersion of toxic gases and the explosions of vapour clouds. As a result there is a general ability to calculate E.
Today much effort is spend on the calculations of the probabilities P. Although we think that this is worthwhile, this may not give the results that are expected, as the public, and the authorities, are not used to and often not interested very much in probabilistic calculations. Discussions about risk tend to focus on the size of the effect, and the favourable influence of a low probability is hardly taken into account.
We think that there are a number of reasons for this lamentable state of affairs, the most important being the complete absence of a good and universally accepted definition of the concept of 'acceptable risk'. We also think that for risk-analysis to become a succesful engineering tool, a good definition of this concept is a necessity, and we would like to plead that government, society and industry come together in a work-shop or a committee to thrash out the criteria.

In risk analysis AKZO had a flying start by taking a course at the ICI-Mond-Division, five years after ICI started their hazard assessment studies. In this field there is good co-operation and exchange of information between ICI and AKZO, because the standpoint of both is that whereas we are competitors on the market, the safety of our chemical plants is a joint interest.
As our first object for study we have chosen a chlorine destruction unit that is in operation at one of our chlorine sites. It is a rather simple type of plant and as such it is ideal for a first study in hazard assessment. Furthermore, it plays an important role in the safety of the chlorine production factory.
Now it is not my intention to present the complete analysis we carried out, as that would comprise far too much detail. Instead, I will use a simplified model of the unit, which is given in figure 1. The installation consists of four main components:
- a vessel filled for 70 per cent. with caustic soda
- a cone shaped reaction section with an ejector on top
- a pump that feeds the ejector with liquid taken from the bottom of the vessel
- a heat exchanger to remove the heat of the reaction.

The flow of caustic through the ejector creates a slight underpressure, which sucks in the chlorine containing gases. The chlorine is absorbed in the caustic spray, and the remaining gases are vented into the atmosphere via the stack.

There are two control loops:
- a quality control loop for keeping the concentration of the free caustic in the vessel constant
- a level control loop which regulates the supply of fresh caustic.

In addition there are a high and a low level alarm.
When, for instance, the concentration of free caustic in the vessel becomes to low, the quality control loop activates the valve, and more of the contents is pumped to storage. The level starts to fall, and that activates the level control loop which causes fresh caustic to be pumped into the vessel.
What we wanted to predict is the probability that the system will fail and chlorine will escape into the atmosphere.
Obviously, there are four possible modes of chlorine escape:
1. Vessel is empty
2. Vessel is full, but caustic is depleted
3. Circulation stopped
4. Gas passage is blocked.

Let us work out the first mode as an example of what we did.
When will the vessel become empty? The most probable failure that will lead to an empty vessel is a closure of the level control valve. In this case the difficulty is that there are but few hard facts about the failure rates of control loops and we have to make an estimate. Unless the operating conditions are very extreme, we may assume that a failure of a typical control loop occurs once or twice a year. This is confirmed by the work of Professor Lees of Loughborough University and by others. In parentheses, I would like to point out that Professor Lees has presented many data on these and similar problems recently at a Symposium of the Institute of Chemical Engineers, held at Edinburgh.
On the face of things we will have to reckon with a failure rate of the valve of 1.5 times a year, but that is not the whole story as:
- In a well designed control-loop most of the failures go in the safe direction, which here means an open valve. It is estimated that only one of three failures will lead to a closed valve;
- Most failures occur gradually and are self-revealing. They will lead to proper action by the operator before any harm is done.

A normal estimate is that about a quarter of the failures in the control loop will appear suddenly and may lead to serious consequences. Working all this out by simple arithmetic gives a failure of once in 8 years that will occur suddenly and will surprise the operator.
From process calculations we know that it takes at least half an hour before the vessel becomes empty and chlorine will start to be vented to the environment. In addition the system is equipped with a low level alarm which mostly works when called upon, but which may fail sometimes. As Mr. De Heer has pointed out in his paper, the probability that the alarm will be found in a failed state strongly depends on the frequency of testing. On average, an alarm will fail halfway between to tests and will be unavailable for the second half of the test period. Now the typical failure rate for an alarm module is once per 10 years, and if it is tested once a year it will be unavailable for half a year in 10 years on average, which means a probability of 5%. There is a 95% probability that the alarm will respond.

When the alarm works and when the alarm does not work, what is the probability that the operator fails to react correctly? This is a very difficult question to answer, as it involves human factors. The subject of human error has been discussed extensively in the literature, but very little of it is quantitative. Data are scarce, and most of the discussions are based on guesses only and therefore should be handled with care. In 1974, however, ICI presented a paper at a symposium for Instrument Engineers (at Welwyn) which gives a list of human failure data, which we can use as a guide (figure 2). Since these published data refer to lapses in attention only, it should be checked whether lack of ability to cope, training or motivation might have an influence. The

figure illustrates clearly that the time available to the operator for taking the correct measures, is extremely important. When he has only a few minutes to act, the probability of failing to do so is nearly one hundred per cent. If time is unlimited, this will come down to 2% if the alarm works and to 10% if it does not.
In the AKZO case the operator has at least 30 minutes to react correctly, and according to figure 2 that would mean a failure rate of 25% in case of no low level alarm and of 5% if the alarm works. The data of ICI, however, refer to complex plants, and in our simple system we thought it acceptable to lower the rates to 10% and 2% respectively.
All information collected up till now, can be summarized in a fault tree given in figure 3. This gives a chlorine emission due to a failure in the level control-loop of once in about 350 years.
This figure is, of course, wholly unrealistic, as we considered only one of the four modes of failure. Of the other three modes, two are the result of failure of control loops and can be analysed in the same way as we just did (figure 4). The remaining mode, however - no circulation because of pump failure - should be analysed on its own. Figure 4 shows that this mode gives the most important contribution, a probability of failure of 0.23 per year.
Let's now see whether a chlorine escape of once per 4 years could be qualified as acceptable.
So far we have only looked at probabilities, now we should take the effects in consideration too. For that we need a gas dispersion model which allows us to calculate the amount of chlorine the population in the neighbourhood may be exposed to. Secondly, we need a set of criteria that allow us to predict the hazards of inhalation of chlorine, which in high concentration is a rather dangerous gas. Let us take the criteria first.

The only criteria on toxic gases that give a relation between size of effect and allowable frequencies are those published by ICI. The effect is split-up over different hazard categories and an allowable frequency is adjudged to each category equal to what ICI thinks is socially acceptable. We think that this is a good approach. (Figure 5).
There are four categories:
- Category 0 the area where there is no smell and no inconvenience to the public
- Category I chlorine can be smelles and in consequence causes some inconvenience, but no harm is done. The situation is undesirable, however, and a frequency of once a year is deemed acceptable for the site as a whole
- Category II can be attended by some degree of distress and damage to vegetation. Claims are possible. Is not acceptable more often than once per 10 years for the site as a whole
- Category III personal injury and even a fatality may occur, and a frequency of only once per 100 years is deemed to be acceptable for the site as a whole.

In category III an additional criterium is imposed, stating that the individual risk of death outside the plant should be many times lower than the risk from all other activities in life.
We think that the criteria summarized in figure 5 are realistic and are a good starting point for further discussion on risk criteria which should be started as soon as possible.

To take a concrete example, let us assume that the unit has a through put of 600 kg chlorine per hour and that after a complete break-down it takes 10 minutes to get the situation under control again, then 100 kg of chlorine will have escaped. The effect of this outside the boundary of the site is calculated with the help of a computerprogramme that contains:
- a detailed weather model, consisting of 648 permutation probabilities for direction of wind, wind speed and stabilities in the atmosphere
- for 18 directions of wind, the distance of the source to the down-wind boundary, and the height of nearby buildings
- the stack height
- a Pasquill dispersion model.

For a given emission the computer calculates the probability that the hazard at the boundary of the site will lie in one of the categories.
Figure 6 gives the frequencies we might have found for the emission of 100 kg we discussed earlier. We can see that in this case the frequencies are:
Category I : 24%
Category II : 69%
Category III : 3.5%.
Combined with the source frequency of 0.24 per year this leads to incident frequencies of 0.06, 0.16 and 0.008 per year for the three categories. We found that the allowable frequencies were 1.0 for category I, 0.1 for category II and 0.01 for category III. The destruction unit, however, is only one of the potential sources of dangerous gases at the site. If the plant records show that the fraction the unit will contribute is 20%, then this lower the allowable failure frequency with a factor of five to:
Category I : 1 per 5 years
Category II : 1 per 50 years
Category III : 1 per 500 years.
Figure 6 shows that with the one unit system the limits are exceeded, so modifications become necessary. One road open to us is to look at the relative contributions of the four failures modes we discussed above, and to try and change them in such a way that the limits are met. Another way would be to change over from a one unit system to two systems in series, and that indeed is the solution adopted at AKZO.

For the presentation of this case a simplified model of the chlorine destruction unit was used. However, this could be dangerous as it might give some the idea that risk analysis is a relatively simple matter. That conclusion would be absolutely wrong. In carrying out our analysis we encountered many difficulties and pitfalls that have not been mentioned in this paper for reasons of time.
In conclusion, however, I would like to stress one more point. In the case discussed the potential chlorine emissions were relatively small and therefore the frequency of failure could be allowed to have a rather large value. This means that most failures will belong to the class of normal breakdown failures, well known to every plant technician. Failures of this type are the easiest to predict.
If one has a system where some failures will easily lead to disaster, one has a completely different situation. The allowable frequency of an incident has to be extremely small. Normal breakdown failures cannot be tolerated and have to be designed out. In that case risk analysis is about unlikely coincidences of events leading to disaster.
To assess the hazards under these circumstances almost always turns out to be devilishly difficult. It will take a lot of time and it calls for much experience and a very fertile imagination.
Analysing risks in the way I have sketched often is time-consuming and sometimes rather tedious. But we think that the effort is necessary and that the method we use is a good one because it covers both effect and probability. For in risk analysis one should avoid the misconception that probabilities are unimportant and only effects matter.

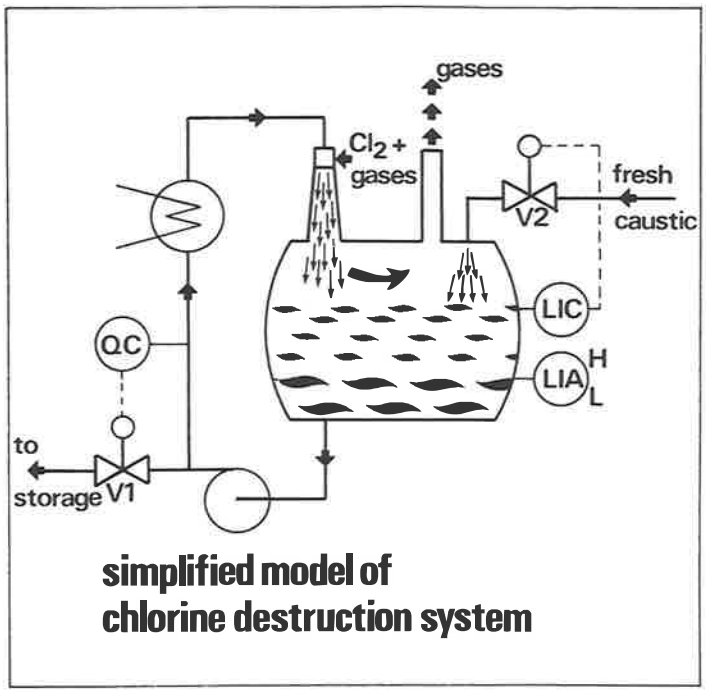


Figure 1

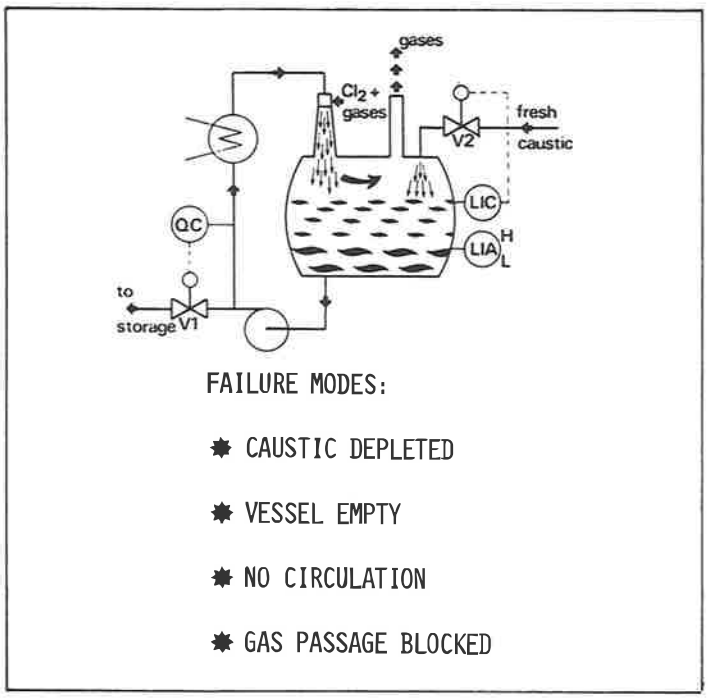
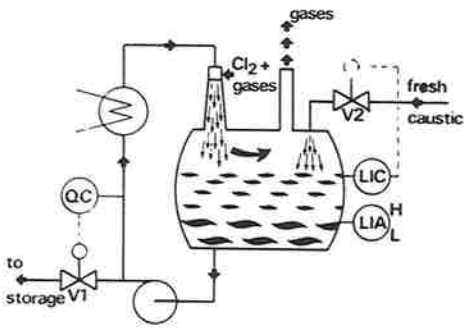


Figure 2



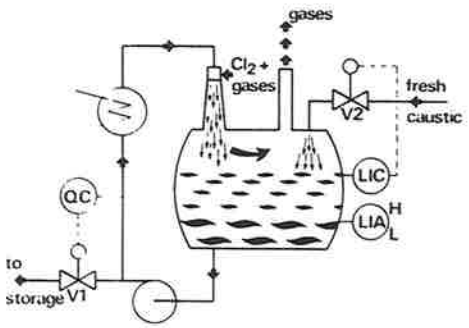
CONTROL LOOP:

FAILURE RATE	1.5 / YEAR
FAIL TO DANGER	1/3
SUDDEN	1/4

LOOP FAILURE

SUDDEN / DANGER = 1.5 x 1/3 x 1/4 = 0.12 / YEAR

Figure 3



ALARM:

FAILURE RATE

TEST FREQUENCY

$$\text{FAILURE PROBABILITY} = \frac{1/2 \text{ YEAR}}{10 \text{ YEARS}} = 0.05$$

Figure 4

PROCESS DEVIATION	OPERATOR TO ACT WITHIN	OPERATOR AIDS	PROBABILITY FOR FAILURE TO ACT (%)
RISING/FALLING LEVEL	<5 MIN	LI OR LIA	90-100
	0.5-1.5 HR	LI	25
	0.5-1.5 HR	LIA	5
	>2 HR	LI	10
	>2 HR	LIA	2
RISING/FALLING PRESSURE	<5 MIN	PI OR PIA	75-100
	>0.5 HR	PI	20
	>0.5 HR	PIA	5
RISING/FALLING TEMPERATURE	<5 MIN	TI OR TIA	75-100
	0.5 HR	TI	20
	0.5 HR	TIA	5
	>0.5 HR	TI OR TIA	5

Figure 5

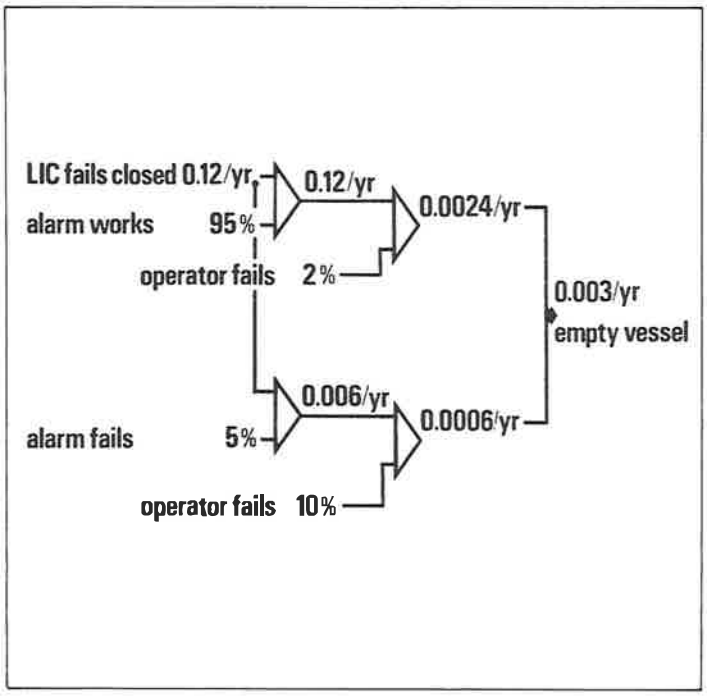


Figure 6

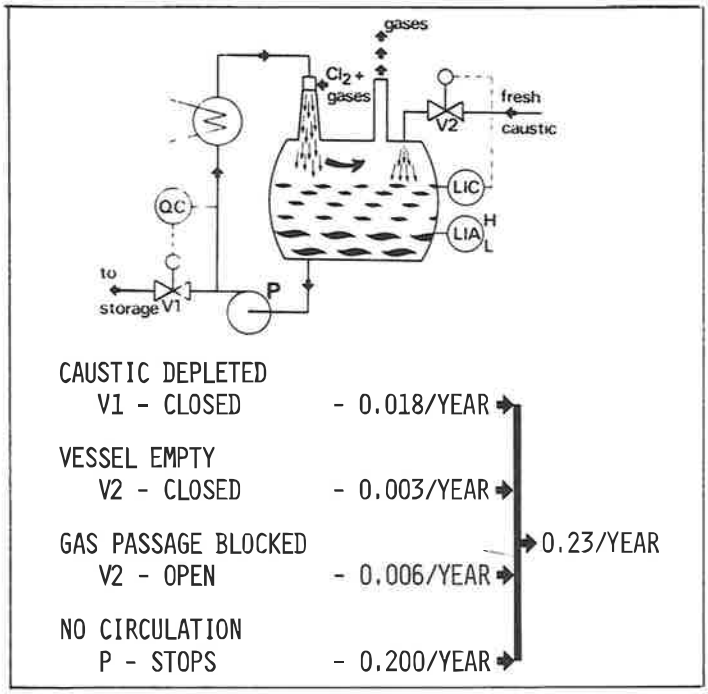


Figure 7

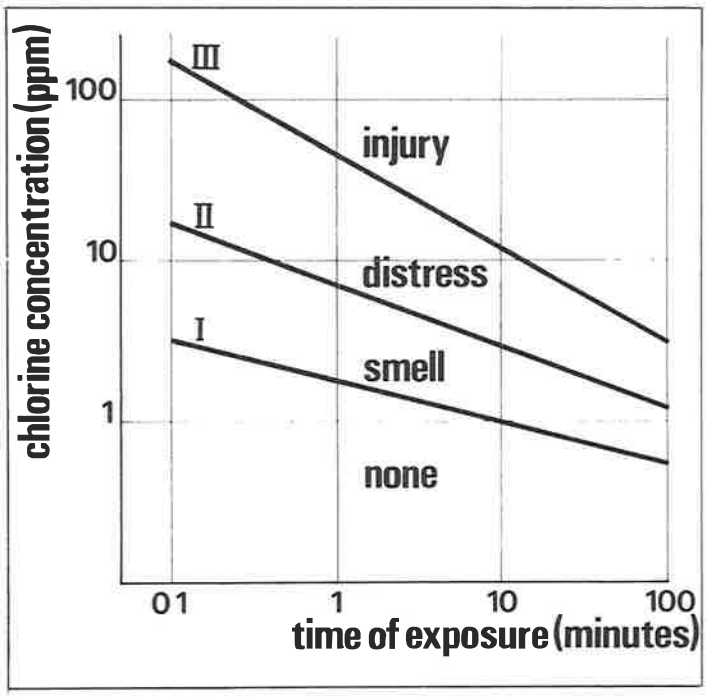


Figure 8

100 KG Cl_2
10 MIN ➧ COMPUTER PROGRAM ➧ CAT I 24 %
CAT II 69 %
CAT III 3.5 %

	FREQUENCY 1/YEAR		
INCIDENT	I	II	III
ESCAPE 0.24/YEAR	0.06	0.16	0.008
ALLOWABLE FOR SITE	1.0	0.1	0.01
ALLOWABLE FOR UNIT (20%)	0.2	0.02	0.002

Figure 9

General Aspects of case studies in Risk Analysis

Drs. J.J. Schwarz and Drs. P.G. Schipper
Central Organization TNO
Apeldoorn
The Netherlands

Being the last to present a paper at this conference, we feel that it may be of interest in trying to narrow the gap between the more generalizing papers such as those by Otway and Rowe, and the more specific ones, as for instance by Vis van Heemst. As a firm theoretical framework in risk analysis in lacking, we can only hope that it will be possible to find a connection between general knowledge based on various case studies in risk analysis - especially knowledge concerning the consequences in terms of decision making - and more general knowledge based on existing ideas. This inductive - deductive approach will give insight into some dangers related to the development of technology in general, with the drafting construction and location of technical systems in particular, and the reaction of the public to those dangers as well. The problem of societal acceptance is, in our view, very important.
Society has a growing awareness of dangers and in the last decade a number of calamities or dangerous situations have been brought to the attention of a large number of people.
It seems no longer possible to hide the problems linked to the risks inhearent in technical systems. The decision making process becomes increasingly important in this respect, especially when risks of technical systems are involved. A strong disagreement between various interest groups, and also between the authorities and the public, have the potential to undermine our democratic decision system especially if major risks are involved.

Recently it became widely recognized that technical systems frequently produce undesirable consequences in addition to the desired beneficial ones. Nowadays undesired consequences are viewed to occur to the environment of a technical system and eventually to the society as a whole.
One aspect is the occurrence of dangerous situations sometimes accompanied with damage and loss of human lives. Another aspect is a shift in societal values which calls for a (re)evaluation of the way technology and technical systems are introduced into our society.
The increase in scale and complexity of modern technical systems is responsible for the possibility that calamities may occur such as explosions or the discharge of hazardous materials into the environment.
Some believe that human efforts are not adequate for reducing major risks that find their origin in technology.
Strehlow and Baker[1] for instance, have pointed out that in recent times there is a large increase in both the frequency and the destructiveness of all types of accidental explosions. Probably the same can be said about accidental releases of hazardous chemicals into the environment. The transformation of the nuclear energy debate to the industrial production, transportation and storage of chemicals may contribute to this belief also.
Otway and Pahner[2] for instance, have suggested that the nuclear energy debate can serve as an excellent case study, because the attitude of the public to the risks of nuclear power sets, in many instances, a limit to the development of it. It is possible that questions about the safety of nuclear energy will lead to the same questions and doubts about the safety of other types of technologies, and technical systems.
There are some indications that this might happen.

- Most of the risk analysis studies of technical systems are just a few years old. So there has not been much time to evaluate the validity and reliability of these studies.
- In the Netherlands, interest groups and regulating agencies are asking for risk

analysis, in order to decide on the safety of certain technical systems. This contributes to the awareness of different kinds of risks.

- Farmer, safety advisor to the United Kingdom Atomic Energy Authority has said: "When one examines, in the detail that is currently given to reactors, the possible hazards from other industries, one gets the feeling that one should be discussing all major hazards in a country and not concentrating on one source of hazard such as nuclear. I believe that we have been isolated in the nuclear community for too long" [3].

Government, interest groups and the public will become more and more aware of the undesired effects on the physical, biological and social environment as a consequence of the various risks generated by technology.
Roughly two types of undesired effects can result. The first type of effects is based on the knowledge that a certain kind of technical system has the potential to trigger physical damage mechanisms and the second type is a result of the actual triggering of such mechanisms.
The assessment of the potentialities of undesired effects is important for understanding the reaction of people living in the vincinity of certain systems. In the first place the awareness of dangers resulting in psychological stress and fear is relevant here.
Secondly, the uncertainty as a consequence of decisions concerning risk generating technologies is enlarged by the psycho-social effects of these potentialities.
The assessment of the actual triggering of physical damage mechanisms is also subject to uncertainty because of insufficient data and inadequate methodology. If one takes this into account, then it is not surprising that most of the studies in risk analysis have been limited to an identification of the possible types of damage to man and to man-made structures (risk estimation).
Experience has taught us that the damages which can result from events with a low frequency of occurrence are difficult to quantify, so quite often the evaluation of undesired events is merely based on the imagination of the decision maker.

Besides this problem there is the problem of the knowledge and awareness of the public. If the public knows that certain risks exist, but believes in the regulating agency or the decision maker, who says that the risks are very low, then probably the public will not start worrying.
When, however, the public does not have so much confidence in the sponsor or the regulating agency and gets the idea that risks exist they don't know of, then it is possible that the public starts estimating the perceived risks itself. These risks are not estimated and weighed in the same way as the decision maker does, because the public has not sufficient reliable information and will refer to single accidents in systems that resemble the systems at hand. Generally spoken, the public is poorly trained in handling statistics. Another problem is that a certain technical system benefits certain groups or the population as a whole, while only small parts of the population will have to bear the most severe risks. Conflicts of interests may then arise, not only between groups but also between the authorities and the population. This aspect imposes special problems on the application of risk analysis because the reliability and validity of the estimations and calculations must be of a high standard.
At the moment, the public, the sponsors and the authorities differ in opinion about the safety (or the risk) of technical systems.
The risks as estimated by the public by means of intuition, information and/or experience influence the attitude of that public. Other social and cultural background factors determined by religion, education or political choice, are modifying these attitudes.
So the attitude may be different from the behaviour. Over a longer period of time, however, the attitude itself may change.
This means that it is very difficult to predict the behaviour of people who become aware of risks in their environment. Generally we can assume that the public expects that the regulating and controlling agencies will guard over their safety.
These agencies, however, have also to take into account economic and (other) social aspects such as employment. Further, absolute safety, can never be attained.
The first figure gives the relations [4] between a threat, as a consequence of certain

risks linked with technical systems, the people, who are exposed to this threat, and the authorities who have a mandate from the people to protect society against serious damage.

The task of the authorities is to make a link between the results of the risk estimation and the risk evaluation[2].
The problem is that in the past too little attention was paid to the perception of risks and to the reaction of people to threat, so that the decisions about the acceptance of risks must be inadequate from a societal point of view. On the other hand the controlling agency will ask for a quantitative risk analysis from sponsors such as industry. The industrial society, however, knows that risk analysis will not reveal all possible hazards of their technical systems. In this situation it will be of interest to discuss a few case studies in order to get more insight in the risk estimation and evaluation problems. Before we do so, however, we will look somewhat closer at the nature of risks.

The nature of risks

Until now we have used the word "risk" in an undefined sense. It certainly is a source of confusion as the word means something different to different people. It includes probability expressing the uncertainty associated with a specific undesired consequence, the type and magnitude of the undesired consequence, and the value of both of these terms to exposed people. Risks can be distnguished in many ways. One of the most commonly used is the distinction between natural and man-made risks. Both types can be subdivided into two groups. The first group contains risks which are characterized by undesired consequences in the long run resulting from undesired events, which, however, themselves are viewed as "normal". The pollution of water, air and soil for instance belongs to this group. The magnitude of the undesired consequence is locally not extremely high.
The second group contains risks which are characterized by undesired consequences resulting from undesired events which will happen suddenly. The consequences of these events may result immediately or on the long run. Typically the magnitude of the undesired consequence can locally be very high. Examples of these groups of risks are, fires, explosions, the massive release of chemicals, etcetera.
To illustrate this, let us have a look at the World's Waters. It is known that less than 50% of the total direct oil pollution results from marine operations; 45% results from non-marine operations (the use of highway motor vehicles and industrial machinery) and only 5% results from tanker casualties[5].
It is estimated that by atmospheric fallout of hydrocarbons at least the same amount of pollution reaches the Oceans. The contribution of the oil pollution of the Oceans due to different operations is given in figure 2.
If the pollution of the Oceans by oil is dangerous for the health of people in the long run, then the efforts to minimize this danger on a world-wide scale should be concentrated on the "normal" operations. In the local situation, however, tanker casualties, although responsible only for a few percent of the total oil pollution of the Oceans, receive much attention because in the local area this pollution is immediately desastrous.
As said already, the domain of risk analysis is the quantification of the uncertainties, that are associated with specific undesired consequences. As we have seen from the example given, this can be a quantification of the possibility that oil pollution of the Oceans will bring an end to life on this World or it can be a quantification of the possibility that a local area will be desastrously polluted by oil due to a tanker casualty.
It will be clear that the only possibility for minimizing the uncertainty connected with risks, is a risk analysis of technical systems in their environment and not isolated. Due to the scale and the complexity of the technology, uncertainties will be left where risks are difficult to define and to estimate in relation with the risk of the "total" system.
Further it is necessary to acquire a more comprehensive insight in the precise effects of calamities upon our society. Up till now the effects are measured mostly in terms of victims (death and wounded) and in economic loss.

However, the following effects seem also of importance here; effects on human health, social disruption and the impact on environmental quality.
These aspects make the (benefit)-risk analysis more complicated because, if they are taken into account, the effects of calamities should be weighed differently in the analysis than is done now. In his lecture V.d. Kley, for instance, pointed out that a small flood North of Amsterdam in Holland, gave a far more intensive emotional shock (although no one was killed) than for instance accidents with ships. The last type of accidents, however, may have more far-reaching consequences than the first one, in terms of people killed and environmental pollution. Another special problem is the time-lag between benefit and risk of a certain technical system or technology.
Burton, Kates and White[6] have shown that the public has a tendency to deny the risk of natural disasters, or to endow the phenomenon with a rigid periodicity. Alternatively, they may rely on authorities, who have the full responsibility, for hazard prediction.
All these aspects have a substantial influence on the acceptability of a certain technical system in a certain environment.
This means that governments have to decide about levels of acceptance one way or another. If they want to do so, then it is necessary to do research on this aspect. In order to obtain a more comprehensive insight in the risks which are (un)acceptable for society the way used most often is to compare risks. In most studies on risk analysis natural hazards are playing an important role in the comparison of risks. They are then used as an implicit level of acceptance because they belong to the "normal" risks of life.
When we make a tentative comparison between Holland and Japan in this respect, we can see that Japan suffers from more natural hazards than Holland. Due to geographical and geological conditions Japan is frequented by typhoons, heavy rains, snow falls, tidal waves and earthquakes. Over many years this has caused substantial losses, both in number of victims and in damage to property.

These losses are substantially higher than in Holland. In the flood of 1953 nearly 1800 people perished and since then only some people died as a consequence of natural events like storms, lightning, etcetera.
When we compare for instance the number of people killed in traffic accidents we see in Japan traffic accidents took 586 173 lives in 1973 with 26 million automobiles on the road[7]. In Holland nearly 2500 people were killed in accidents with 3 million registered automobiles. This gives about 1 death per 44 cars in Japan and in Holland 1 death per 1200 cars. The two countries are comparable regarding density, technological development, etc., although there are large cultural and social differences.
So the idea that there is a relationship between the amount of natural hazards and the acceptance of technological risks can only be a hypothetical one[8]. Cross cultural research has to be performed in order to obtain sufficient evidence for this relation. If this relation exists, however, then decisions about the acceptability of risks have to take into account these types of unconcious acceptance levels as well.
The comparison of technological risks with natural hazards, the last ones used as a norm, neglects the dynamic character of societal acceptance however, so research on this subject has to be performed regularly. Other acceptance levels based on comparison are, for instance, the categories voluntary - unvoluntary, history, different types of technological risks, costs-effects, etcetera.

Case histories

In order to obtain more insight into the problems we have mentioned, two cases which have been studied by TNO, will be discussed. Furthermore we will devote some attention to the Flixborough disaster.
All cases have in common that contradictions have resulted as a consequence of different opinions about the acceptability of potential or actual triggering of the physical damage mechanisms.
The first case is about a risk analysis study of a rail-yard where trains loaded with various hazardous materials, such as chlorine, LPG, gasoline, etc. are switched.

The second case is the Flixborough disaster.
The third case is about the risk problems of a large office building situated near a gasoline storage area, a canal and a highway.
For the sake of clarity we will state here that it is not our intention to give a detailed description of the analyses performed. We are interested in the general aspects, which can contribute primarily to a better understanding of risk phenomena in our society.
The first case is about the problem of risk reduction of train switching. Near a large city in the Western part of Holland lies a railyard where cargo trains are combined. Some of these trains are transporting hazardous materials, such as chlorine, gasoline, LPG, etc. Because a very densely populated city lies in the neighbourhood of the existing rail-yard, the State Railroads have planned a new yard at a larger distance of that city.
This also gives the opportunity to modernize the switching system by automatization, so that necessary switching with dangerous materials can be executed is a safer way.
The problem was, however, that the local authorities of the town where the new terrain will be situated had plans for the extension of the building area. The distance between the building area and the new railyard would be too small to avoid certain risks.
The study was aimed at an estimation of the risks for people in the new building area as a function of the distance from the rail-yard. To enable the authorities to maintain a situation for the built-up area as safe as possible, the following generalizing conclusions were obtained from the study:
- It was possible to determine a minimum distance between the rail-yard and the built-up area for a few types of effects only such as fires, explosions, etcetera. For other types of effects (toxic vapors for instance) it was impossible to determine a safe distance.
- More than formerly the potential dangers to people in the surroundings, were investigated in this case. Because other kinds of risk in the area appeared to be unknown, it was impossible to estimate the risks of the rail-yard relative to the other kinds of risk to the population.

As to the methodology, the following problems had to be faced when we tried to quantify the risks.
- Data about past activities had to be used to predict activities in the future.
- Individual bias in the interpretation and identification of damage mechanisms, may result in the neglection of "less important" factors.
- The necessity to reduce complexity, in order to be able to handle the problem.
- The use of data which are not reliable enough for the correct estimation of the probability of rare events. This leads inevitably to results that are less certain and accurate than one may wish to obtain.

The next case is the Flixborough disaster.
Two commissions were installed to investigate the explosion of a caprolactam plant of Nypro in Great Britain in 1974. The first tried to find the cause of the explosions and came to the conclusion that a temporarily by-pass, which was installed a few month's before the disaster, could not withstand all the pressures and temperatures, used in the process. The second commission was given the task to study whether new regulations ought to be drawn up to prevent major industrial hazards in the future. The last commission produced a list of eight types of installations, which by virtue of the product, technology or scale of operations, could constitute a major industrial hazard. These types of installations are now called "notifiable installations". Many of the problems encountered go far beyond matters of legislation. Prof. Harvey, chairman of the second committee said that these installations raise the question whether certain technological developments are intrinsically unmanagable and whether society should do without them and take a pace backwards. The report of the first committee, reveals also the uncertainties linked with the prevention of disasters. The report says that the disaster is a consequence of mistakes having a very low probability, made at the drafting and construction of a change in the installations. Such a combination of mistakes will probably never happen again.
The mistakes were not only made in construction but also in the field of management. The lessons to be learned are many. They are varying from the notion of the lack of

suitable data about industrial installations and about explosion of unconfined vapor clouds, to a total re-evaluation of risks connected with the use of risk generating technologies.
The only valuable conclusion is, that we know far too little about the dangers of these installations, and that we only can make a plea for better data, and make some arrangements to prevent equal or worse consequences in the future.
The last case is a very interesting one.
It started with the refusal of civil servants to accept a new office building that was located at a distance of about 200 metres from a gasoline and refined oil storage with 17 tanks. After that a special committee advised about research which would give more insight in the impact on the building of an explosion of a vapor cloud of gasoline. When such an explosion happened then the construction of the building might be affected and the windows on two sides of the building would be smashed. Pieces of glass would be blown into the building.
The most interesting part of this case is, however, that it is the first instance of laymen having made their own risk assessment, and that they have concluded that this risks are unacceptable. Also of special interest is that the refusal of the civil servants is largely based on knowledge of the effects of an explosion of a gasoline vapor cloud in 1974 at Roosendaal in Holland.
It is also surprising that these people pointed at other types of risk they were exposed to, namely the risks connected with the bulk transport of hazardous materials by road and on the canal, which is almost on the doorstep.
If we look at figures 3, 4, 5 we can see that the amount of chemicals transported in bulk by water and by road have increased substantially since the mid-sixties[9].
So it might be that these two aspects are more important for the assessment of the risks people in the building are exposed to in the future than is expected now.
Safety measurements have been prepared to reduce the probability that a substantial amount of gasoline will flow out of the tanks. The reduction of the effects will be difficult because the tanks are located close to each other.
The safety measurements taken are:
- inspection of the welding of the storage tanks
- safe-guards to prevent overflow of gasoline from the tanks
- no filling of tanks during very stable wather conditions
- warning system inside the building so that the people can be evacuated in time.

The formulated wish by the representatives of the civil servants to locate the fuel storage elsewhere will not be effected.

Conclusions

The three case-histories gave us some information that may be generalized to a certain degree. From description of the reported cases it can be seen that various aspects of acceptability deserve a closer look.
It can be confirmed that the acceptance of risks by interest groups is highly influenced by knowledge of previous accidents. This accounts for specialists as for laymen as well. This means that with regard to the acceptance the potential of undesired effects is as important as the actual occurrence. There are also indications that often natural hazards are used unconsiously as a basic level for the acceptance of man-made risks on a societal level. This approach neglects the dynamic character of societal acceptance, however. Concerning the weight of effects it is necessary to change the definition of calamities or disasters which are nowadays mostly defined in terms of the number of fatalities and the economical value of loss.
Other effects as human health, social disruption and the impact on environmental quality, also in the long run, must be taken into account as well. Most of the latter effects of a disaster are difficult to estimate and are complicating the risk analysis. The cases discussed reveal a tendency to simplify the estimation and evaluation of risks however. So it is not surprising that strong disagreements exist about the scientific and societal usefulness of risk analysis.

To sum up it is necessary to give quite an effort to improve the method of risk analysis and especially to aspects concerning the acceptability of risks.
If we want to reach this end then it will be necessary to improve the methodology of risk estimation considerably, to give more attention to risk evaluation and to search for new technologies which have a less hazardous character.

REFERENCES

1. Strehlow, Roger A. and Wilfred Baker
"The Characterization and Evaluation of Accidental Explosions"
NASA-C.R.-139 779 (june 1975)

2. Otway, Harry J. and Phillip D. Pahner
"Risk Assessment"
Future, April 1976. 122-34

3. Farmer, F.R.
"Letter to the editor: Risk Quantification and acceptability"
Nuclear Safety vol. 17
no. 4. july-august 1976. 418-21.

4. Schwarz, J.J.
"Veiligheid als maatschappelijke waarde" in:
Afsluiting van de Oosterschelde, een open vraag?
Congresmap Practische Studie Delft, 7 april 1976

5. Cash, Don E. et al.
"Energy under the Oceans, A technology assessment of Outer Continental Shelf Oil and Gas Operations"
University of Oklahoma Press 1974, Appendix B. 275-309

6. Burton, I., Kates, R.W. and White, G.F.
The Human Ecology of Extreme Geophysical Events
Natural Hazards Research Working Paper no. 1 University of Toronto (1968)

7. Takei Isao
"The State of Risk Management in Japan"
Risk Management July 1976, 53-6

8. Schwarz, J.J.
Maatschappelijke Aanvaarding van Technische Risico's
TNO-Project 1. 1975, 11-17

9. Hoeven, Erik van der, Bert Nieuwpoort en Jan van Hal
"Wanneer komt de Grote Klap?"
Milieu Defensie no. 1, Februari 1977, 22-28

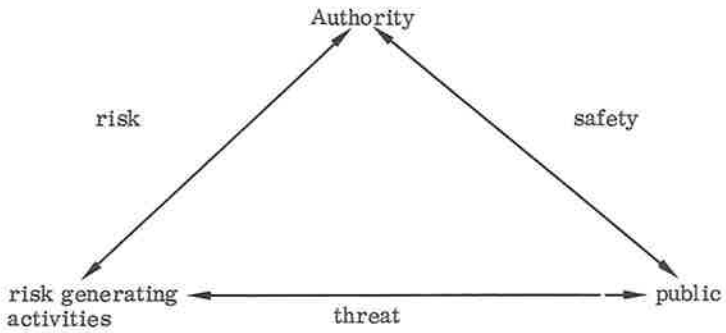


Figure 1. Relations between risk generating activities, public and authorities in connection with hazards

estimated annual direct and indirect oil pollution of the world's waters (1969-1970)

source	volume (barrels)	percent of total direct pollution
marine operations	16,100,000	46.1
non marine operations	17,400,000	49.9
offshore oil and gas operations	1,400,000	4
total direct pollution	±35,000,000	100
atmospheric fallout	63,000,000 to 630,000,000	
total oil pollution	98,000,000 to 665,000,000	

source: energy under the oceans 1973

Figure 2.

lives and assets claimed by past accidents by force of nature

	1966	1967	1968	1969	1970	1971	1972
lives lost	628	607	259	183	249	348	637
asset losses including public civil facilities, farm land, farm products and other (in hundred million yen)	3,308	3,694	2,331	2,916	3,452	4,972	7,720
(u.s. million dollars)	(1,102)	(1,231)	(777)	(972)	(1,150)	(1,657)	(2,573)

source: "bosai hakusho" or white paper on loss prevention, 1974 ed. p. 272-273

Figure 3.

transportation (bulk, containers etc.) in holland in million tons

category	year	total	waterway	rail	road
oil and oil products (refinery)	1965	27,2	12,6	2,6	12,0
	1970	37,3	11,5	2,3	23,5
	1971	36,1	11,5	2,1	22,5
	1972	36,5	12,0	2,0	22,5
	1973	40,8	12,4	1,9	26,5
	1974	35,1	10,5	1,7	22,9
	1975	-	8,9	1,6	20,3

source: m.d. - febr. 1977

Figure 4-1.

transportation (bulk, containers etc.) in holland in million tons

	year	total	waterway	rail	road
fertilizers	1965	6,5	1,8	1,0	3,7
	1970	6,8	2,5	0,4	3,9
	1971	7,1	2,8	0,5	3,8
	1972	7,5	2,9	0,7	3,9
	1973	7,1	2,9	0,6	3,6
	1974	-	2,6	0,7	4,4
	1975	-	2,4	0,7	3,5

source: m.d.-febr.1977

Figure 4-2.

transportation (bulk, containers etc.) in holland in million tons

	year	total	waterway	rail	road
chemicals	1965	11,0	0,8	0,9	9,3
	1970	19,9	1,6	0,9	17,4
	1971	20,5	1,6	0,9	18,0
	1972	20,8	1,3	1,0	18,5
	1973	21,1	1,6	1,1	18,4
	1974	-	1,9	1,0	20,4
	1975	-	1,7	0,9	19,9

source: m.d.-febr.1977

Figure 4-3.

PANEL DISCUSSION

Panel

Ir. A.W.M. Balemans, chairman
J.E. Bannister
Ir. H.J. de Heer
T.A. Kantyka
J.T. Kopecek
Dr. H. Otway
W.D. Rowe
Drs. J.J. Schwarz
Ir. M. Vis van Heemst
C.S. Windebank

(Balemans) As you see, nearly all speakers are in the panel, with the exception of Mr. Van der Kleij. He asked me to excuse him and he explained that he had three meetings today. That is also a kind of risk, he said.
The groups have formulated a large number of question, and I doubt whether we can answer all of them. They are extremely varied and cover many aspects of risk analysis. This clearly indicates, I think, that quite a number of problems in risk analysis are unsolved or only partly solved. Therefore, I do hope that you will not get the impression that everything is known already, but rather that there are still many things that can be investigated fruitfully and that you all can add to the store of knowledge and experience. For if we look upon risk analysis as a continuous part of the control-system for activities, then we will never solve all problems connected with it, as it will change in the course of time to follow the changes of a dynamic society.
Quite a number of questions clustered around the concept of acceptable risk. May I ask you, Dr. Otway, to start giving an answer to this cluster of questions? By the way, will all members of the panel be so kind to read the question or to summarize the problem that has been put forward?

(Otway) Thank you Mr. Chairman. I am ashamed to say that I cannot find the question I had selected, it must be in my pile but it got lost somehow. While I am searching, let me make some general comments that may make it easier to interpret some more detailed answers later on. Many of the questions show a concern with the product of risk assessment studies. They ask: How accurate are the results? Does the accuracy justify a study? Do people believe the results?
I would like to suggest that risk assessment, at the present at least, should be viewed as an interactive, multidisciplinary process. The insights it provides and the assistance in understanding both technological and social systems, are the product. The important thing is the process of doing it and what one learns by doing it, numbers are not yet an important part of risk assessment studies. In other words, many of the questions show a dichtomy between product and process, and the product is not the important part yet. I would say that risk analysis should be thought of as a set of methodologies for aiding the making of better decisions, and certainly not as a method for mechanically making decisions.
In the meantime, I have found the question, which runs: "What does the panel think about the possibility of arriving at some simple numerical criteria for the acceptability of risks? For one can estimate a risk and say simply: 'Will this risk be acceptable or not?' ".
In view of the general remarks I have just made, it will surprise no one, I think, if I say that in my opinion the probability of arriving at simple criteria is very small. So the answer to the question is: No, it probably cannot be done. The reason is that the acceptability of risks is a difficult concept because the acceptance of risks by the public is an extremely complex phenomenon. It is determined not only by the statistical estimates we make, but also by psychological factors. Do people feel that they have

given their consent to being exposed to a risk, do they have some control over the outcome, may effects be delayed, are there implications for social structural changes? And so on. I think that each risk situation will have different criteria for acceptability.

(Balemans) Thank you. Does Mr. Rowe want to add something?

(Rowe) I think I should re-emphasize what Dr. Otway has said, that we have a process and a decision that comes out of the process. These are two wholly different things; I don't think we will ever have a process where we simply turn a crank and out come all the answers. The purpose of the process is to illuminate all factors that can affect what we are trying to do - the mechanical things, the projects etcetera - to identify what the risks are, and also to understand how people look at risks as individuals, as groups and as society as a whole, and to understand how they react to risks. The only model we have are the people, so our information must come from looking at people and how they react, trying to understand what the motivations behind their actions are, and whether they are concious or unconcious.
What I am suggesting is that the methodology is a means of bringing all this knowledge together, so that we can study it as a whole. Then we can identify what we think are the critical parameters; there are usually only a few. We then provide our insights and opinions to the decisions makers. They have to combine our insights and critical parameters with other aspects that may be political, economic or personal. They have to melt all this into a value judgment and they have to show people what they have done.
The question at the bottom of quite a lot of queries about risk analysis is, I think: "Why do we go through with this whole process and spend a lot of time and money on it?" In my opinion the answer is that we have no choice anymore, we have to come up with credible answers. If we don't, the decisions we want to take will be held up or we may have people going to sit-ins trying to block our decisions. What we are and should be trying to do in the process is to make the pathway to the solution apparent, credible and visible. When the decision maker has made his decision, the process will have given credibility to whatever his decision is. Then everybody will agree with it. Credibility is the most important, and we can have credibility only if we come up with credible answers arrived at by a pathway that is visible to all.
If I were a witch doctor in a small native society and somebody came to me with a big question and I went into my dance and incantations and wild gyrations, and came up with: 'This is right' and everybody walked away saying that they agreed with me, then I would be a successful risk analyst in my society. Well, we must be successful risk analysts for each of our countries, but we must do this with different kinds of incantations and gyrations. However, instead of making these secret so that only the witch doctor can mumble them, we must make them visible, as all of us want to be able to mumble them.

(Balemans) Thank you Mr. Rowe. It always is a pleasure to hear you giving a popular account about what risk analysis is really about.
I think that Mr. Vis van Heemst also has a question on acceptable risk, in his case on occupational and public safety.

(Vis van Heemst) The question is: "Should there be different standards of risk acceptance for those within industry and for the public outside?"
Well, the answer is: Yes! When a new plant is built, the public outside the boundary should not be exposed to additional hazards. They did not ask for it and often, they will not have any direct benefit of it. There may be indirect benefits, but that should not enter your considerations when you investigate risks.
Inside the boundary the hazard level is usually expressed as FAFR, which means Fatal Accident Frequency Rate. A FAFR of one means that there is one fatal accident in 10^8 hours of being exposed to that particular situation. 10^8 hours sounds a bit arbitrary, but the number is based on the following computation: If you have a factory with 1000 employees who work there for forty years continuously, five days a week and eight hours a day, then the summed total of their working hours is about 10^8. In general the

FAFR of a plant will be about 4. For people outside the boundary, the risk should be a hundred to a thousand times lower, and then the probability is comparable to that of being stuck by lightning.

(Balemans) There were so many questions about this subject that I think we should still go somewhat deeper into acceptable risks. Mr. Rowe, I am not asking you as an employee of the US Environmental Protection Agency to set limits for the Netherlands, but could you say something about figures for acceptable risks? Are there any figures?

(Rowe) I don't know. I think the acceptability comes through the process. As I mentioned before, in my book I have tried to develop an applied methodology. The important point is not that I did it, as I am sure that people who are smarter than I am, will do it better. Important is that it turned out to be possible to do it. For now you can show people what the problem was, how you tackled it, what you did and what you did not do. And I think that acceptability and acceptance comes out of that process. I do not think that there are any set levels of acceptability unless you go down to what I would call 'thresholds' of acceptable risks. These thresholds are the things that are completely uncontrolled, that man has no power over, such as the probability of the sun exploding or the probability of being hit by a meteor while walking along the street. And there you are down to levels of 10^{-13} per individual per year. If you put this fatality rate into a life table for 100,000 people, for example, and work out the average life-shortening caused by this additional risk, it comes out to be just one second. I suspect that all of us are prepared to live with a reduction of one second of our lives. The real question, however, is how much higher are we willing to go for the particular benefits that we gain. So in each case it is a balancing, first of direct costs and benefits, then a balancing of indirect costs and benefits for society. Then we have to investigate what can be done to reduce the risks to a level that seems reasonable to us and then we have to say: "Who are we, putting risks on people who are not getting benefits out of it appropriately". All we can say is that the risks have been taken care of the best we can, but that is never perfect. In other words, I don't think there is one general number for acceptability.

(Balemans) Thank you, Mr. Rowe. Then I have a question here that runs: "Is there sufficient evidence at present to permit political discussion of risk acceptance?" Before asking one of the members of the panel for his comments, I think I should say something about this, not only as the chairman and a member of the panel, but also as a civil servant.
In the question the word evidence is used and this will suggest to the unwary that political decisions are taken with as much objectivity as is possible. This is a very optimistic outlook upon reality. Those with first-hand knowledge of political decision making know that facts, and even hard facts often play a relatively minor part compared with emotional considerations. Science, including the discipline of risk analysis, should help to prevent that political decisions are being based exclusively on emotional considerations. Don't conclude from this that I am against emotions in politics. Politics is about people, and deciding on the fate of people without any emotional involvement is both extremely dangerous and wicked. In the ideal situation, however, there should be in policy making a healthy balance between facts and emotional considerations.
I'll illustrate my remarks with two examples of recent decisions taken in the Netherlands. My first example is the decision that has been taken with regard to a nuclear power station. As is well known, the problem of nuclear power is not only safety - all over the world the nuclear power industry has an excellent safety record. In my opinion the most important problem is radioactive wastes, that will have to be stored for at least 10,000 years before their radioactivity has become harmless. Nobody can take responsibility for what will happen in the next 10,000 years.
According to the decision taken by the regional authority called 'Rijnmondraad', a nuclear power station should not be build on the Maasvlakte - to the south of the Hook of Holland - since this is a high risk area already. At the same time the construction of a nuclear power station on an artificial island off the coast was thought to be a good pro-

position. In my opinion all this is based on faulty reasoning as it does not square with the facts known about nuclear energy. It was a political decision based on emotional grounds and not on facts.
My second example is the whole decision making process with regard to the closing of the Eastern Scheldt. After the disastrous flood of 1953, the Delta Act was drafted and passed Parliament in a remarkably short time. It stipulates that the northern three of the four arms of the Rhine-Scheldt estuary shall be closed by dams, the Haringvliet by one with sluices and the other two by dams without any openings. The decision to dam up the estuary was taken twenty years ago and was partially based on facts, as the civil engineers said that closure would be difficult, but could be done. But for the most, it was an emotional decision as the country still was deeply shocked by the terrible loss of life caused by the 1953 flood. It should be remembered what Mr. Van der Kleij stated in his paper yesterday: Every flood in Holland is treated as a national disaster, even when there is no loss of life.
The Delta Act also lays down that secondary dikes will have to be constructed higher up, to control the currents. When the two northernmost closures and the secondary dikes had been effected, no dirty Rhine water could enter the Eastern Scheldt anymore, which quickly became clean again and turned out to be an important ecological resource. Political parties, action groups and nature conservancy agencies stepped in and started arguing that the original decision had been taken twenty years ago when there was no appreciation for ecological values. The government wisely decided to re-open the discussion and appointed a Committee, which came up with some highly original solutions. Then the country turned again to the civil engineers, who said that the proposals of the Committee could not be carried out, but that it would be possible to effect closure by a pillar dam that would allow a damped tidal movement in the Eastern Scheldt. The government accepted this advice and took the decision to build the pillar dam. I think that the political decision taken in 1976 was based less on emotional grounds and more on factual information, in this case ecological and risk information.
Having said all this, I now turn to Mr. Schwarz to ask him whether he wants to comment on the original question.

(Schwarz) I would like to add that I have the impression that members of parliaments are confronted more and more with very deep and difficult problems and that they often do lack the expertise to handle these problems adequately. I think that this is very serious and strikes at the roots of our democratic decision system, for it means that chosen representatives of the people are not able anymore to weigh and judge upon these difficult societal problems. Still they have to do it, and it is not surprising that they will tend to rely more on emotional than on factual considerations. Still, there is the example of the United States, where Congress insisted on the creation of the Office of Technology Assessment (OTA). When a difficult problem comes before Congress, the experts of OTA study it and dissect it in a report that can be understood by non-experts. In this way the members of Congress have regained their ability to judge upon even very difficult questions that cannot be understood without the help of the expert.

(Balemans) Thank you Mr. Schwarz for your important remarks on this subject. Mr. De Heer has a totally different subject in his pile, as I think that one of the groups voiced some doubts on the statistics on data and components.

(De Heer) The question is: "How meaningful are the final results of risk-analysis in view of the following doubts:
a. Should not the data on component reliability represent the efficiency of their maintenance instead of the reliability of the components?
b. The input of the effect of the known element is based on very incomplete knowledge."
As to the first part of the question I can be very short; this is treated in my paper. You may remember that I defined the failure rate as the number of failures observed in a certain time, divided by the time T. In that rate the effect of maintenance is included.
About the second part I could say that I would not like to be quoted as having said it.

Still, there is an element of truth in it as sometimes you are not sure about your input data. Then you can do a sensitivity analysis. You vary your parameters and see whether the results show a large spread or not. If they do, probably you will need better input data. And in some cases it does not matter at all whether your input data are relatively incorrect, because you are working with very small numbers indeed, 10^{-4} or 10^{-5} for example. Often it will be sufficient if your order of magnitude is correct, as it does not matter at all whether you come out at 2.10^{-5} or at 5.10^{-5}. Of course this depends on the situation.

(Balemans) Thank you Mr. De Heer. I turn again to Mr. Rowe, who has a question on the same subject, I think.

(Rowe) Yes, I have a question which is very long and detailed, and not wholly clearly formulated, I fear. I will be able to answer some parts of it, the others will have to be answered by Dr. Otway, I think.
Let me take out the general parts to begin with. Then first we are asked: "How far is the present way of handling risk estimates and risk analyses?" Then there is a part saying that methodologies used for solving complex societal problems usually are very complex too. And further on there is: "The quantitative methods are often difficult to understand and to interpret, even among experts, and the public often questions the data bases."
The first part is unanswerable as we can answer that only when we have come to the end of the road and can look back. Then we can say, perhaps, in 1977 we were that far and in 1967 we had not started at all.
The second part contains a notorious misunderstanding. Methodologies cannot solve problems! Problems are solved by human beings! These methodologies only provide a framework in which to view the problem. The information is put into perspective and made visible. There are no buttons you can push or cranks you can turn, and out come all the answers. As I said yesterday, you are working with imprecise data, so you can not expect precise answers, and the results will only be numerical to a limited extent.
And on the third part of the question my answer is: Who would deny the right of the public to question the validity of our methods and data bases? The public has a perfect right to question everything we are doing. They can be right or they can be wrong. If they are wrong, it is our task to make visible why, and if they are right, well we can only roll up our sleeves and say: Okay, you were right, we will do it again, now using your method.
Dr. Otway, do you like to comment on what I have just said?

(Otway) No. I completely agree with you.

(Rowe) Let us go on with the specific parts of the question.
"Otway indicates that statistical analysis, such as the method used by Starr, applied to risk evaluation, does not lead to valuable results. We would regret a total rejection of the Starr-method and its replacement by the attitude approach, as Starr more or less feeds in an objective yard-stick or criterion, which sooner or later could influence the psychological reaction of individuals and communities."
Let me say that this probably the best information we have: what society is actually doing and what society is. In the absence of better information I personally agree that we ought to use it to the extent possible until we have a better criterion. That better criterion might come from attitude studies, but whether that will change public opinion is another question. I do not believe that we can change public opinion, I think that we can make things visible and let people judge for themselves.
Dr. Otway, would you like to comment?

(Otway) I would both agree and disagree in a modified way. One of the things I mentioned yesterday is that there are essentially no objective probabilities. If we leave out the experiments with the perfect machine that one reads about in textbooks, we can say that there is an element of subjectivity in every probability estimate. There is also subjectivity in so-called objective analyses and there is some subjectivity in just re-

cording the data. We do put in subjectivity when we analyse the data, for example, the point I was trying to make yesterday was that in order to get risk-benefit data from national statistics, one has to make assumptions. Equally reasonable people with the same data can make assumptions that differ an order of magnitude or so.
I agree that one can get some information out of the statistical data, for example if you are proposing a new risk with a level of 10^{-2} per person per year, you can see that this is not in line with existing risks. I think that the limitation of statistical analysis is that it provides interesting background information - I would not advocate to throw it away altogether - but that you cannot expect to get at the underlying determinants of risk acceptability.

(Balemans) I think there was a second part to the question.

(Rowe) Yes, there is. It says: "Rowe indicates that risk is not the simple product of probability and consequences and even the consequence is not independent of probability. This probably stems from the fact that it is a five step approach from cause of event to consequence value. He has not clearly separated the risk estimate part of the excercise from the risk evaluation part, including perception, unlike Otway. This approach may render more difficult the comprehension of risk assessment."
Looking at my five step approach of extimation, I believe that there are consequence evaluations on a subjective level just in estimating what the risk is, and there are also subjective evaluations when you come to evaluating what the risk should be. They appear in both places, and I am very specific when I say that they <u>appear</u> in both places. This complicates the comprehension of risk assessment, but I have never said that risk assessment was simple.

(Balemans) Thank you Mr. Rowe. There is a question about not forgetting things and items in risk analysis which, I think, could be answered by Mr. Kantyka.

(Kantyka) The question runs: "How does one minimize the risk that one forgets some items when carrying out a risk analysis?"
The technique which I mentioned in my paper is an extremely thorough and systematic process. It takes considerable time to analyse even a small part of a plant and it is carried out by a group of people taken from different disciplines. Every aspect of the plant is taken into account and the proces is repeated in a slightly modified form at different stages of process development, design and operation. So there are several chances of spotting a hazard. And every time a modification is introduced, the process is repeated, so I think that the technique is using such a fine net that it is highly unlikely that any fish will escape it.

(Balemans) Thank you Mr. Kantyka. Mr. Otway also wants to say something on the subject.

(Otway) I fear I am becoming repetitious, but I want to add something. An important part of the process is to help identifying and isolating all these consequences and to minimize the number that get by. It is not necessary to assure that you have them all, as you are carrying out the excercise in order to learn about them.

(Balemans) Thank you. Mr. Vis van Heemst has a question about small changes and the introduction of new pieces of equipment.

(Vis van Heemst) Yes I have and answering it is rather difficult as I don't see exactly what was meant. If the question aims at the introduction of a completely new type of equipment, about which no data are known, then the situation is rather difficult. I think you can use two strategies. First, you can make the most conservative guess you can and start from that. Second, you can try to break down the thing into parts and make a risk assessment on each of them.
If the question aims at repairs, then again it is difficult to give a general answer as the

most important source of hazards is human failure. This is far more a management problem, as management will have to decide how many checks are necessary before the plant may be started up again after a repair.
A third possibility is that the question aims at a permanent change in your plant. Then I agree with Mr. Kantyla, who has just said that you should repeat the process and assess the hazards anew.

(Balemans) You were speaking about human failure, and there is a question about that. May I invite Mr. Kantyka and Mr. De Heer to answer it?

(Kantyka) We are asked: "It is readily admitted that human beings are more or less unreliable. Does this imply that the solution for complex and hazardous operations is full automation?"
Well, complex and hazardous plants have already a high degree of automation, otherwise their safety would be very much impaired. I don't think one could entrust the operation of hazardous plants to ordinary operators. By increasing automation we reduce the number of operators and hence we reduce the chance of human error. Of course, at the same time we increase the number of maintenance engineers and fitters, and therefore we are transferring the chance of human failure from one group to another. If you disregard costs for a moment, then it is clear that a line must be drawn somewhere. Where you draw the line depends on the confidence you have in your operators and the confidence you have in your maintenance engineers and fitters.

(De Heer) Mr. Kantyla has just said everything I wanted to say and I agree completely with him. I would like, however, to emphasize that you cannot banish human failure from your plants. If you automate, you get an inhaerently safer plant, but human error will rear its ugly head again in maintenance. So I would like to repeat what Mr. Vis van Heemst just said: With respect to safety, risk and hazards, one of the most important task of management is to decide upon the number of checks that have to be carried out after you did something with your plant that falls outside normal operation.

(Balemans) Thank you. When we are talking about safety, I think that Mr. Kopecek has a number of questions about the LNG study.

(Kopecek) One is: "Did you consider the possibility of the vapour cloud exploding?" Yes, we did. We looked at the experiments of the US Coast Guard and at the experiments carried out in Britain at the Thornton Research Centre. We have concluded from the results that it is almost impossible to detonate an unconfined methane vapour cloud. Recently, we completed a theoretical study to see whether we could shock up a methane cloud in such a way as to cause detonation. Theoretically it may be possible. But in case of an accident we don't believe that you will ever reach a condition whereby an explosion will occur.
In the same vein is the question: "Did you consider the grounding of the tanker as it comes into Los Angelos Harbour?" Yes, we did. Fortunately, the bottom of Los Angelos harbour is nothing but mud and beer cans and we found that at the speeds the LNG-tanker will be going, the stresses imposed on the hull after grounding will not be sufficient to cause any spillage of LNG. It is a double hull vessel and we have calculated that it is about 50% stronger than comparable single hull vessels.
A very important question is: "Did you consider the probability of sabotage?" Yes we did. Sabotage is a very serious initiating event possibility and it was identified quite early in the study. But since it is an act committed by humans, it is extremely difficult to quantify. So we designed a very extensive and elaborate protection system for the terminal, and I am not at liberty to reveal it. We think that this protection system will keep out most if not all saboteurs.
The last question I have here is: "How did you convince the public in the Los Angelos area that the operation as proposed is safe?" Let me tell you that there are 34 permits that must be secured before the terminal can be build. They range from Federal permits to one from the local Fire Department. We have briefed each and everyone of

these groups very carefully on what the risk assessment study yielded. We have discussed the magnitude of the risk. We have talked to other groups aside from these regulatory bodies to answer their questions if they had any. It has been a democratic process all the way and although it has been said that the democratic system is the wordt form of government, I think it is better than the next form.

(Balemans) Mr. Rowe, there still is a question about reduction of events.

(Rowe) "What does the panel prefer to do? To reduce the consequences of an event or to reduce its probability?" Well, I don't think there is a general answer. Personally I think that you first have to decide whether risk reduction is warranted. Then you have to look at the particular situation. In some cases you might be able to reduce the probability, in others you might be able to reduce the value of the consequence, which as I said before, is not necessary the size of the consequence.

(Balemans) There is a question about communication between the public industry and government. Mr. Schwarz, would you try to answer that one?

(Schwarz) It says: "What is the best method of communication between industry, the public and the government on the subject of risks of industrial activities, and is there anything known about the results of the various methods of communication?"
I could be very short about this, as I don't believe there is a best method. All methods that give the results that you wanted to achieve, are best. We can delve somwhat deeper and try to identify the channels through which the information flows between industry, the public and the government. We have more or less formal channels, such as political ones (parties and so on), newspapers, television, the wireless etcetera, and we have more informal ones - gossip and rumour. But we don't know what kind of information flows through each channel nor how the information in these channels influences the public.
What is really meant, I think, is: "When should industry use these channels of communication?" Often communication begins only after something has happened and then it is far too late. After something has happened, no one can give the right information anymore, no one can correct false information anymore, because everyone is saying: This has happened and it clearly is the fault of X or Y.
So if a certain industry is a source of well identified risks, the public should be informed as early as possible, and long before anything has happened. Then the information flow to the public should not be a haphazard affair, it should be done continuously. I know that it is easier said than done. We have had some examples in Holland, for instance the discussions about the future of the Waddenzee and about industrial islands. I think this is the best way to do it; one should not wait till something goes wrong or until decisions cannot be reversed or adapted. Still, there can be difficulties and uncertainties. Sometimes, it is not wholly clear what information is available or how the public will select among the facts that are presented to them. It is also very important to have some idea of the emotional load the information will impose, as it is not only a cognitive process, emotions are involved too. Another important point that should not be overlooked, is the credibility of the man who is giving information. Does he have the confidence of a large number of people, and is he independent to a certain extent? So I think that, if you give information about controversial subjects, the best way to do it is to be open and honest. You should look for emotional reactions, as these often point to anxieties, and you should try to remove these anxieties whenever possible. If you keep all information from the public and something happens, then you will get the conflicts I mentioned in my paper this morning.

(Balemans) Thank you Mr. Schwarz. I feel that the art of communicating with the public should be developed further as fast as possible. When you don't show what you are doing now, your decisions will not be accepted in the future.
Mr. Bannister, I think you had another question about confidence?

(Bannister) It is a question about politicians and their confidence level. It is rather personal and says: "Mr. Bannister has little confidence in experts, but can he say a few words about the confidence level of politicians?"
The first thing I ought to do, is to say that I did not say that I had little confidence in experts. What I did not like was the idea of experts being left to take the decisions. As I see it, the role of an expert is: first helping to solve the problem and secondly helping in decision making. If it is an important decision, it needs to be looked at in several ways. From these considerations I drew two points about experts. First of all, the problem of the expert taking over the decision making process, saying: 'I am the only person that can understand the problem, I will tell you the answer'. And linked with this is the problem of the manager, or managing director, or executive who lets him, who gives away his responsibility until he gets a decision.
The only comment I have on politicians, I am afraid, is a rather rude one, that they commit both of these sins. First of all they use an expert to justify what they are trying to do, and then they quickly reverse roles and take on the role of the expert and say: "We know best" or "We know what is best for you". And I don't know who first coined the phrase, but the comment that comes to mind - and I think it is true of a lot of things we have been talking about during these two days, but in this context I apply it to politicians - that politics is certainly too serious a subject to be left to the politicians.

(Balemans) Thank you Mr. Bannister. Mr. Rowe, you have a question about decision making and uncertainties.

(Rowe) Yes. I am asked: "How do the decision makers work with uncertainties? What is done in the USA?"
In general, I think, there are four possible ways of reacting to uncertainties.
a. To ignore the uncertainties, something which I think is absolutely incorrect.
b. To recognize that uncertainties exist and that in some situations no rational decision can be taken. I am sure that all of us have been faced with questions that at that particular time we could not answer.
c. To try to reduce uncertainty by gathering more information. Here the ground rule is that the cost of gathering the information should never exceed the value of the information we are trying to acquire. In theory we should balance these at the margin, but it is often hard to put value on information, so in many cases it is indeed a difficult balance to make.
d. Probably the most important thing to recognize is that there are many situations when there is information, but we still have to rely on value judgements in making the decision.

In connection with the things that Mr. Bannister has said, I would like to identify three different kinds of value judgments: the scientific value judgment, the social value judgment and what I call the managerial value judgment.
The scientific value judgment is the kind of thing that we ask scientists to do for us, such as: What is the dose-effect model to be used for radiation, or for investigating the carcinogenicity of vinyl chloride. Then we have to do all kinds of epidemiological experiments, and at the low levels we are talking about they may cost billions of dollars. But in the end the scientists come and say: "Well, here are the limits of our uncertainty, and this is what we think is most likely." This information is a scientific value judgment, it is not fact. We can easily have one group of scientists saying: It should be this, according to our hypothesis, and another group saying: According to our hypothesis, it should be that. The reasons for this may vary from differences in hypotheses to trust or distrust in the material.
When we are talking about acceptability, we are talking about social value judgments. What is an acceptable balance if we know on the one hand the scientific judgments about the possible damage and on the other, the benefits we would like to have. Now at least in a democratic society, this social judgment has to be made by participation of every knowledgeable member of society.
Having made the social decision, we then have to go to what I call the managerial decision. We have to implement, and if it is a regulation, we have to implement it in

such a way that when someone violates it, we can say: "He has violated it" and go to the courts and prove it. Here, the scientist comes back in again. He tells us how we can measure these things, how we can put numbers on them so we can get our fingers behind them. Very often what we thought was best socially, now has to be modified so we can implement it in a realistic manner.
That is the way I think we tend to deal with uncertainty in society.

(Balemans) Thank you. Mr. Windebank has the question: Is the current use of the word risk misleading or different? That seems to be another definition problem, I think.

(Windebank) I am not sure that I understand the meaning of that question, I have got a feeling that it is loaded, but I don't recognize where.
Of course, everybody here has a good enough understanding of the English language to know that words assume different shades of meaning according to context. But I would say that all people here in the room are using 'risk' with the same understanding and that is the meaning of the word. The audience may have noticed that in my paper I did not use the word 'risk' at all, except in the title. I used the word 'hazard' instead, and this was for a particular reason. In the world of insurance, which I am very closely associated with in day-to-day work, the word 'risk' has a particular meaning. Throughout the English speaking world it is used to represent the item which is being insured. That apart, I have a preference for the word 'hazard'. I think that the word 'risk' is more appropriately used when we are talking of voluntary actions, such as crossing the road. Where we are talking of unvoluntary occasions, such as being stuck by lightning, I feel the word 'hazard' is probably a little more appropriate. This, of course, is somewhat pedantic.

Mr. Chairman, perhaps I may go on directly with my second question, which is: "If risk analysis is proving effective at reducing risk, will that be reflected in insurance premiums?"
I would like to answer that as an engineer and not as an insurance man, which I am not. I would like to make two points.
The insurance premium can be likened to the price of a product, in the same way that the risk or hazard, expressed arithmetically, can be likened to the cost of that product. I think that there is the same relationship between premium and hazard as there is between price and cost of any product on the market. There are all kinds of other factors to take into account, other than cost, when the price is being determined.
The other point I would like to make is that, if risk analysis is proving effective and the excercise itself must be making some contribution, then the more we carry on with it, the more effective it will be.

(Balemans) Thank you, Mr. Windebank. A quick look at my watch has told me that we are nearing the end of the panel discussion. We are sorry that we have been unable to answer all questions that have been put to us, but in view of the sheer quantity of questions that have been thought out by you all, this was impossible from the start. For our last question I turn to Mr. Rowe and Dr. Otway again, who have something about the legitimacy of trying to influence public opinion.

(Rowe) It says: "Making an approach credible can be extremely costly. We wonder how important it is to have a multidisciplinary team when doing a risk analysis. Is there an obligation to influence public perception of the two sides of an issue? We might even ask whether we have the right to influence public opinion?"
Although I think it is an important question, I'll try to make my answer as brief as possible. Everyone here has been and will be trying to influence the opinion of his public. If you don't agree with something, you will start to argue which is a way of trying to influence opinion, and if you agree you will say nothing or express agreement, which is another way of influencing opinion.
The difference is, I think, between trying to influence public opinion and trying to

manipulate public opinion. If you want to influence public opinion, it is very important to provide the public with all information so that they can make their own judgments. As to manipulating public opinion, there is a famous saying of one of our Presidents that you cannot fool all of the people all of the time.
The complicated problems we are talking about here usually have many sides, and you can expect that in society you will have many different groups with different points of view and different personal investments in the issues. Each of them tries to influence the opinion of the other groups. I think that it is important that everybody has an opportunity to have their own input. If these are made clear and put into proper perpective, one can change public opinion simply by letting them see what there is. This, however, is my personal opinion, I am sure that other members of the panel will have their own.

(Otway) The first part of the question asks whether the multidisciplinary approach is necessary. In our experience it is extremely valuable, it does broaden and enrich the analysis. We have found that in putting together people with different disciplinary skills a broader perspective is acquired. In relation to changing public opinion or attitudes, I would like to point out that this is the third largest business in the USA; a few years ago over thirty billion dollars was spent yearly on advertising, which can only be called attitude change. Psychologically it is very complex, there are perhaps five to ten competing effects involved. We don't really know very much about it, it is unknown, for example, why the same communication changes some people's attitude in one direction and other people's in the other. If anyone is thinking of undertaking an attitude change program, I think he probably could find better uses for the money. First it may not work at all, and secondly, if it does work, it may not work in the direction you would like it to work.
One factor, known to be important, is the credibility of the communicator, mentioned by Mr. Schwarz a few minutes ago. At any moment you can start building up your credibility, but it should be realised that it is a long term process. It implies of course that all information given to the public must be factual and that the communicator should present both sides of the issue.

(Balemans) Ladies and gentlemen, we have now come to the end of the panel discussion.
I feel that in these two days we have seen that risk-analysis should be developed as parts of a watch-dog science, that evaluates, changes, improves and limits the consequences of technological developments and ensures that the community will not be dominated by certain techniques, but that technology should be for the benefit of the community. I readily admit that this directly leads to the famous problem of how to guard the guardians. I thank the members of the panel and the leaders of the discussion groups for their contribution, and I thank you all for posing so many interesting and clever questions.

Contents