methodologies for hazard analysis and risk assessment in the petroleum refining and storage industry

Prepared by Concawe's Risk Assessrnent Ad-hoc Group

S. Hope
E.N. Bjordal
H.M. Diack
B W Eddershaw
L. Joanny
G. Ortone
F.G. Payne
A.H. Searson
K.W Sedlacek
W. van Strien

Den Haag
December l982

concawe

concawe

ABSTRACT

The report provides readers both within and outside the petroleum industry with an overview of the methodologies already in use or being developed, to assist and supplement risk management practices.

The report briefly describes the consecutive steps in the identification, assessment and comparison of hazards and associated risk. These techniques can be helpful in setting the priorities for the decision on measures to reduce risk.

When quantifying risk e.g. for the comparison of alternative design cases, the use of a consistent data base is stressed. It is pointed out that the risk assessment techniques described in the report, although potentially valuable tools for improving overall safety performance, have shortcomings particularly in dealing with human factors.

In the appendices examples are given of the techniques, ranging from checklists to the prediction of human error.

A glossary is appended to define terms as they are used in this report and a list of recommended further reading is included.

Dit rapport geeft lezers - zowel binnen de olie-industrie als daarbuiten - een overzicht van de methoden die gebruikt worden of in ontwikkeling zijn ter ondersteuning en aanvulling van practische risicobeheersing.

Het rapport geeft een systematische beschrijving van de identificatie, beoordeling en vergelijking van potentiële gevaren en de daarbijbehorende risico's. Deze technieken kunnen nuttig zijn bij het stellen van prioriteiten wanneer besloten wordt tot risicobeperkende maatregelen.

Het belang van het gebruik van een consistente gegevensbank bij het kwantificeren van risico, b.v. bij het vergelijken van verschillende mogelijke technische ontwerpen krijgt speciale aandacht. Er wordt op gewezen, dat de in het rapport beschreven methoden voor het beoordelen van risico's, hoewel in beginsel waardevolle hulpmiddelen om tot een verbetering van de veiligheid in het algemeen te komen, toch hun tekortkomingen hebben, in het bijzonder waar menselijke factoren in het geding zijn.

De bijlagen bevatten voorbeelden van de technieken, variërend van checklijsten tot werkwijzen voor het voorspellen van menselijke fouten.

Verder is een glossarium toegevoegd waarin de in het rapport gebruikte termen worden gedefinieerd, alsmede een lijst van aanbevolen literatuur.

Der Bericht vermittelt Lesern aus der Mineralölindustrie und aus anderen Wirtschaftszweigen einen Überblick über bereits praktizierte und noch in Entwicklung befindliche Methoden zur Einschränkung von Betriebsrisiken.

In knapper Form werden die einzelnen Schritte der Bestimmung, der Beurteilung und des Vergleichs von Gefahrenquellen und mit diesen verbundenen Risiken beschrieben. Diese Methodik erleichtert die Bestimmung der Prioritäten und die Entscheidung über Maßnahmen zur Risikoverringerung.

Bei der Risikoquantifizierung, z.B. für den Vergleich von Designalternativen, wird die Notwendigkeit der Verwendung eines konsistenten Datenbestandes unterstrichen. Trotz ihres Wertes als Mittel zur Verbesserung der allgemeinen Betreibssicherheit weisen die in dem Bericht beschriebenen Methoden der Risikobeurteilung Unzulänglichkeiten auf, und zwar insbesondere im menschlichen Bereich.

Im Anhang werden Beispiele für die Methoden geboten. Sie reichen von Checklisten bis zur Vorhersage menschlicher Fehler.

Ferner enthält der Bericht ein Glossar mit Begriffsbestimmungen und ein Literaturverzeichnis.

Ce rapport fournit aux lecteurs, appartenant ou non à l'industrie du pétrole, une vue générale des méthodologies déjà utilisées ou en cours de développement destinées à soutenir et à renforcer les pratiques d'évaluation des risques.

Ce rapport décrit brièvement les étages successives de l'identification, de l'évaluation et de la comparaison des dangers et des risques associés. Ces techniques peuvent aider à établir les priorités parmi les mesures à prendre pour réduire le risque.

Lors de l'évaluation du risque, par exemple pour la comparaison de différentes solutions au niveau du projet l'emploi d'une base de données cohérente est mis en évidence. Le rapport souligne que les techniques d'évaluation du risque décrites, bien que constituant des outils précieux susceptibles d'améliorer la sécurité dans son ensemble, sont insuffisantes en particulier lorsqu'il s'agit d'estimer les facteurs humains.

On trouve en annexe des exemples de techniques, allant de listes de vérifications à la prévision de l'erreur humaine.

Egalement en annexe, on trouve un glossaire qui définit les termes employés dans ce rapport et une bibliographie des ouvrages dont la lecture est recommandée.

Il rapporto fornisce al lettore, sia all'interno che all'esterno dell'industria petrolifera, una rassegna delle metodologie già in uso o in fase di sviluppo per assistere ed integrare le procedure di controllo dei rischi.

Il rapporto descrive brevemente le tappe per l'identificazione, la valutazione ed il confronto dei pericoli e dei relativi rischi. Queste tecniche possono essere utili nello stabilire un ordine di priorità delle azioni da prendere per ridurre il rischio.

Dovendo quentificare il rischio, ad es. nel confronto di casi di progetti alternativi, viene sottolineata l'importanza di una base di dati omogenei. Viene anche fatto notare che le tecniche di valutazione del rischio descritte nel rapporto, anche se costituiscono strumenti potenzialmente validi per migliorare la sicurezza globale, hanno però dei limiti, particolarmente quando si tratti con il fattore umano.

Nelle appendici sono dati esempi di tecniche che vanno dalle liste di controllo alla previsione del fattore umano.

Viene anche allegato un glossario dei termini usati in questo rapporto e una lista di ulteriori letture raccomandate.

El informe ofrece al lector, tanto en la industria petrolera como fuera de ella, una visión general de los métodos actualmente en uso o en desarrollo, para ayudar y complementar las prácticas de tratamiento del riesgo.

Describe brevemente los pasos consecutivos en la identificación, evaluación y comparación de la peligrosidad y del riesgo asociado. Estas técnicas pueden ser útiles para establecer prioridades al decidir medidas para reducir el riesgo.

Al cuantificar el riesgo, p.ej. para la comparación de casos de diseño alternativos, se insiste en el empleo de una base de datos compatible. Se destaca que las técnicas de evaluación del riesgo descritas en el informe, si bien son medios potencialmente valiosos para mejorar la seguridad general, tienen particularmente inconvenientes al tratar con factores humanos.

En los apéndices se dan ejemplos de los técnicas, desde las listas de control a la predicción del error humano.

Se añade así mismo un glosario en el que se definen los términos empleados en el informe y una lista de bibliografía recomendada.

C O N T E N T S

C O N T E N T S (contd.)

1. INTRODUCTION

This report provides an overview of methodologies which can supplement existing risk management practices, with particular reference to major hazards.

It is written with petroleum refining and large scale storage installations in mind although many of the principles involved are applicable to the transport of petroleum feedstocks and products by road, rail, sea and pipelines.

The report is not intended as a manual for the specialist, but rather for all persons who wish to be informed about these developments and their applicability.

As this report serves as an overview it should be borne in mind that the data therein contained are quoted for illustrative purposes and should not be interpreted as CONCAWE recommendations.

2. HAZARD ANALYSIS AND RISK ASSESSMENT AND THE CAUSES OF INCIDENTS

2.1 RISK ASSESSMENT OR HAZARD ANALYSIS ? *

Risk assessment is the systematic examination of an actual or proposed industrial installation to identify, and form an opinion on potentially serious hazardous occurrences and their possible consequences. Its principal purpose is to assist decision-making on risk avoidance or risk reduction measures although in certain cases a risk assessment may be used in public decision-making on the location of a proposed installation or continued acceptability of an existing installation.

Although the term "risk assessment" is chosen in this report there are other related words and expressions which are not always clear. Sometimes these are defined and sometimes not. The most frequently interchanged words are "hazard" for "risk" and "analysis" for "assessment", thus giving four expressions, i.e. risk assessment, risk analysis, hazard assessment and hazard analysis, all of which may be found in the literature.

i) An analysis is considered to be a technical procedure following an established pattern.

ii) An assessment is the consideration of the results of the analysis in a wider context to determine the significance of the analytical findings.

iii) A hazard is considered to be an inherent property of a substance or a situation which has the potential to cause harm, e.g. hydrogen fluoride is a hazard because of its chemical nature, and a falling stone is a hazard because of its kinetic energy.

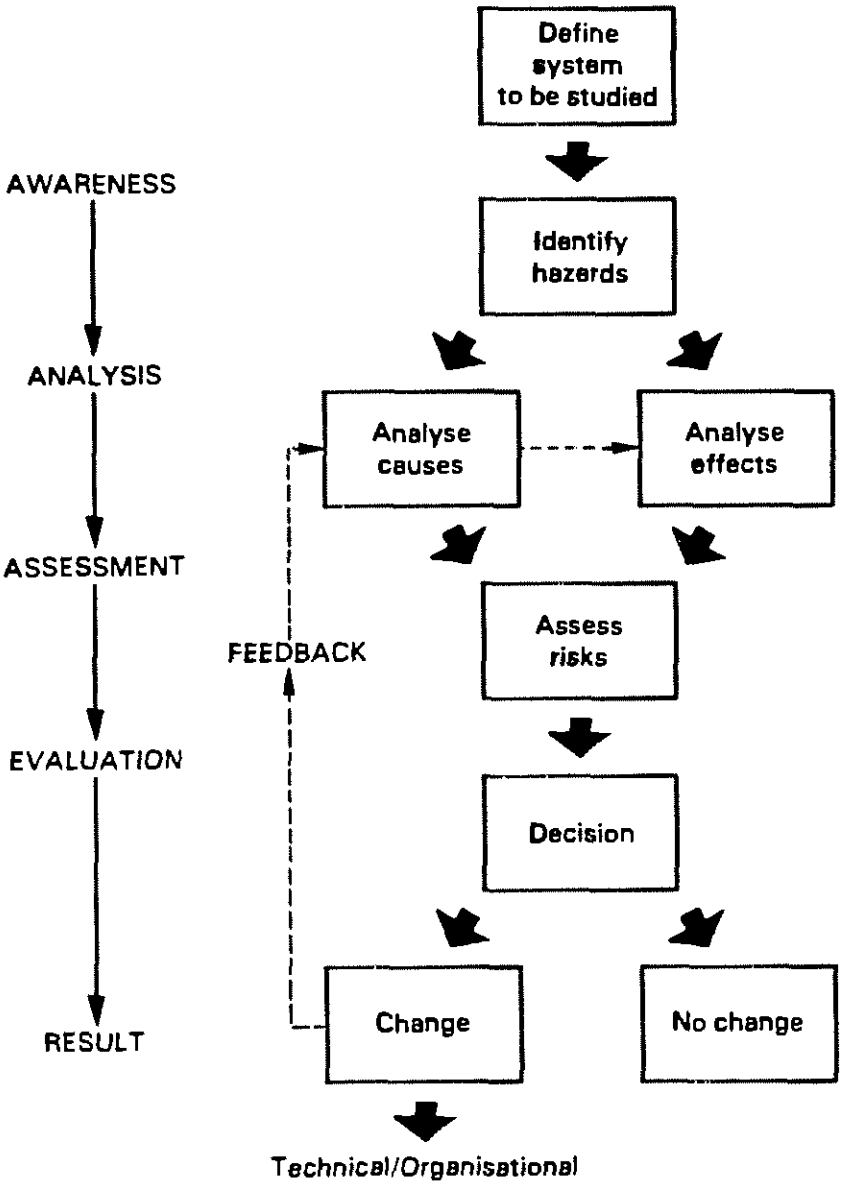
iv) Risk is considered to be related to the consequences of a hazard potential being realised and causing harm. Hence people and property may be considered "at risk" from a nearby hazard. Risk is sometimes expressed in mathematical probability terms involving both failure and consequences, e.g. the chances that a hydrogen fluoride containment system will fail and cause an escape of hydrogen fluoride. This may or may not cause damage. The probability that people will be harmfully affected by the released material can often be calculated, and the two results combined. Sometimes, however, risk tends to be restricted only to consequences such as in: "Should the failure occur the risk to people will be .....etc."

---

* For a comprehensive GLOSSARY OF TERMS see Appendix V.

Within these broad definitions "hazard analysis" is seen as being more technically specific than "risk assessment", and is part of it. The flowscheme shown in Fig. 1 outlines the overall procedure.

Fig. 1 Overall procedure



2.2 THE CAUSES OF INCIDENTS

Legislative authorities reflecting public concern, point to the records of large scale processing industries where serious loss of containment resulting in explosion, fire or release of toxic chemicals has occurred. These potential hazards have remained virtually unchanged for many years. They have on occasion caused loss of life and injuries to employees and sometimes to members of the neighbouring public. However, a review of the references (1) shows that worldwide, only a few incidents involving loss of life

arose from petroleum refining and storage operations and that the accident rate is below the average for manufacturing industry as a whole (2, 3). Nevertheless, there is concern about the potential for large scale future incidents even though there have only been a few of such incidents in the past.

Major incidents nearly always have more than one single cause. In most cases there is a prime cause resulting in a loss of containment of hydrocarbons which may catch fire and possibly explode, but it is very rarely that areas outside the installation are affected.

There are important differences between the hazards associated with refinery processing, and those in storage and handling whether the latter are at refinery sites or at separate locations. A number of processing activities involve elevated temperatures and pressures, whereas storage and handling is mainly at ambient or near ambient conditions (except for liquefied petroleum gases) although inventories are usually much larger.

However, although processing and storage activities incorporate safeguards against hazards, which vary in nature and sophistication depending on the type of the activity and its location, both have risks which can be assessed.

An analysis of available major incident data shows that all of them result from one or more of the following causes, most of which can be controlled or their consequences mitigated.

- design/construction failure
- operating error
- equipment failure (may derive from operational error)
- maintenance weaknesses
- insufficient supervision and training
- natural phenomena
- external interference

In order to put those causes into perspective, analysis of refinery incident data from the records of a large company suggests a typical distribution shown in Appendix I.

Each of these potential causes has to be considered in conjunction with the possible consequences and in this regard must be considered in the light of specific local circumstances. It should also be borne in mind that well established and rehearsed emergency procedures are essential to control and minimise the effects of an incident, should one occur.

A more detailed review of the causes of incidents is also given in Appendix I.

3. THE MANAGEMENT OF RISK

Before describing the methodologies of hazard analysis and risk assessment, the practice of risk avoidance and control as part of management's responsibility for reliability and safety is first outlined in this section.

As design and process technology has evolved and the complexity of operations has increased, safety standards have been developed and improved throughout the industry. Some differences occur which reflect company preferences, local circumstances and statutory requirements of the country in which the installation is situated.

Thus management is increasingly concerned with the need to identify, analyse and assess hazards at all stages in the life cycle of an installation, from the initial project proposal through to final shutdown. This systematic approach enables management to rank potential hazards in order of priority, thereby enabling risk to be reduced in a realistic and cost effective manner.

The life cycle is summarised in Table 1:

Table 1 Life cycle of an installation

Stage	Comments
1. Planning	Includes strategy, research and development and process selection.
2. Process design	Lay-out of installation and broad equipment specifications agreed.
3. Design engineering	Preparation of engineering drawings and detailed specifications for equipment fabrication, purchasing and operation.
4. Construction and commissioning	Erection, checking, testing and introducing feedstock.
5. Operations	Including periodic shutdown for maintenance, modifications or for operational reasons.
6. Final shutdown	Operations terminated and plant dismantled for disposal.

Risk management within this life cycle depends on the following:

i) Sound standards of engineering design must be used.

ii) Quality control procedures must ensure that all equipment conforms to design specification.

iii) All equipment must be inspected, maintained and tested at suitable intervals.

iv) Personnel must be experienced and trained in the use of clearly defined procedures.

Failure to apply these principles will almost certainly invalidate the use of results from any of the modern systematic hazard analysis techniques.

The basic practices of risk management applied by companies in the European petroleum industry are described in detail in Appendix II.

For the majority of installations, the level of risk can be judged from relevant accident statistics. However, there are cases where this may not be feasible or realistic e.g. for a new process installation of unprecedented size, modifications to an existing plant or when design standards have been improved. In such cases there is a need for additional techniques to assess the level of risk to life, property and the environment.

These techniques are complementary to the more pragmatic ways of problem identification and assessment. They highlight how hazards can occur and provide a clearer understanding of their nature and possible consequences, thereby improving decision-making. They range from relatively simple qualitative methods to advanced quantitative methods in which numerical values of risk are derived.

They are most effectively applied during the planning, process design and design engineering stages when it is generally possible to make changes which are less expensive than when the plant is being built or is operational. In practice, such methodologies have been used to examine plant siting, lay-out, improve safety levels in operating and maintenance systems and solve technical problems.

It is within this context that the various methodologies described in section 4 should be considered.

Comment on management of risk would not be complete without reference to the importance of well planned and rehearsed emergency procedures, to minimise the possible effects of an incident, should it occur. Such procedures include communications, fire-fighting, personnel protection and medical treatment, provision for seeking assistance and evacuation.

The possible impact of incidents on adjoining installations must also be borne in mind. If there is a potential risk to neighbouring communities or amenities, then there must also be co-ordination with the local authorities' emergency plans.

Regular training, including exercises in emergency procedures, fire-fighting drills, etc., helps to maintain a high state of preparedness, and often points to improvements in the emergency plans.

4. ANALYTICAL PROCEDURES

As defined in section 2, hazard analysis is considered to be a technical procedure following an established pattern. Its application often assumes that sound engineering standards, operating and maintenance procedures and safety policies are already being employed. The procedures described in this section fall broadly into two categories i.e. qualitative and quantitative.

4.1 QUALITATIVE PROCEDURES

These provide a more formalised and structured approach to hazard identification. Of the various procedures described below, those from section 4.1.2 onwards are more recent developments.

4.1.1 Check-lists

Check-lists are essentially simple and empirical and generally used to check compliance with good engineering design and operating practices. Many companies have their own check-lists for specific areas of design and operation. A number have been published (4) and although these relate mostly to the chemical process industry, they have application in petroleum refining and downstream installations.

Check-lists should be designed to stimulate thought and enquiry. The questions should preferably be "open" rather than in a form which requires "yes/no" answers e.g. after having identified that overpressure may exist, asking "How is the system protected against overpressure?" rather than "Is the system protected against over-pressure?"

Nevertheless, for a check-list to be comprehensive, it may have to contain many questions, and as experience reveals problems, more questions have to be added to the list. Check-lists can therefore be cumbersome, and the user may be misled into believing that all aspects which ought to be questioned have been covered without confirming that this is so.

Further, a check-list is general and will not be exactly appropriate to a specific project. By their nature, check-lists provide no quantitative measures. Thus they do not allow relative ranking either of hazards or of the effectiveness of designed protection against risk. This is a drawback in complex systems having several hazards.

4.1.2 Hazard Indices

Hazard indices are also empirical but their use provides a better basis for assessment and subsequent decision. The most widely known method is probably the Dow Fire and Explosion Index (5) devised by the Dow Chemical Company for its own use (see Appendix III).

It primarily aims at identifying fire, explosion and chemical reactivity hazards in a plant design. It is best carried out at an early stage of the project, when changes to the process and plant lay-out can most easily be made. It can also be used for audit purposes on an existing plant.

The Dow Index is computed by applying a number of empirical hazard factors which reflect the properties of the materials being processed, the nature of the process, spacing of the plant equipment and the judgement of the analyst about them. The Index is then used as a criterion for selection of preventive and protective design features from a range of standardised systems. It gives no credit for safety features which will be, or already have been, installed.

The Dow Index is aimed only at the evaluation of fire and explosion hazards of process plant. It does not provide the same depth of consideration to handling operations and does not include auxiliary facilities.

A more recent hazard index, principally developed for the chemical industry is the Mond index (6). This expands the Dow Index to include wider consideration of storage and loading/unloading areas. Additional factors in the index computation are the effects of toxic materials in the process and also those lay-out features which clearly modify the risk potential. The range of factors contributing to this index figure is therefore greater than in the Dow Index, and some are semi-quantitative (see Appendix III).

A technique which enables estimation of physical damage arising from fire and explosion in an installation, is the Instantaneous Fractional Annual Loss (IFAL) procedure (7). This is not based on arbitrary factors but estimates the physical effects from a study of the features displayed by the design, and computes a theoretical loss figure (see Appendix III).

These empirical methods provide an insight into the implications of the design through the detailed considerations required for factor estimation. The importance of possible protective measures can be assessed, and valuable information is provided regarding future operating practice and planning of response to emergencies. They have the limitations that they do not give a complete picture, and should therefore not be used in isolation but used to supplement other hazard studies.

4.1.3 Open-Ended Procedures

The methods described in sections 4.1.1 and 4.1.2 have the disadvantages in that all hazards may not be exposed. The importance of interaction of some of the hazards may also not be appreciated. More open-ended systematic methods offer a better chance of overcoming these disadvantages. The best example of these is The Hazard and Operability Study technique or HAZOP (8). Variations of this technique may be made by bypassing certain features of it but its full value is thereby diminished.

HAZOP is essentially a qualitative procedure in which a small team examine a proposed design by generating questions about it in a systematic manner. Each member of the team should have some particular responsibility in the project including future operations as well as design. The questions, although prompted by a list of guidewords, arise creatively through interaction between the team members. They uncover deviations from the design intention so that as each deviation is revealed, possible causes and resulting effects can be considered. Thus potential safety and operability problems are identified and appropriate action can be taken.

To assist in the identification of hazardous deviations, the team will usually find it helpful during the exercise to compare the proposed design with relevant engineering standards at suitable stages in the HAZOP procedure.

By using the HAZOP method, the need for action is decided semi-quantitatively based on the team's experience and judgement of the seriousness of the consequences, together with the expected frequency of the occurrence. In situations where uncertainty remains about the hazard, numerical analysis using the techniques reviewed in section 4.2 may be helpful to probe causes and malfunctions, clarify priorities and provide better guidance for decision-making.

Quantification may help to make a decision on a minor problem e.g. if it is revealed that a rise in liquid level in a compressor suction drum would cause damage by liquid carry-over, disagreement between team members on whether single or double trip protection should be provided, can be reconciled by quantification using approximate failure data. Such calculations can be performed quickly in a study meeting.

Thus although identification is carried out rigorously and to a certain extent fault paths are probed, detailed fault analysis is not normally a systematic part of the HAZOP procedure. Its main purpose is to identify the main hazards and operability problems and to establish their causes. Generally, the method is not concerned with high hazard/low probability events or with combinations of them. In addition to its open-ended approach favouring identification of potential problems, a fundamental strength of HAZOP is the encouragement of cross-fertilisation of

ideas between members of the study team. Its success depends on the degree of cooperation between individuals, their experience and competence and the commitment of the team as a whole. An extract from a published study (8) is given in Appendix III as an example.

4.2 QUANTITATIVE PROCEDURES

If numerical analysis of the way in which hazard can arise is required, techniques which incorporate probability estimates must be used.

The first stage of these techniques is usually qualitative e.g. as in a Fault Tree Analysis, and it must be borne in mind that even without proceeding to the quantitative stage such an analysis can be a very helpful qualitatively. A typical example of this approach can be a Maximum Credible Accident Evaluation (MCAE), which is based on judgement and experience.

A number of differing quantitative techniques have been developed all of which use logical simulation models, numerical data and mathematical computations. The applications of these methods are currently increasing and care should be taken not to exceed their inherent or logical limits. Conceptually, virtually all of these methods fall into one of the following five categories or attempt to adapt the original concept to special circumstances.

i) Fault Tree Analysis (FTA)

ii) Failure Mode and Effect Analysis (FMEA)

iii) Random Number Simulation Analysis (RNSA)

iv) Techniques for Predicting Human Error (THERP)

v) Epidemiological Analysis

Further details of these techniques illustrated by examples, are given below and in Appendix III.

4.2.1 Fault Tree Analysis (FTA)

The underlying principle of fault tree analysis and similar techniques (9) is the construction of a logic diagram containing all conceivable event sequences, mechanical and human, which could lead to a specified failure. The basic procedure is as follows:

i) The failure (or "top") event is specified e.g. overfilling a particular storage tank.

ii) All causative chains of events leading to the specified failure are identified.

iii) Probabilities and frequencies can be assigned to each event, and thus an overall probability or frequency for the specified failure can be calculated.

iv) The most significant events or sequences can, therefore, be firmly established. Also if the frequency of the failure event has to be reduced, analysis of the contributions to it from various parts of the quantified tree can show where the most effective action can be taken.

A fault tree traces an undesirable event back to its roots. Tracing a primary event forwards in order to define its consequences, also referred to as incident sequence analysis (20), results in an event tree. These two trees together comprise a cause-consequence diagram.

FTA is versatile. It can be of value qualitatively by highlighting failure pathways and their nature and also by providing clarification of causative events and their interaction. Possibilities for risk reduction may thus be tentatively suggested before numerical data are applied to the tree. Of course, without quantification, reduction in probability of the top event cannot be assessed.

Its particular application is not for tracing the failure path of specific components, but to investigate further the consequences of those events indicated by a HAZOP study, or to examine the failure of a plant system e.g. to explore subsequent possible failures if a pressure relieving device in a crucial operation fails to do its job properly, or to explore the follow-on effect of another incident.

The technique is particularly suited to mechanistic options e.g. valve open or closed. Time and rate dependent events i.e. changes in critical process variables, degrees of failure, dynamic behaviour etc., are not easily represented.

For complex installations, the alternatives to be assessed (branches of the tree) become so numerous that with a realistic use of manpower and other resources a full analysis is impracticable. It is necessary to be selective in the use of the technique, confining it to the areas of greatest uncertainty and sensitivity. Furthermore, it will be appreciated that there may be difficulty in determining probability factors for varying causes in a consistent way. This inevitably requires the analyst to use subjective judgement, possibly leading to bias.

A simple example of FTA, relating to the overfilling of a process tank is shown in Appendix III.

4.2.2 Failure Mode and Effect Analysis (FMEA)

The underlying principle of this analysis (10) is to examine all components and operating modes of an installation with the objective of determining the consequences of malfunctions and failures. FMEA is applicable in the design and construction stage, but is particularly suited for examining existing plant e.g. to identify the need for safety activities.

The analysis is formalised in order to apply it to complex systems with a large number of components. The main steps of the analysis are as follows:

i) All individual system components are listed e.g. control valves, pumps etc.

ii) All failure possibilities for each component are identified.

iii) For each failure mode the effects on other system components are determined and the resulting impact of the overall performance or integrity of the system is evaluated.

iv) The probability and seriousness of the results of each specific failure mode are calculated and compared.

Failure Mode and Effect Analysis (FMEA) is generally applicable to the same type of installation or process as Fault Tree Analysis (FTA). The difference of approach between the two methods is that FTA starts from the failure event ("top down"), whilst FMEA starts with the individual components and assesses the consequences of their failure ("bottom up").

The strength of FMEA, particularly for complex systems, lies in its completeness, as failure modes are identified. Appendix III considers part of the same example as used for FTA and develops it by an FMEA approach.

In comparing FMEA with FTA it should be appreciated that under most circumstances FMEA is much more time consuming.

4.2.3 Random Number Simulation Analysis (RNSA)

This method, which is also called the Monte Carlo Method (11, p 67), uses a Fault Tree or a similar logical model of the installation or the process under review as basis for the analysis. However, in contrast to the conventional Fault Tree Analysis, the probability of each individual contributing failure event is not expressed as a single number but more realistically as a range of probabilities over which the failure event can occur. In addition, the severity of the component failure or the event contributing to the "top" failure e.g. loss of containment can now be expressed as a function of its probability. Taking flooding as an example of a hazard, the simple input of x days of rain and y days of no rain may be

inadequate or even misleading. The severity of the rainfall can now be related to its frequency x_1 days of drizzle, x_2 days of light rainfall etc.

The ability to differentiate in this way (for each contributing event if necessary) makes the RNSA a flexible analytical tool.

The precise technique and the constraints of the method are difficult to describe in general terms, but a simplified example of a storage tank rupture and oil release caused by a fragment from disintegrating equipment is shown in Appendix III to explain the principles involved.

The basic steps of the method are as follows:

i) The Fault Tree or logical model is established.

ii) For each independent component of the Fault Tree where there is a range of probabilities, a probability/failure severity curve is determined.

iii) Each of these curves is divided into a number of segments e.g. one hundred discrete values.

iv) The first overall failure probability is calculated as a single value, selecting at random one of the discrete values for each independent component.

v) The process of calculation is repeated, until the individual results form a probability distribution curve of the overall failure probability.

It is important that genuinely independent components or events are properly identified before applying the random number selection process, in order to avoid distortion or bias of the final probability distribution curve.

If components are interdependent, the analysis usually becomes more complex requiring considerable analytical experience and skill.

A Random Number Simulation Analysis requires detailed preparation and numerous repeated computations. A random number generator is required and access to data processing equipment is necessary.

The result of the analysis i.e. a distribution curve of the probability of the failure event, is, however, conceptually much more realistic than a single numerical value for those specific problems for which the method is applicable.

4.2.4 Techniques for Predicting Human Error

In an industry already employing high standards of technology, it is becoming increasingly important to reduce human errors at all levels in the organisation in order further to improve safety

performance. New methods are being developed to investigate human mistakes, whether due to personal errors or those due to organisational weaknesses. An example of the latter is the "goal method" (12) which relates the goals of an individual operator, responsible for the operation of specific equipment, to the goals of the plant as a whole. This method is helpful in training operating teams, particularly with respect to their reactions in emergency situations. However, the most commonly used numerical method for the measurement and assessment of personnel induced errors is called Technique for Human Error Prediction (THERP) (13, 20). This procedure involves the following steps:

i) The relevant human activities, which may create a hazard, are identified.

ii) The associated failure rates are estimated.

iii) The possible effect of such human mistakes on the entire system are analysed.

The numerical factors used in estimating human failure rates are usually empirical or statistical, and may sometimes be determined by experiments or transposed from similar tasks.

The main application of THERP in hazard analysis studies in the process industry is to provide estimates, in quantifying fault trees, of the probability of an operator's error as a causative event or of his failing to take effective action in preventing a potentially hazardous situation from deteriorating. These estimates can be used similarly in Fault Tree, Failure Mode and Effect and Random Number Simulation Analyses.

The most important limitation of THERP is that it cannot cope with human decisions, e.g. those which involve elements of technical judgement particularly in emergency situations. A further difficulty is that even for comparatively simple tasks e.g. pressing a button, adverse factors related to the work-place environment, can significantly change the failure rate of an operator. This aspect has to be considered independently (see Appendix III for further details).

4.2.5 Studies using the Epidemiological Approach

There are numerous methods in use in various sectors of industry to forecast malfunctions or failures of components or systems. Analysis of past performance data and of failure reports may reveal causative factors or likely event frequencies. Results can be used to improve design features, maintenance schedules and other requirements. Such data are in fact very frequently used as input to Fault Tree, Failure Mode and Effect, and Random Number Simulation Analyses. However, past performance data can also be used independently as bases for special analyses, to improve the failure

rate of components and systems by attempting to detect underlying causes of malfunctions or failures (see Appendix III). There is no simple way of formalising the procedure of data analysis. Often it may be useful to begin with the following steps:

i) Acquire as much relevant data as possible relating malfunctions and failures to operating conditions.

ii) Analyse this information to check whether specific failures have common elements which may identify underlying causes.

iii) Repeat this process by varying the relationships of malfunctions to operating conditions.

The validity of conclusions from such analyses rely to a very great extent on the quality of the data base and the statistical significance of anomalies found in the sample.

Adoption of the results from an existing analysis is possible only when the circumstances being examined are similar.

4.3 CHOICE OF PROCEDURE - A WORD OF CAUTION

The choice of procedure and depth of analysis will vary with the nature and potential scale of the hazard, and the stage in the plant life cycle at which the analysis is applied e.g. in the early phases detailed design information is not available.

The procedures facilitate the sytematic identification of safety aspects of a process or installation, particularly where experience is lacking. The most sophisticated methods provide tools for solving particular problems e.g. those involving high complexity or severity of consequences. Furthermore by enabling the available data to be formalised in a logical manner, omissions in the data base are highlighted and errors in the analysis minimised.

However, there are certain limitations common to all the methods which must be borne in mind:

i) The analysis represents to a varying extent the analyst's interpretation of the installation, and particularly when the system being analysed is complex the analyst may inadvertently introduce bias.

ii) It is absolutely essential that all the data used are truly relevant to the case being analysed. In practice data are often scarce, incomplete or not directly applicable.

iii) Sometimes, assumptions about major hazard events have to be based on extremely limited statistical data for events which happen infrequently. This will introduce an additional degree of uncertainty.

iv) The prediction of human behaviour is extremely difficult and where it plays an essential part in the analysis this will result in further uncertainty.

v) Some of the techniques are very complicated and detailed and demand appreciable specialist manpower and time resources.

vi) The nature of the methodologies can easily lead to mis-interpretation and misuse of the results.

The strengths and limitations of the procedures in the proceeding sections is accounted for in more detail in Appendix III, section 10.

5. ASSESSING THE CONSEQUENCES

So far the identification of potentially hazardous situations and the minimisation of plant and equipment failure have been considered. The second major consideration in overall risk assessment is an analysis of the possible harmful consequences if there is plant or equipment failure.

These two considerations taken together, form the technical analyses which in turn may be put into a wider assessment framework. The consequences can be considered as having three components, viz. the physical effects and the effects on human beings and on the environment. These are briefly reviewed.

5.1 EFFECTS AND MAGNITUDE

The main physical effects arise from the escaping gases or liquids catching fire or exploding. The effect on human beings is through fire, explosion, or, in certain cases, acute toxicity.

5.1.1 Fire

The nature of any crude oil and its products is such that on escape from its containing vessels, pipelines, etc. it will give rise to a fire if the other combustion requirements, viz. vaporisation in the case of liquids, oxygen in the right quantity and a source of ignition of suitable strength are also present. It is because of this intrinsic property that design practices, operating and emergency procedures, etc. are implemented to:

- avoid escape of material
- minimise the amount if there is an escape
- prevent any escaping material from catching fire
- tackle the incident quickly and effectively if there is a fire.

It is because of the structured and rigorous approach to incident avoidance and minimisation that nearly all incidents which may have the potential to cause a major fire do not do so. It is inevitable, however, that occasionally some fires will escalate in size and will take longer to bring under control. The physical damage will be more severe. Furthermore, there is a greater possibility of impact on people in the immediate vicinity, i.e. those tackling the incident, because of sudden increases in the severity of the fire or other concomitant risks when further equipment fails as a result of the fire. In this regard, note should be taken of two extreme situations where the possibility exists of the fire escalating abnormally:

i) A fireball where for a short time the rate of burning is increased rapidly and the heat radiation effects, particularly on people in the immediate vicinity, are correspondingly intensified.

ii) A Boiling Liquid Expanding Vapour Explosion (BLEVE) in which vessel rupture occurs as the consequence of external fire and an instantaneous release of burning hydrocarbons suddenly extends the area of the fire and creates a fire-ball. Vessel fragments may be scattered over an area considerably wider than the harmful zone of heat radiation.

5.1.2 Explosions

Explosions with significant overpressure effects are caused by unconfined or, more likely, partially confined vapour cloud explosions. Such vapour cloud explosions can cause significant damage to buildings and equipment in the vicinity, in fact they may be capable of causing collapse of structures. Harm to people may be effected directly such as someone close to the explosion incident being hurled by the force of the explosion over the ground or against a structure. The more probable harm, however, is being trapped by a collapsing structure, struck by falling material, or a missile, or by broken glass.

5.1.3 Exposure to Toxic Materials

This report is concerned only with toxic effects arising from the sudden release of a large quantity of material which can cause harm in relatively low concentrations. It is not concerned with the possible harmful impact of frequent, or regular, exposure to low concentrations of a material over a long period of time because the analysis and assessment process is different from that applicable to sudden large releases and exposure.

There are many chemicals which are used in refining or blending processes as treating agents, inhibitors, catalysts, etc. which if they suddenly escape in an uncontrolled way may cause harm to people in the immediate vicinity concerned with the operation of the equipment. There are only very few cases where the quantity and location may be such that other persons nearby on the site, or just outside if located close to the site boundary, may be affected.

The possible toxic impact of each chemical, whether used or generated, can only be examined in its own particular circumstances, especially its location on the site.

5.1.4 Assessment of Magnitude

Whatever form the harm takes, fire, explosion or toxicity, it is nevertheless necessary to determine:

- How much material is likely to escape?
- What is likely to happen to it, over time and distance, i.e. the physical consequences?
- What is the effect on people?

The estimated amount of material which is likely to escape is very much bound up with the failure rate assessment because it is inextricably linked with the nature and size of the equipment failure which has been assumed. However, with the postulated equipment failure and a knowledge of the process considerations, the total amount which can escape, the time, period and the ratio of vapour to liquid can be determined with sufficient accuracy using established chemical engineering calculations.

However, from this point onwards the accuracy of successive estimations becomes poor.

The most likely thing to happen to escaping hydrocarbons in practice is that they will disperse and not ignite. However, when they do ignite, experience indicates that they are most unlikely to explode.

If ignition occurs very quickly near the release point, heat flux and temperature calculations can be made to determine the possible physical harm to neighbouring equipment. There is accumulating experimental evidence from large scale trials which are producing data in this field.

Secondary damage and feeding of the initial fire is much more uncertain but estimation of these effects is not impossible if simple assumptions can realistically be made. However, care must be taken not to oversimplify the assumptions. If, however, ignition is assumed to be delayed the calculation of the physical consequences becomes considerably less certain. Such calculations must start with dispersion calculations. Much technical expertise is being devoted to the development of dispersion models but even the most advanced thinking in this field has to make considerable simplifying assumptions to make the models manageable. Account must be taken of the physical state of the ejected material, its release rate, natural topography, intervening structures, atmospheric conditions, homogeneity of the cloud and so on. It is not realistic for this report to recommend any particular models as it is a highly specialised subject on which expert opinion should be sought for any particular case.

Having determined the dispersion characteristics the next requirement concerns assumptions about ignition sources and these are by no means straightforward. The way in which the subsequent fire develops will depend on the dispersion and ignition assumptions

and calculations. There is a very high probability that the fire will flash back to the source, possibly ending up as a pool fire, but the extent to which it deviates from a simple flash back is more of an assumption than a calculation. It can of course be realistically assumed that local fire damage in the path back to the source will be severe.

However, the biggest single concern about delayed ignition is that a large enough vapour cloud may form, under conditions which can give rise to a vapour cloud explosion rather than simply to a fire. Although having identified the possibility there is no way of forecasting by technical calculation whether a particular equipment failure will in fact give rise to a vapour cloud explosion. All that can be said is that explosions are not impossible and their severity can vary widely. Nevertheless, a reasonable estimate can be made of the structural damage which could be caused if cloud combustion developed into a severe explosion. The translation of material damage into human casualties is so speculative that in practice it can be no more than a statistical assumption which in any given case may be orders of magnitude wrong.

The summation of the uncertainties inherent in calculations of consequences particularly with regard to harm to members of the public is perhaps best reflected by comparing desk studies, where it is not uncommon to find predictions of very high rates, with actual experience where serious casualties among members of the public are very few and far between.

5.2 CRITERIA OF ACCEPTABILITY

It is implicit in all decisions on safety built into plant design, construction and operation, that there must be some inbuilt acceptability criteria with which the plant management is satisfied. Most industry acceptability criteria, or the rationale leading to these criteria, are not routinely stated explicitly. They are usually inferred from or incorporated in international, national, industry and company standards, codes, design practices and procedures, etc. Furthermore, they are not fixed for all time and circumstances, but are subject to revision in the light of new knowledge and experience. It is also implicit that such criteria are not, and cannot be, founded on the basis that failure is impossible.

It follows that the level of risk to which those on, or in the vicinity of, a plant or installation are subjected is determined by the management concerned, excepting insofar as supervisory authorities have intervened to enforce various statutory requirements. However these have normally been specific, relating to well-defined aspects, and of a relatively limited nature.

The challenge which is now having to be faced, and indeed the demands which are being made in certain situations, are that this

is not enough. The argument is that for any particular development proposal or even existing activity, the rationale and acceptability criteria must be clearly established in explicit terms and be exposed to public and independent scrutiny. Such a proposal requires that design, construction and operating practices should be subject to systems of safety reviews of increasing scale and sophistication. Whilst there can be no objection to increased safety vigilance through appropriate reviews, the problem is that these demands are promoting a safety dimension which incorporates an ever widening application of the methodologies discussed above to the point where there is much concern about the value of the conclusions which are drawn, for instance when related to the quality of the input data and the amount of technical expertise required to do the studies. In order to clarify why this is so, it will be helpful to comment on the analytical process which is incorporated in these safety reviews. Such a review, taken to the limit, can be summarised as follows and it will be appreciated that this is a very simplified statement:

i) By one of the techniques previously described e.g. HAZOP the process is searched minutely for faults, uncertainties, weaknesses, etc. in design and operability.

ii) Insofar as such faults, etc. can be corrected by improvements in design and operability, this is done.

iii) For the remaining parts of the process and equipment, and starting with those which are assumed to have a higher probability of malfunction, a failure rate is then established using, for example, fault tree analysis.

iv) By integration a combined failure rate for the whole process, or part of the process is established.

v) An assessment is made of the nature and the amount of substance which can be released, and then by use of a suitable dispersion model its subsequent dispersion is estimated.

vi) It then requires an expression of the possible impact of the dispersed material, e.g. if it may explode, the overpressure considerations; if it may burn, the heat effects; if it is toxic material, its possible toxic effects. The possibility of any of these happening and their possible magnitude in terms of deaths, injuries or damage is also estimated.

vii) Finally, by considering iv) and vi) above an overall statement of risk of death or injury or material damage is estimated.

viii) A cost/benefit analysis (CBA) may be helpful to establish priorities.

It is self-evident that the accuracy of the end result of such a complete analysis requires a considerable amount of technical expertise and practical experience, very many assumptions about failure possibilities, dispersion modelling, environmental impact

and human behaviour, and finally a considerable quantity of relevant data. Such an analysis, however, only has a value if it is used to help make a decision, and in this regard it is helpful to establish what kind of decisions can be made.

a) If the purpose of the safety review is to search a new design, or changes in a design, in order to seek out possible faults or weaknesses for correction it would clearly be sufficient to consider only stages i) and ii) above.

b) There may be situations, however, where this is not considered enough. Possibly a failure in a particular part of the process could have very severe consequences and further safeguarding or other technical options should be considered.

   In this case, iii) and iv) above may be introduced to get a better understanding of the comparative safety of the extra safeguarding or the other technical options. The need for such calculations will probably have required some broad appreciation of the considerations implicit in stages v) and vi) although not necessarily requiring the detailed analyses which these stages can generate.

c) From a public point of view, however, even b) may not be considered enough. The demand may be that some statement corresponding to stage vii) above is made. This is, in effect, a statement of residual risk and any action which arises, apart from questioning its accuracy, is of a socio/political nature, not technical. Its significance can only be that the figures can be compared with statistics on deaths, injuries or material damage caused by other human activities or natural phenomena. The implied assumption is that there is some criterion or threshold value below which the casualty rate, or the scale of damage, is acceptable, and above which it is unacceptable. The value of such a criterion, assuming there is one, is beyond the scope of this report as it is concerned with public perception and sociological considerations and not with technical matters. A well-known report (14) is an example incorporating stage vii) analysis. It may be felt that a report which requires the detail of stage v) but with only a broad statement of land utilisation and population densities within the calculated damage area, i.e. a limited stage vi) is considered enough to assist in making the socio/political decision. Another example of such a report is reference (15) which deals with a natural gas liquids pipeline installation.

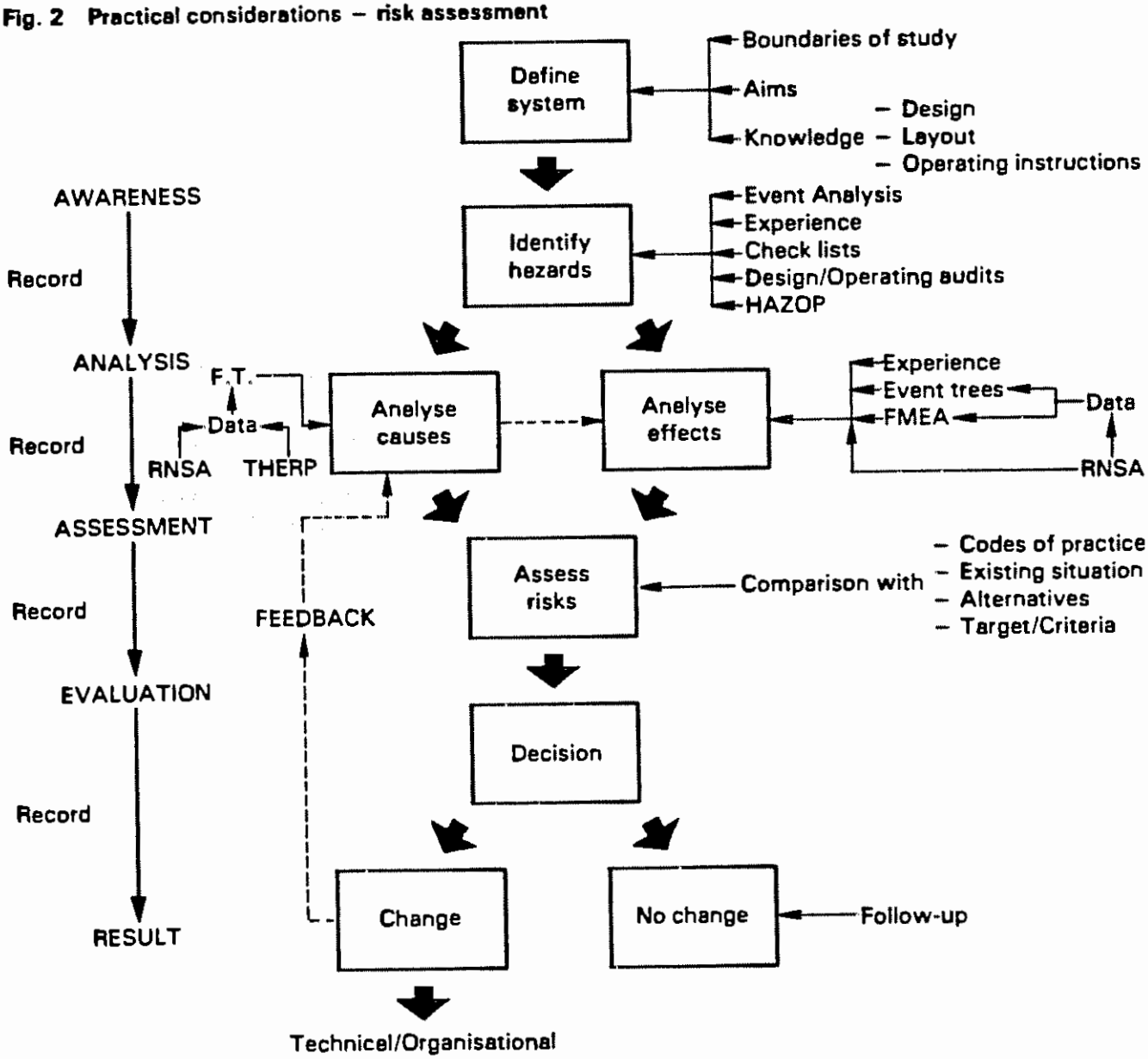
   In contrast to c) it should be specifically noted that the studies referred to in b) concern safety comparisons between different technical options or marginal safety improvements caused by extra safeguarding.

   Studies under a) and b) therefore should be considered as potentially very valuable tools to assist routine decision-making in areaa of safety uncertainty or concern.

6. PRACTICAL APPLICATION

The effectiveness of risk assessment or hazard analysis procedures involves a number of practical considerations (see Fig. 2). An example of a procedural check-list is shown in Appendix IV. Some specific aspects are reviewed below.

Fig. 2 Practical considerations – risk assessment



6.1 OBJECTIVES AND SCOPE

Before commencing a study, its objectives and scope must be defined explicitly. The purpose of the study and the fundamental assumptions made must be clearly stated.

Where more than one study is required, possibly simultaneously, the boundaries must be specified to avoid overlap or omission of potential hazards. The possible effects of incidents in neighbouring installation and adverse natural phenomena e.g. storm conditions, should also be taken into account. Such studies must also be co-ordinated to enable investigation of interactions between one part of the system and another.

6.2 PROCEDURAL ASPECTS

Procedural aspects should be considered whenever applying any of the methods described. The following section is related in particular to HAZOP studies. The validity of the results depends on the information available, the way it is used and its relevance to the process or installation and its operation, as follows:

- The piping and instrumentation drawings and the plant equipment and process data must be correct and up-to-date.
- The physical plant lay-out and equipment must comply with specifications e.g. materials of construction and control valve failure actions.
- To assist in the identification of hazardous deviations, the team will usually find it helpful during the exercise to compare the proposed design with relevant engineering standards at suitable stages in the HAZOP procedure. For example, the review of a furnace in a proposed plant design may be expedited by reference to the company's furnace standards, using a specially prepared check-list to ensure that all safety aspects are systematically covered.
- Operating procedures should be in accordance with written instructions.

A study at the project design stage can identify those features which must be checked once the plant is constructed and in operation. Field audit procedures are normal practice for existing plant. The resources required for a study i.e. organisation, manpower and skills, will vary with its objectives and scale, as follows:

- In the case of a new project, studies will be done at several stages of its development. The composition of the team will change as responsibilities for various aspects of the design change. Normally members will have an engineering background. At certain stages members with a legal or medical background should be included. Teams will be guided by an independent safety specialist.
- Small teams e.g. for a HAZOP study on existing equipment, usually have constant membership representing all appropriate interests concerned with the project. Guidance will be by a safety specialist with experience in the technique.

- A quantification and assessment study is usually carried out by one or two specialists.
- Should an external team be appointed, the commitment and co-operation of Company staff is essential, preferably by including a few Company representatives.

Before a HAZOP, designers will have confirmed that the proposed design is to relevant engineering standards. However, team members will need to have knowledge of such standards and during the study will seek to confirm that the design is to the standards. Team members may find an aide-memoire helpful in searching for potentially hazardous problems in the proposed design. Such aide-memoires, if appropriately designed, encourage the interactive questioning which is desirable in the technique. They could also ensure that all safety aspects are covered. But care must be taken that they are are not used as check-lists otherwise the value of the HAZOP technique will be decreased.

All studies should be followed up to ensure that agreed actions have been taken and that preventive measures have not introduced potential hazards elsewhere.

6.3 RECORDS

Studies should be recorded and retained as a basis for future design work and for the guidance of operating personnel. Problems which have been identified and the actions taken should be highlighted. The records can also provide the background to, if not the basis for, the documentation required by licensing authorities.

6.4 THE USE OF NUMERICAL DATA

The application and limitations of numerical methods when further insight into identified hazards is required have been described.

Some practical considerations concerning the use of numerical data are indicated below:

- The actual performance of a new plant may differ from that predicted at the design stage, and therefore hazard data should be carefully reviewed.
- Some types of plant are more subject to modification than others, due to technical innovation and feedback of experience.
- Care should be taken to avoid disregarding potential hazard events because there is uncertainty about the failure mode or because their probability or frequency is low.

- In the course of a risk analysis calculation the tendency to err on the conservative side is analytically unacceptable.

- Common mode effects which may result in simultaneous failure of several components or systems require careful consideration.

6.5 THE PROBLEMS OF HUMAN BEHAVIOUR

The influence of human beings on incidents, either as a principle cause or in supplementing the action of protective systems has been emphasised.

Human response to unexpected events is complex and difficult to predict in hazard analysis and data is often not available. Some estimated probabilities of human failure are shown in Appendix III.

6.6 FOLLOW-UP

The results and conclusions of a risk assessment, and the assumptions used, should be checked by the operating personnel. The techniques assume that a plant will function as predicted and that its human and material components will behave similarly to elsewhere, and this may not be the case.

Thus the original study should be checked following commissioning, to ensure that the assumptions and predictions are still valid. This should be repeated at intervals in the light of actual operating experience, so that differences can be identified and data on reliability collected.

7. CONCLUSIONS AND RECOMMENDATIONS

7.1 CONCLUSIONS

From the information reviewed in this report, the following principal conclusions can be drawn:

1. The potential major hazards from petroleum refining and storage installations may give rise to fire and explosions and to a lesser degree the release of some toxic substances. These hazards have remained virtually unchanged in their technical nature for many years.

2. Risk assessment is being increasingly used to evaluate the impact of accidents on members of the public and employees. In Europe, information on major accidents has been well documented and analysed both by industry and the competent supervisory authorities. Thus it is considered improbable that people in the vicinity of the site are subjected to risks of a nature other than those described in the report.

3. The accident rate* in the petroleum refining and storage industry is below the average for manufacturing industry (2,3) and because of continuing efforts by the industry a significant increase in the accident rate is most unlikely.

4. Currently used hazard identification and mitigation techniques to reduce the frequency and seriousness of incidents are continually being refined and updated. New analytical methods may be developed but it is not foreseen that they will give a sudden improvement or open new insight into the process of identification and mitigation of hazards. Futhermore there is no indication that any single method will become predominant.

5. Current methods for the analysis of hazards and risk are, within their inherent limitations, valuable tools for improving overall safety performance. However, they have shortcomings particularly when dealing with human factors, principally due to lack of precise data and of adequate methods to analyse the behaviour of human beings in an industrial environment. This is especially so when complex and rapid decisions are required. The multiple use of worst-case-probabilities is analytically unacceptable.

6. Automatic control and safety devices are widely used in the petroleum industry. Operational control is increasingly

*see Appendix V - GLOSSARY OF TERMS

being facilitated by process computers, which are also used to assist in decision-making. However, it seems likely, as well as desirable, that the need for human decisions will continue especially at the level of operator and supervisor. Therefore the problems related to the prediction of human behaviour in risk analysis will not be eliminated.

7. The extrapolation of risk assessment studies from predictions of equipment failure and incident frequency to the estimation of casualties is subject to considerable uncertainties.

8. Quantitative analytical methods can be employed to rank potential hazards, compare technical alternatives and identify cost-effective solutions. It can be expected that in these areas their use will spread.

7.2 RECOMMENDATIONS

Based on the above conclusions the following recommendations are made:

1. Managements of petroleum installations should review the effectiveness of their present risk assessment practices. Risk assessment and control should be applied during all stages in the life of an installation from site acquisition to final decommissioning. Quantitative methods should be used when appropriate.

2. The assessment procedure should be flexible and reflect the particular circumstances of the installation. The concept of a single rigid methodology applicable to all petroleum installations should be avoided.

3. The inherent and unavoidable uncertainties of such assessments should be borne in mind.

4. Where design or technical alternatives are available, the comparative risks as well as the comparative economic benefits should be considered.

5. Since quantitative risk analyses depend on reliability (and accuracy of performance) data, the petroleum industry should investigate the possibility of improving the collection of information for such analyses in a structured way.

8. REFERENCES

1. Davenport, J.A. (1977). A survey of vapor cloud incidents. Chemical Engineering Progress, September 1977.

2. UK Health and Safety Commission. Newsletter No. 19, August 1981, London: HMSO.

3. US National Safety Council. Accident Facts. 1980 Edition.

4. Balemans, A.W.M. et al (1974). Check-list: guidelines for safe design of process plants. In: Preprints of the 1st International Loss Prevention Symposium, The Hague/Delft, 28-30 May 1974. Amsterdam: Elsevier.

5. American Institute of Chemical Engineers (1981). Dow's Fire & Explosion Index, hazard classification guide. 5th Edition. LC 80-29237.

6. Lewis, D.J. (1980). The Mond fire, explosion and toxicity index applied to plant layout and spacing. In: Loss prevention, Vol. 13. New York, NY: American Institute of Chemical Engineers.

7. Munday, G. et al (1980). Instantaneous fractional annual loss - a measure of the hazard of an industrial operation. Paper presented at the 3rd International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Basel, Switzerland, September 15-19, 1980.

8. Lawley, H.G. (1974). Loss prevention: operability studies and hazard analysis. Chemical Engineering Progress 70, 4.

9. Fussell, J.B. (1976). Fault tree analysis - concepts and techniques. In: Generic techniques in systems reliability assessment. Ed. by Henley, E.J. and Lynn, J.W. Amsterdam: Noordhoff.

10. Lambert, H.E., et al. (1978). Material control study: A directed graph and fault tree procedure for adversary event set generation. In: NATO Advanced Study Institute on Synthesis and Analysis Methods for Safety and Reliability Studies. Urbino, Italy, 415-435.

11. Sobol, I.M. (1974). The Monte Carlo Method. Chicago, Ill.: University of Chicago.

12. Embrey, D.E. (1981). Approaches to the evaluation and reduction of human error in the process industries. Institution of Chemical Engineers Symposium Series No. 66.

13. Swain, A.D. (1964). THERP. Report SC.R.64.1338 Albuquerque, NM: Sandia Laboratories.

14. UK Health and Safety Executive (1978). Canvey. An investigation of potential hazards from operations in the Canvey Island/Thurrock area. London: HMSO.

15. UK Health and Safety Executive. A safety evaluation of the proposed St. Fergus to Moss Morran natural gas liquids and St. Fergus to Boddam gas pipelines. London: HMSO.

16. Swain, A.D. (1977). Design techniques for improving human performance in production. Revised edition. Albuquerque, NM: Sandia Laboratories.

17. Swain, A.D. and Guttmann, H.E. (1980). Handbook of human reliability analysis with emphasis on nuclear power plant applications Report Nureg/CR-1278 Albuquerque, NM: Sandia Laboratories.

18. Ablitt, J.F. (1973). An introduction to the "Syrel" reliability data bank. UKAEA Report SRS/GR/14.

19. T.N.O. Industrial Safety Data bank: Failure and Accidents Technical Information System (FACTS), for incidents with hazardous materials (in English), Apeldoorn, The Netherlands: T.N.O.

20. Incident sequence analysis; event tree, method and graphical symbols (1977) DIN 25 419, part 1. Probabilistic evaluation, (1979) DIN 25 419, part 2.

9. FURTHER READING

Although this is a general report, some readers may wish to read further. The literature on risk assessment is very extensive. Only a selection of references is suggested here. There is a further reference list in each reference.

Fault Tree Analysis

Prugh, R.W. (1981). Practical applications of fault tree analysis AIChE Loss Prevention, Vol. 14.

Brown, D.M.; Ball, P.W. (1980). A simple method for the approximate evaluation of fault trees. European Federation of Chemical Engineering, Third International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Basel, Switzerland, September 15-19, 1980.

Reactor Safety Study: an assessment of accidents risks in the US Commercial Nuclear Power Plants Report WASH 1400 1975, US Atomic Energy Commission (Note: illustrates also the use of RNSA).

Failure Mode and Effect Analysis

Procedure for performing a failure mode and effect analysis (1977). Report MIL-STD-1629A. 1977. Washington: US Department of Navy.

Taylor, J.R. (1973). A formalisation of failure mode analysis of control systems. Report M16584 1973 Atomic Energy Commission Research Establishment Risø. National Laboratory, DK-4000 Roskilde, Denmark.

Human Error

Embrey, D.E. (1981). A new approach to the evaluation and quantification of human reliability in systems assessment. Third National Reliability Conference.

Howland, A.H. (1980). Hazard analysis and the human element. European Federation of Chemical Engineering. Third International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Basel, Switzerland, September 15-19, 1980.

The Human Operator in Process Control (1974). Editors: Edwards, E. and Lees, F.P. London: Taylor and Francis.

Random Number Simulation Analysis

Lavere, J.M.; Kalli, H. (1977). Usefulness of the Monte Carlo Method in Reliability Calculation. Trans. American Nuclear Society, Vol. 27.

Hazard and Operability Studies

Lees, F.P.; Roach, J.R. (1981). Some features of, and activities in Hazard and Operability (HAZOP) Studies. The Chemical Engineer, October.

Chemical Industries Health and Safety Council (1977). Hazard and Operability Studies. London: Chemical Industries Association.

Lawley, H.G. (1976). Size up plant hazards this way. Hydrocarbon Processing, Vol. 55, April 1976.

Cause-Consequence Diagram

Nielsen, D.S. (1971). The cause consequence diagram method as a basis for quantitative accident analysis. Report M-1374, May 1971. Risø National Laboratory, DK-4000 Roskilde, Denmark.

Risk Analysis/Studies

Lovati, A. (1980). The conclusive results of a risk and safety assessment Chim. Ind. M62(6) (in Italian).

Hauftmans, U. (1980). Fault Tree Analysis of a Proposed Ethylene Vaporisation Unit. Ind. Eng. F 19(3), (in German).

Lawley, H.G. (1980). Safety Technology in the Chemical Industry. A problem in hazard analysis with solution. Reliability Engineering, October, 1980.

Bjordal, E.N. (1980). Are risk analyses obsolete? European Federation of Chemical Engineering. Third International Symposium on Loss Prevention and Safety Promotion in the Process Industries. Basel, Switzerland, September 15-19, 1980.

Lagedec P. (1979). Dossier. Faire Face aux risques technologiques. La Recherche No 105, November 1979, 1146-1153.

Andurand, R. (1979). Le rapport de sureté et son application dans l'industrie. Annales des Mines, Jul/Aug 1979 115-138.

Taylor, R. (1979). A background to risk analysis 1979 Risø National Laboratory. DK-4000 Roskilde, Denmark.

Andrews, W.B.; Atwell, L.D. (1979). Risk assessment of sour gas facilities. APCA/PNWIS Annual Meeting Alberta 7-9 November, 1979.

Kletz, T.A. (1978). Practical applications of hazard analysis. Chemical Engineering Progress, Vol. 74, October, 1978.

Risk analysis of six potentially hazardous industrial objects in the Rijnmond area, a pilot study (1982). A report to the Rijnmond public authority. Dordrecht: Reidel.

concawe

methodologies for hazard analysis and risk assessment in the petroleum refining and storage industry

APPENDIX I – THE CAUSES OF INCIDENTS

CONTENTS

1. INTRODUCTION

This appendix reviews in detail some of the causes and mitigation of incidents in the petroleum refining and storage industry, outlined in section 2 of this report.

These are:

- design and construction failure;
- operational error;
- equipment failure (may derive from operational errors);
- maintenance weaknesses;
- insufficient supervision and training;
- natural phenomena;
- external interference.

In order to put the causes of incidents into perspective, an analysis from the records of one company suggests the following typical distribution:

Nature of cause	%
- design faults, equipment failures, construction and modification errors	30
- deficiencies in plant operation	45
- inadequate maintenance and inspection	20
- other causes	5
Total:	100

2. DESIGN FAILURE

Most equipment used in the petroleum refining and storage industry is of proven design meeting well established operating service requirements. Hence, the integrity of the plant as well as its efficiency is, for the most part, implicit in the design. Nevertheless the possibility exists that a particular piece of equipment may in practice prove to be under-designed for operating conditions not foreseen in the original specification.

Specialised equipment e.g. conversion process reactors, may have to be constructed to standards which are not compatible with conventional equipment. This may require more advanced operating techniques although this in itself does not imply a reduction in the safety of the designed facility or component.

It is a feature of modern plant designs, sometimes with larger inventories, that they also incorporate advanced safety features and

emergency equipment, including back-up or duplicate components in critical services e.g. emergency shutdown systems. This requires appropriate training to handle such equipment, but it also engenders greater flexibility in identifying and correcting abnormal operating situations. On the other hand, it may not always be possible or even desirable to retrofit modern safety features into older plant and so operating procedures are modified to take this into account.

3. OPERATING ERROR

The role of the operating personnel, who must be well trained and motivated, is essential to the safe operation of a plant. Nevertheless possibilities for human error are many and varied. Some typical examples are:

- instructions which are insufficiently clear or not understood;
- misinterpretation of instrument readings;
- errors in transfer of information between different departments;
- anxiety or stress under abnormal situations;
- equipment inadequately marked e.g. valves, pipelines, etc.;
- poor working environment e.g. noise, access, housekeeping;
- illness;
- over-familiarity.

These considerations apply not only to plant operating personnel as such, but to many others including maintenance, fire and safety and ancillary staff. In those cases where the consequences of an operator making the wrong decision can be severe, the possibility of reducing the degree upon which he is relied upon to intervene e.g. by means of automation, can be examined.

Substantial progress has been made in the design of fail-safe equipment and developments are continuing particularly in the diagnosis of incipient problems, often by means of process computers. Nevertheless, operators in particular have to exercise judgement under conditions of urgency or stress in a real or perceived crisis. Current risk assessment methods tend to place more emphasis on equipment orientated analyses. This is possibly due to the not inconsiderable difficulty of adequately predicting and quantifying human reactions referred to above (also see section 4.2.4 and Appendix III). It is also quite correctly assumed that very often actions by operators will usually rectify an unforeseen deviation from the normal operating plan before a hazardous situation develops. The importance of operator training procedures is referred to below (item 5).

4. EQUIPMENT FAILURE

Equipment failures may occur during the operation of otherwise properly designed and installed equipment and components.

Some potential reasons for such failures are defective manufacture or construction, engineering faults not revealed by maintenance and inspection procedures, fouling, vibration, damage by mobile equipment etc. Mobile testing facilities prove efficient during the construction stage as well as in existing plant, to identify the use of wrong construction materials, which otherwise might pass unnoticed.

5. MAINTENANCE WEAKNESSES

The role of maintenance, including statutory inspection, is to ensure safe, efficient and economic operation of plant equipment. This calls for a professional judgement and close consultation between engineering, operating and, where appropriate, safety departments. A periodic review of work permit procedures and other aspects of safe working practice is vital.

Scheduled maintenance and regular inspection procedures are essential in pre-empting disruptions to normal plant operations, and selective maintenance can reduce the failure rate of critical components.

Equipment should not be modified during maintenance until changes are reviewed and authorised.

6. INSUFFICIENT SUPERVISION AND TRAINING

Effective and updated training procedures for operating personnel are essential in reducing the number and severity of hazardous situations, both for existing and new plant. Particularly in computer assisted operations, if training routines are not properly structured and maintained, the computer can become a barrier between the operator and his understanding of the process plant which he is operating.

These procedures may vary from formal classroom training e.g. using process simulators, to on-the-job training in equipment operation, the assessment of safe working conditions and the use of safety equipment.

Improved motivation resulting from such training should encourage reporting of potential accidents and near-misses and enable the causes to be eliminated.

7. NATURAL PHENOMENA

Conditions arising from natural phenomena e.g. lightning, flooding, subsidence, icing etc., may cause damage leading to hazardous situations. Whilst these occurrences are relatively infrequent, appropriately designed and maintained installations operated by trained personnel will reduce their consequences, but may not necessarily eliminate damage.

8. EXTERNAL INTERFERENCE

These causes may arise from actions which are difficult or even impossible to control by the plant management e.g. sabotage, acts of war, etc. They also include follow-on, or "domino" effects from incidents on neighbouring plants. Whilst the effects can often be mitigated by protecting critical parts and preparing adequate emergency procedures, they are not considered further in this report.

concawe

methodologies for hazard analysis and risk assessment in the petroleum refining and storage industry

APPENDIX II – THE MANAGEMENT OF RISK – PRINCIPAL PRACTICES

CONTENTS

1. INTRODUCTION

Section 2 of this report emphasises that risk management should be practised at every stage of a refinery project from inception to initial startup then on through the subsequent operating life of the plant.

It also emphasises that the use of the various methodologies of risk assessment - such as described in section 3 - depend for their value on the use of basic sound engineering standards, design practices and maintenance and operating procedures. A fundamental requirement also, is that the plant design and operation must comply at least with the statutory regulations and standards of the country in which the refinery is located.

This Appendix therefore reflects the need for risk assessment and control as an integral part of each stage in the life of a project - design planning, process design, design engineering, construction, commissioning, ongoing operation through to final shutdown and dismantling.

The basic techniques are, in most cases, not sophisticated but rather are based on management structures and procedures (e.g. quality assurance) which will facilitate the systematic application of expertise and experience available in the company. A number of the recommended practices such as keeping of inspection and maintenance records are not, exclusively, directed towards safety: they may not be formally designated as safety activities. Nonetheless, they are working tools for identification and assessment of hazards and determination of corrective action.

From the report it will be clear that it is advisable to consider the use of hazard analysis and other risk assessment methodologies at the various stages of a petroleum refinery project, for assurance on the identification of potential hazards - and their possible effects - and give a firmer base for decision making. Ideally, they should be applied first at inception and design planning stages when fundamental decisions affecting safety are likely to be made and which it will be difficult to change subsequently. And then systematically they should be used in the succeeding stages not only to verify that earlier recommendations have been implemented but also to identify potential hazards which might have been unwittingly introduced during the later project activities.

The Appendix therefore deals with not only a range of recommended basic risk assessment and control practices but also suggests the place of the more sophisticated techniques. The basic practices represent a consolidation of petroleum refining industry procedures, the majority of which are utilised by the major oil companies. There are, of course, variations in detail and emphasis according to management styles and other local factors.

But overall, the practices described in the Appendix should form a cumulative basis through which the ultimate objective of a safe operating plant can be achieved.

2. DESIGN PLANNING

Hazard analysis and risk assessment should start at the inception and design planning stages of a petroleum refinery project, when fundamental decisions affecting safety are likely to be made, which will be difficult to change subsequently. Particularly critical items in this category are:

2.1 Site Selection

Assessment of risk to and from adjacent property is an essential part of the site selection procedure for a new project. In many cases, a formalised evaluation will be required by the Local Authority.

2.2 Process Selection

In cases where alternative processes are available for the required duty, e.g. for alkylation, process selection may be influenced by capital and operating costs, manpower requirements, availability of utilities and environmental considerations.

In addition, it is likely that there will be differences in the nature and magnitude of the risks associated with each of the alternative processes, and these factors should be evaluated by means of a formalised safety review, using the appropriate qualitative and quantitative techniques described in this report. This will enable not only the necessary protective design features to be estimated (probably only in outline form at this early stage of the project), but also may suggest as an alternative to protection, inherently safer features of the process or plant, which may be adopted instead.

3. PROCESS DESIGN

Management must establish monitoring and control systems and training activities, to ensure that potential hazards are recognised and controlled during the process design stage. Practices for achieving this include the following:

3.1 Design Practices Manual

In order to ensure quality and consistency of plant designs, the company practices should be documented in a design practices manual. The following safety design items would be appropriate for inclusion in such a manual:

- basic design philosophy and concepts;
- minimisation of potential fire and explosion hazards that exist in petroleum refining operations;
- features required for the safety of plant personnel (means of access and escape, safety showers, etc.);
- protection of equipment against overpressure, negative pressure, and high and low extremes of temperature;
- flare, blowdown and relief systems;
- emergency shutdown systems;
- plant and services lay-out and spacing;
- fireproofing of plant equipment and structures;
- fire protection measures (including firefighting) for refinery facilities;
- requirements for protection of refinery buildings, including blast resistance and prevention of toxic gas entry.

3.2 Safety Training for Process Design Engineers

As part of the overall training and development of engineers, process designers should receive appropriate training in design safety and techniques for hazard analysis.

3.3 Design Specifications

Safety considerations should be an integral part of all stages of preparation of a Design Specification. This requires specialists to be available for consulting with the designers during the course of the design work as well as for review of the completed document. Specialists in all the appropriate disciplines should be involved, e.g. instrument, electrical, mechanical, corrosion and safety engineering. Special attention should be given to risk assessment and control in cases where novel processes or new technology are involved. Safety reviews of the the Design Specification should be carried out by experienced personnel at the final draft stage. These reviews should be formally structured utilising techniques, such as the Hazard and Operability Studies, to ensure a consistent and thorough approach. This action will confirm the recommendations of previous studies and also provide added assurance that the Design

Specification does not carry unidentified hazards. The completed Design Specification should include a "Design Considerations" section in which the basis that was used for designing the safety facilities (e.g. the contingencies which determined the sizing of pressure relief and blowdown systems) is recorded. If special safety design features or variations or interpretations of normal design practice are incorporated in the Specification, they should also be noted in the Design Considerations. The purpose of this section is to document and explain the safety design basis of the project; this information will be essential for safety reviews or expansions during the subsequent life of the plant.

In addition, an "Operating Guide" section should be included, which will form the basis of the detailed operating manual and procedures which will be developed subsequently by the operations staff responsible for plant start-up.

4. DESIGN ENGINEERING

Refinery projects of large or medium size will normally be engineered by one of the specialist contractor companies, and the following paragraphs are based on this assumption. The same general approaches are applicable to smaller projects handled within the company's engineering organisation.

The following are practices and procedures which should be considered by the company management as a means of ensuring that the engineering design of petroleum refinery plant will be carried out in compliance with recognised codes and standards, and in accordance with the intent of the Design Specification.

4.1 Engineering Contractor Bid Review and Selection

The capabilities of the Main Engineering Contractor are highly significant in controlling the quality of the finished plant, and the company should therefore carefully evaluate the Main Contractors which are under consideration for carrying out the detailed engineering, purchasing and construction of a new project.

Engineering specialists should be included in the bid review procedure for selecting the Engineering Contractor. This is to ensure that the requirements of the Design Specification are fully appreciated, and to evaluate the competence of the bidding contractors in each specific area of engineering.

In the case of fixed price contracts it is particularly important that all safety requirements are clearly defined in the Design Specification, and it should be established that the contractors understand these requirements and adequately demonstrate their intent to comply.

4.2 Engineering Standards

The company should establish the codes and standards which are to be applied to the engineering of its projects, whether carried out by its own staff or by outside contractors. Engineering standards may be drawn from a number of different sources, and may differ for various locations. Examples of such standards would include mandatory national or local regulations, company engineering standards based on field experience and R&D work, and the specific Codes of Practice covering pressure vessels, piping, electrical area classification etc. It should be noted that most countries have independent organisations which set standards and codes for the petroleum industry in conjunction with the industry itself.

4.3. Liaison of Detailed Engineering with Construction

The company should establish systems and procedures whereby it can review the contractor's detailed engineering of a petroleum refinery project, to ensure that company standards and experience are incorporated and that local factors such as proximity to existing plant are taken into account.

It is common practice for the company to establish its own project management team to exercise this monitoring and supervisory function including random checks for quality assurance. Some members of this team may be resident in the contractor's office, such as the process design liaison engineer, while other specialists such as instrument, electrical, machinery and safety engineers will be involved part-time at appropriate stages in the project.

Monitoring of the overall engineering performance should be extended, where appropriate, to sub-contractors and equipment suppliers. Comprehensive check-lists provide an effective means for engineers to apply a systematic review of the contractor's detailed engineering.

The use of a scale model of the plant is a conventional technique used by the Main Engineering Contractors for detailed design of plant lay-out, pipe routing, access platforms, etc. The model also provides an excellent opportunity for hazard identification by the company engineering specialists and specialists in the refinery organisation, particularly operations, maintenance and safety personnel. Check-lists provide a systematic approach to this review. The company should agree a procedure with the contractor for these model reviews to be carried out at appropriate stages of the model construction. At the final stages of design engineering, a systematic safety review may be appropriate, with the use of numerical risk assessment techniques if necessary. Plant changes or additions to the Design Specification may be introduced during the course of detailed engineering: these must be subject to formal safety review and authorisation.

5. CONSTRUCTION

Management systems should be established by the company to ensure that plant construction is carried out by the contractor in accordance with the applicable design specifications and engineering standards.

A "Resident Engineer" function is a conventional means of exercising this control. This requires the establishment of a team of field engineers from the company organisation to supervise and check the contractor's installation standards throughout the construction period. Typical safety-related items that should be carefully monitored include:

- identification and control of construction materials, particularly alloy piping and fittings;
- application of fireproof coatings;
- piping fabrication and support;
- hydrostatic testing of vessels and piping.

Fabrication standards and, where appropriate, performance tests, of major equipment such as pressure vessels and compressors, should also be checked at the manufacturer's works by the company's specialist engineers.

During the construction stage, any plant modifications which involve changes or additions to the design specifications should be subject to formal safety review and authorisation.

At the pre-commissioning stage in a new plant, shortly before construction completion, a pre-start-up safety survey should be carried out by appropriate company specialists. Comprehensive check-lists provide a structured basis for such surveys.

6. PLANT START-UP

Start-up of new refinery plant is a critical phase with respect to potential hazards, particularly if new technology or unfamiliar processes are involved.

Training of plant operators; the formation of a commissioning team of operations, technical and engineering personnel; and checking of equipment, are basic requirements for a safe start-up. Commissioning procedures should include, for example, running-in of machinery, capacity testing of fire protection and sewer systems, checking of emergency instrumentation and testing of pressure relief devices. Special attention should be given to commissioning stages when conditions may differ from normal operation, such as drying out of low temperature plant, to ensure that design criteria of the equipment are not exceeded.

7. MANAGEMENT OF THE OPERATING PLANT

The refinery or its parent company should have a published statement of its overall safety policy. Consistent with these general aims, the management of the operating plant must set up an organisation structure and control systems to ensure that the many safety aspects of operation are given proper attention and priority throughout the life of the plant.

The following are representative of the approaches and practices used by the petroleum companies to achieve this objective.

7.1 Systems and Procedures for Management of Safety

Safety-related objectives, responsibilities and training requirements for all plant personnel should be established in the Job Description document for each position.

A system should be established for the reporting and correction of all equipment faults or deficiencies, and those which constitute a hazard should be given priority.

Modifications either to the plant or proposals to deviate from the operating conditions specified in the design, must be subject to a formalised safety review and authorisation procedure.

There should be a formalised and systematic communication network between the design and operations organisations in the company in order that:

i) New technology, design developments and revised standards can be advised to the operating functions in the refinery. This information should be complemented by advice on the upgrading of existing plant to new standards.

ii) Plant operating experience should be fed back, and design practices and engineering standards modified where appropriate.

A refinery "Safe Operations Committee" consisting of experienced engineers from the operations, maintenance, technical and safety functions, is an example of an advisory and consulting group on matters of safe operations, and which is also responsible for safety review of new projects and plant modifications. An activity of this type also provides a communication network for exchange of operating experience and technology information between the company refineries and central engineering organisations.

Records should be kept of all information relevant to the safety and integrity of the plant equipment, including:

- design specifications covering the original plant and any subsequent expansions or revamp projects;
- mechanical catalogues for the original plant and subsequent expansions or revamps, covering the detailed engineering information on the equipment (construction drawings, machinery data, test certificates, vendors' instruction manuals, etc.);
- equipment inspection and maintenance records;
- safety survey reports and status of follow-up actions.

7.2 Plant Operating Standards

Documentation of plant operating practices (e.g. operating manuals, flow plans, standing orders, etc.) in a practical and readable format is an essential basis for safe operation. These documents should be subject to a formalised periodic updating procedure.

Routine safety checks of the equipment by operating personnel should be established by means of a "Task Book" or similar scheduled arrangement, including operability of safety showers, installation of plugs in vents and drains, condition of fire-fighting equipment, etc.

An effective system of written communications between plant supervision and shift crew (e.g. operator log books) is necessary.

Self-audit procedures may be used to evaluate the standards of operation in a process plant area. This is usually carried out by a small team of personnel from other plants within the refinery. A semi-quantitative evaluation is possible by means of a comprehensive scored check-list.

7.3 Equipment Inspection and Maintenance

An effective equipment inspection organisation must be established to monitor corrosion and other potential defects, so that timely repair or replacement can be planned. Full use should be made of the on-stream inspection techniques that are available, as well as internal inspections during shutdowns.

Inspection information should be critically reviewed as the basis for setting safe run-lengths between shutdowns.

Safety valves and other protective devices must be subject to a rigorously controlled programme of regular testing and inspection. This responsibility should be clearly designated to the appropriate group(s) in the refinery organisation.

Computerised data systems provide a convenient means of recording inspection information and scheduling regular equipment inspections.

Effective monitoring of rotating machinery will enable vibration or other indications of incipient failure mechanisms to be identified and corrected. Advantage should be taken of techniques such as machinery signature analysis (MSA).

Equipment maintenance history, such as pump mechanical seal failures, should also be recorded so that repetitive problems can be identified and appropriate action taken.

Plant turnarounds involve complex operating procedures, intensive maintenance activities, and large numbers of personnel working in close proximity. Management must allocate priority and manpower to the detailed planning and preparations which are essential for the safe execution of a turnaround in a refinery.

The use of semi-quantitative self-audit procedures (similar in concept to those for operations described in 7.2) is an effective technique for evaluating maintenance in a refinery plant or area.

A "Safe Working Procedures manual" should be prepared, covering the normal range of refinery maintenance jobs, e.g. hot tapping, tank cleaning, blinding, exchanger cleaning, etc.

Maintenance and inspection personnel working on refinery equipment may be exposed to potential hazards of flammable or toxic materials, particularly when these activities are carried out on an operating plant. It is therefore essential that equipment to be worked on is first properly prepared by appropriate procedures such as draining, purging, isolation, testing for presence of dangerous fluids, etc., in order that safe conditions for the maintenance workers can be assured.

A work permit system is the conventional method used by the industry for controlling the preparation and release of equipment and authorisation of maintenance work. Management must ensure that the work permit regulations are practical, effective and rigorously enforced.

Good housekeeping in a refinery is generally recognised both as a motivating factor towards safe operating practice and as a measure of operating efficiency. It is desirable that management establish good standards and priority in this area.

7.4 Training

Training activities play a vital part in the overall programme for achieving safe plant operation. It is a management responsibility to establish training needs and allocate priority, manpower and facilities accordingly. Advantage should be taken of modern training aids and techniques, such as simulators and video equipment.

The following should be considered for inclusion in the training activities:

- basic training of new plant operators;
- qualification training for plant operators taking over a specific position;
- refresher training for plant operators;
- training in team leadership for chief operators;
- skills training for maintenance personnel;
- safety training for contractor personnel working in the refinery;
- management of safe operations for plant supervisors;
- training in instructional skills for plant trainers;
- operations experience interchange meetings between plant supervisors.

7.5 Emergency Preparedness

The following are typical of the ways used by the industry to promote preparedness for potential emergency situations:

- preparation of emergency plans and procedures. These should make clear the expected roles of individuals in emergencies. In preparing the plans, a realistic response time for the fire services should be used;
- training in plant emergency procedures, including the use of emergency exercises and simulations;
- training in the control of major fire situations for emergency supervisors;
- on-stream testing procedures for emergency systems;
- fire training, using real fires on training facilities which simulate potential refinery fire situations;
- smoke chamber training in the use of breathing apparatus.

7.6 External Safety Surveys

A survey by an external group is helpful in providing an independent assessment of the safety performance of a refinery.

The survey team, drawn from other parts of the company organisation, will usually include experienced operations personnel, and technical engineering or insurance specialists, according to the objectives of the survey. The following are

examples of safety-related areas that may be covered by such external surveys:

- management organisation and programmes in safety;
- safety of plant operations;
- equipment safety and fire protection;
- safety of specific equipment, e.g. refrigerated storage facilities, flare and blowdown systems, etc.;
- occupational health, e.g. exposure to toxic materials, noise, etc.;
- potential major fire/explosion risks and insurance requirements.

7.7 Reporting and Analysis of Incidents

Reference has already been made to the need for the industry to make constructive use of the operating experience of the refineries as feedback to design practices and engineering standards.

Fire, explosion and other incident reports constitute a vital source of information for identification of common problem areas and trends; and to indicate needs for training or equipment changes. An accident investigation and reporting procedure should therefore be established.

Maximum benefit will be obtained from a company hazard loss reporting system if a standardised format is used. Such a system can be readily designed for computerised data handling.

Statistics from such a system can provide useful feedback for design or management control purposes (e.g. incidence of furnace fires, analysis of incident causes, etc.). However, the limitations and inaccuracies must be recognised, particularly when such data is used for risk assessments. For example, only a limited sample of loss data may be available on the specific hazard under consideration.

"Near-miss" reporting also provides useful material for formal and informal training purposes. When establishing such a system, it is necessary to promote a flow of reports by demonstrating to the operating crews that they will be used constructively and not as a basis for criticism or disciplinary action.

7.8 Safety Department

In most companies, a Refinery Safety Department is established with responsibility for various advisory and safety promotion functions that are most conveniently handled by a group separate from the line departments. Depending on the local organisation structure, these may include activities such as the following:

- advice and assistance on special procedures, toxic hazards, use of work permits, personnel safety equipment, etc.;
- preparation and updating of a "Refinery Safety Manual";
- safety promotions, communications and publicity;
- safety incentive schemes, in which injury-free performance is recognised by monetary awards or gifts. Such schemes can prove effective in promoting safety awareness of the employees, but the limitations of such schemes should be recognised. Experience indicates that the desired motivating effect may be only temporary;
- responsibility for the refinery firefighting organisation and equipment;
- participation in the safety review of plant changes;
- compilation of records and statistics on industrial injuries. In addition to being required for statutory reporting purposes, this information may indicate problem areas where special safety activities should be initiated.

7.9 Employee Participation

The human element is a vital factor in the achievement of safe plant operations, and management should therefore strive to achieve a refinery organisation and culture which encourage safety awareness in the employees, and a conscientious approach in their work.

Open communications and discussion between all departments and levels in the organisation are an essential requirement for success in this area of motivation. In many countries, employee representation on works safety committees is required by law, but in any case there are clear advantages to be gained, in terms of motivation as well as utilisation of experience, from the involvement of plant personnel in the promotion of safe operations. Several of the activities mentioned in this Appendix will benefit from the participation and input of experienced operators, e.g. in the preparation and updating of operating manuals and procedures, model reviews on new projects, and equipment operability checks on new plants under construction.

concawe

methodologies for hazard analysis and risk assessment in the petroleum refining and storage industry

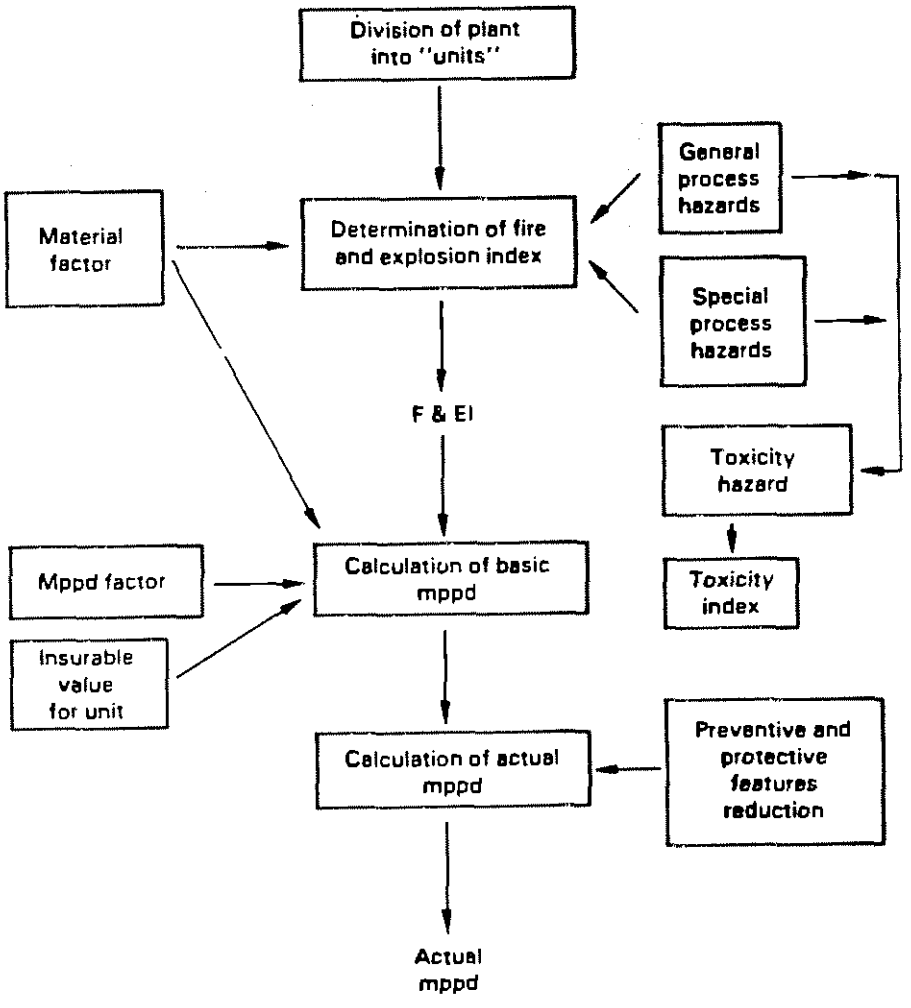
APPENDIX III – ANALYTICAL PROCEDURES

CONTENTS

1. DOW CHEMICAL COMPANY FIRE AND EXPLOSION INDEX HAZARD CLASSIFICATION GUIDE (THE DOW INDEX)

Originally, the Guide served to aid the selection of fire protection methods or provided the basis for the determination of a Fire and Explosion Index (F & E I). It has, in the fifth edition been further developed to enable evaluation of not only the F & E I and the Maximum Probable Property Damage (MPPD) but also the Maximum Probable Days Outage (MPDO) calculation. Some of the factors used in the procedure have been updated. Even in this edition, the Guide only covers process units and not auxiliary plant, such as power generation plant. However, for easy understanding Fig. 1 shows a simplified flow scheme of the procedure. Therefore the fifth edition of the Guide should be consulted when applying this technique.

Fig. 1 Simplified flow diagram for the Dow Index procedure (Dow Chemical Company: Fire and Explosion Index, Hazard Classification Guide).



A number of aspects are explored in deriving the F & E I. These are combined into three factors:

i) material factor

ii) general process hazards

iii) special process hazards.

The Material Factor is an indication of the energy potential of the most hazardous materials - including their likely combination - present in sufficient quantity in the processing plant, to cause hazard. The factor depends on two properties - flammability and reactivity. It may normally be selected from tables in the Guide.

The factor is calculated for each "unit" of the process. A "unit" is defined as ".... part of a plant that can be readily and locally characterised as a separate entity ....". The factor is then modified by two further weighting factors: General Process Hazards (GPH) and Special Process Hazards (SPH). Those in the SPH are wide, covering process temperature and pressure levels, sizes of inventory of flammable materials, potential for corrosion/erosion, how near the process operates to the flammable range etc.

Using the modified F & E I, an assessment is then made of the proposed presentation and protective features in the design, to determine their adequacy. The Guide lists "Basic Preventative and Protective Features". These, according to the nature of the hazard can be selected to reduce the level of potential risk reflected in the Index.

2. THE MOND FIRE, EXPLOSION & TOXICITY INDEX

This index procedure is based on that of the Dow Guide but allows more, and deeper, consideration of an installation e.g. loading/unloading facilities - which are not considered fully in the Dow Guide. Evaluation of hazard from materials, reactions and toxicity is also more extensive.

As in the Dow Guide, the installation is divided into "units". A Material Factor is calculated for each of these, the factor being weighted according to:

i) properties of the materials in the process

ii) the quantities involved

iii) the type of process and whether it is difficult to control

iv) the process conditions

v) materials of construction

vi) lay-out

All but the last item are similar in principle to the equivalent factor in the Dow Guide, although, again, they are developed to give a more comprehensive treatment.

The last factor is novel. It is intended to bring out more clearly the advantageous effects that spacing, access, structure height, drainage etc., can have on hazard potential.

Combination of these weighting factors with the Material Factor leads to a numerical value for a fire and explosion index. This allows the overall hazard to be ranked by comparison with the value of the index for "units of known fire and explosion risk".

The Mond procedure allows several other indices to be calculated - internal explosion, fire load, toxicity. All may be combined to give an overall index jointly representing these hazards.

The use of either Dow or Mond Index procedures at an early stage in a project could reveal hazard potential which it is relatively easy to alleviate before design is advanced. The effect of any design modification should be evaluated by recalculation of the index.

Either procedure can be carried out by a specialist. Better results will be obtained if a small team is used. The team should represent the various disciplines associated with the project; one of the members should be familiar with the index procedure.

For either procedure, a preliminary process flow sheet with rates and inventories is needed, supported by as much as is known at that stage about lay-out and size of equipment.

3. INSTANTANEOUS FRACTIONAL ANNUAL LOSS (IFAL) TECHNIQUE FOR QUANTIFYING HAZARDS

This technique has been used in the examination of petroleum refineries and chemical plant. Its primary aim is to provide a measure of the hazards of an operation through quantifying the losses - in terms of property, human life or production - which can result from them. An outline of the procedure used is given in reference (7).

This measure is expressed as an Instantaneous Fractional Annual Loss or IFAL.

The IFAL technique combines both the probability and consequences associated with hazards and is defined as "the expected average annual loss of that operation, expressed as a fraction of the value at risk". The annual loss is averaged over a number of years. It assumes that the installation is operated over this period under conditions obtained at the time of the evaluation. It is a characteristic property of the operation but its value will change as the process is modified, as equipment is changed or management standards altered. It will not vary as chance brings high or even low loss events.

Calculation of the IFAL requires assessment of three factors:

p - the process factor, representing the inherent hazards of the process;

e - the engineering factor, representing the "effect of engineering design and construction";

m - the management factor representing the "quality of management".

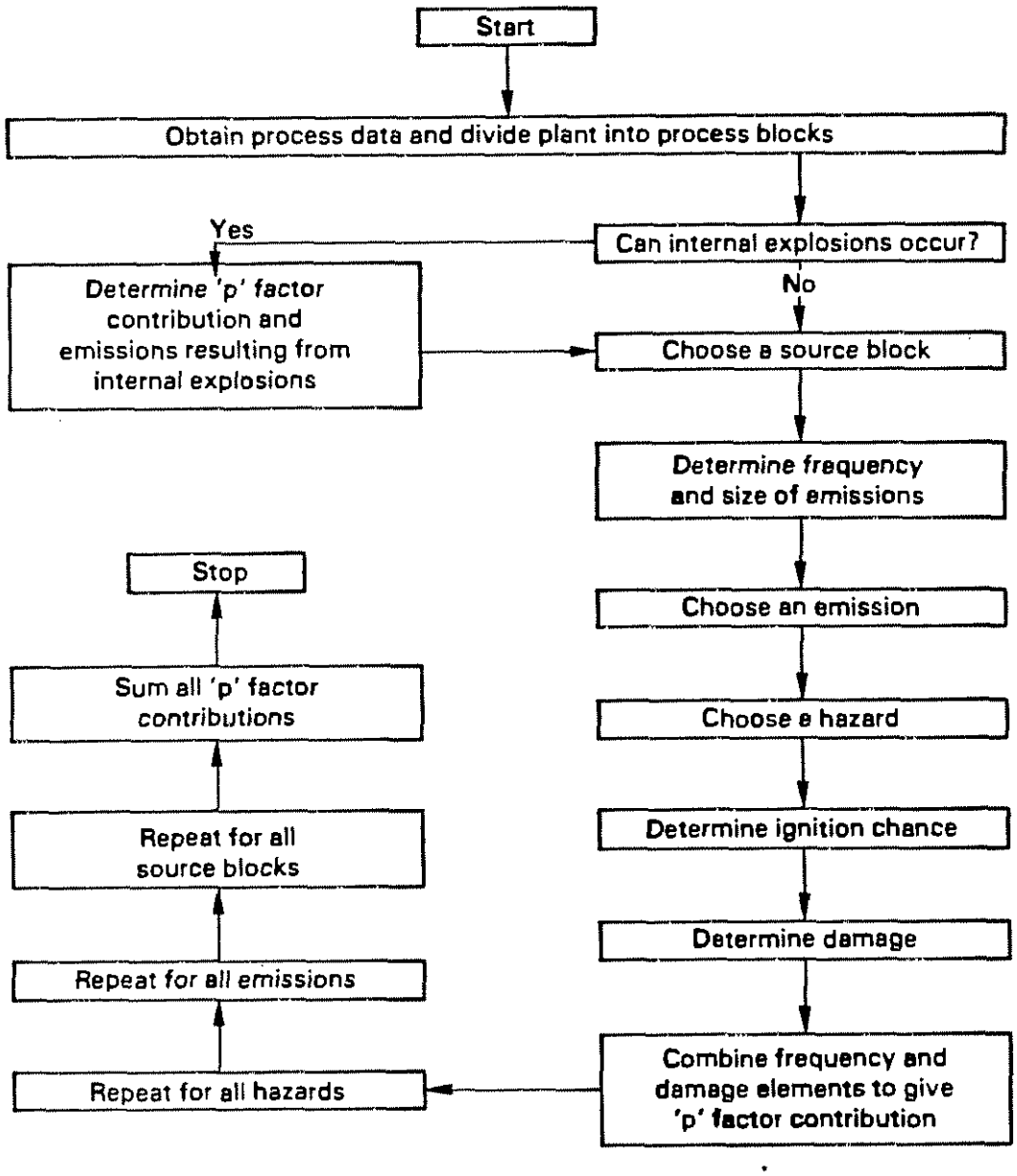
$$IFAL = p \times e \times m$$

The "process factor" is the basis for the IFAL calculation and assumes that the installation is designed, built and operated according to "Standard Good Practice"; "e" and "m" are then taken as unity and the IFAL numerically equals the value of the "p" factor. When the standard of engineering or of management is lower, then "e" and "m" become adjustments to the "p" factor.

Materials assets can be lost due to many hazards e.g. liquid fires, vapour fires, unconfined vapour cloud explosions, confined gas explosions and internal explosions in plant equipment.

Using an algorithmic approach, such hazards are considered in turn in deriving the "p" factor. The procedure is shown in Fig. 2 which is taken from published information (7). Basic data are process flow diagrams, lay-out drawings and physical and chemical data on the materials in process.

Fig.2 Algorithm for calculation of "p" factor in the IFAL technique – taken from Reference (7)



The installation is divided into blocks, in each of which potential releases of flammable material, their sizes, frequencies and chance of ignition are assessed. Damage is quantified not only for a block itself, but also due to "knock-on" effects.

The process factor is obtained by summing all these separate assessments.

Similar to the benefits of the Dow and Mond Index techniques, the IFAL procedure will provide suggestions on ways to reduce loss. Also the effect of one type of hazard can be compared with another because the examination of chains of event (e.g. loss of containment, emission, formation of a flammable mixture, ignition, etc.) enables different hazards to be seen in perspective. Hence suitable hazard reduction strategies can be chosen.

4. HAZARD AND OPERABILITY (HAZOP) STUDY

HAZOP is a systematic search technique for identification of hazards in process plant which is usually applied to piping and instrumentation (P&I) diagrams, with process and equipment data as supporting information. It is a versatile procedure which can be applied to complete plants, or to individual sections of plant, and to associated facilities such as storage, shipping, utilities, etc.

Its most valuable application is to the safety review of the design specification for a new project; but it can also be applied to preliminary flow-plans, and to existing plant for audit purposes or for evaluation of modifications or expansions.

The systematic and detailed nature of the procedure makes a team approach the best method of carrying out a HAZOP study. The standard of analysis and judgement also benefits from the interaction between group members.

The study is based on a procedure which systematically probes each part of the system for every process deviation from normal operation by generating questions, using a check-list of guidewords. The guidewords and their meanings are shown in Table 1 below.

Table 1 List of guide words

Guidewords	Meaning
None	No forward flow when there should be i.e. no flow or reverse flow
More of	More of a physical property than there should be e.g. higher flow rate or quantity, higher temperature...
Less of	Less of a physical property than there should be
Part of	Composition of the system different from what it should be e.g. change in ratio of components
More than	More components present than there should be e.g. extra phase present or impurities
Other	What else can happen apart from normal operation e.g. startup, shutdown...

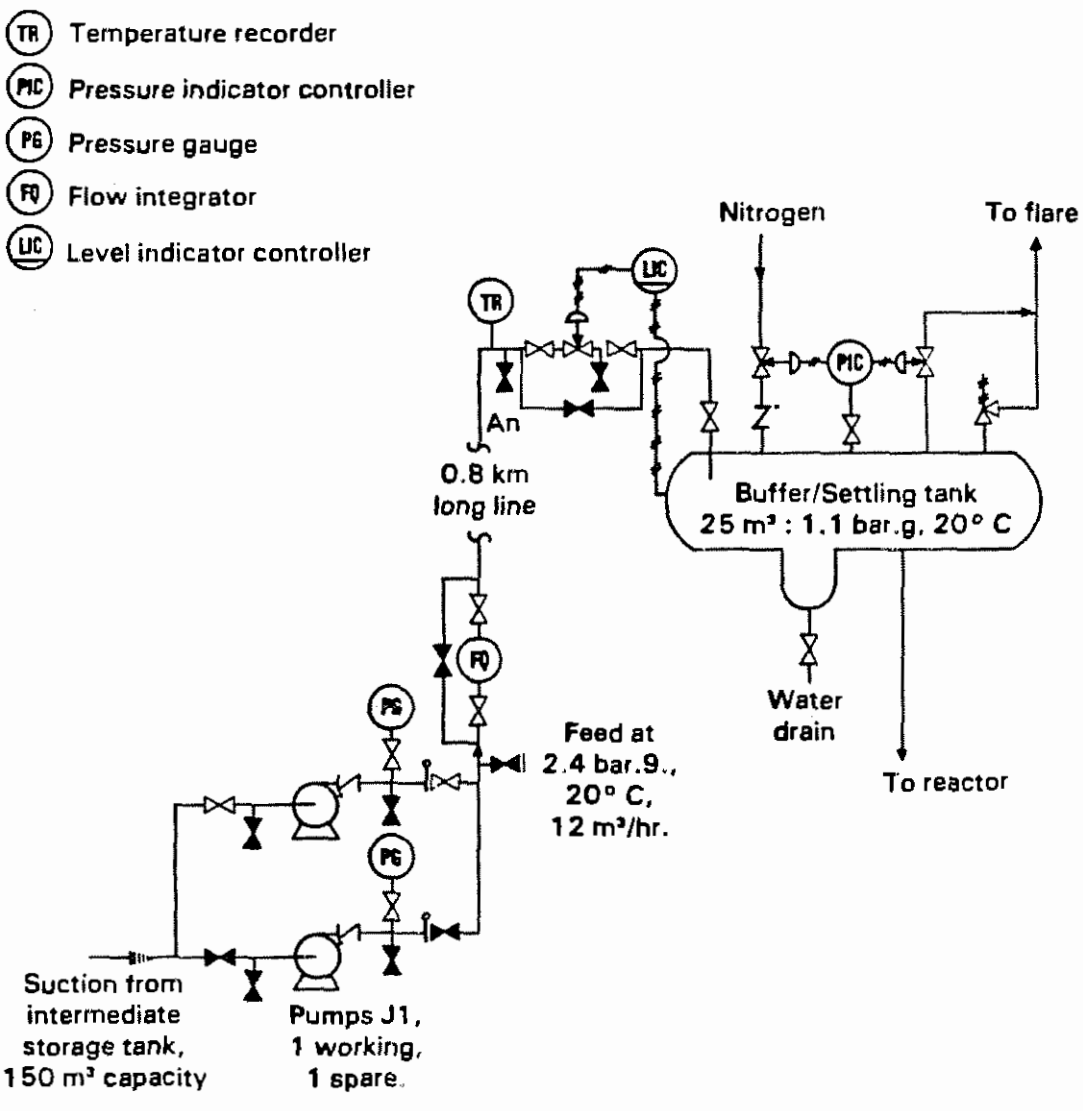
A modified example from a published practical HAZOP study (8) is described overleaf.

Example: Feed supply system to a process reactor

Using the HAZOP procedure, the feed supply system to a process reactor is studied for the "no flow" deviation, to establish the safety measures required.

A light hydrocarbon fraction is pumped from a nitrogen blanketed storage tank into another nitrogen blanketed buffer and settling tank supplying the process reactor. The two tanks are located on separate plants some 800 m apart, and the transfer line runs adjacent to a public road. The buffer tank at the reaction unit provides feedstock surge capacity and allows water, which has an adverse effect on the reaction, to settle out. The flow scheme is shown in the Fig 3.

Fig. 3 Example – hazard and operability (HAZOP) study: feed supply system to a process reactor



The results of applying the guideword "None" (in this case the flow) to identify causes, predict consequences, and decide the preventive actions required, are shown in Table 2 below.

Table 2 Application of guide word "none" to "flow"

Guideword	Deviation	Possible causes	Consequence	Action required
None	No flow	1. No feed available at the intermediate storage tank.	Loss of feed to the reactor and reduced output. Polymer will be formed under no flow conditions.	a) Ensure good communication with intermediate storage operator.
				b) Provide low level alarm on settling tank level indicator controller.
		2. Pump JI fails (variety of reasons).	As for 1.	As for b).
		3. Line blockage or isolation valve closed in error or control valve fails shut.	As for 1. Also pump will overheat.	Install reflux line on each pump. Check design of pump strainers.
		4. Line fracture.	As for 1. Also hydrocarbon will be discharged adjacent to public road.	Partly covered by b). But also institute regular patrolling and inspection of line

The record - which has the typical HAZOP format - only shows causes and consequences which were realistic and on which the need for action was agreed.

The need for action for each problem was decided by the study team on the basis of estimated seriousness of consequence and probability of the problem arising, the actual recommendation involving consideration of other alternatives.

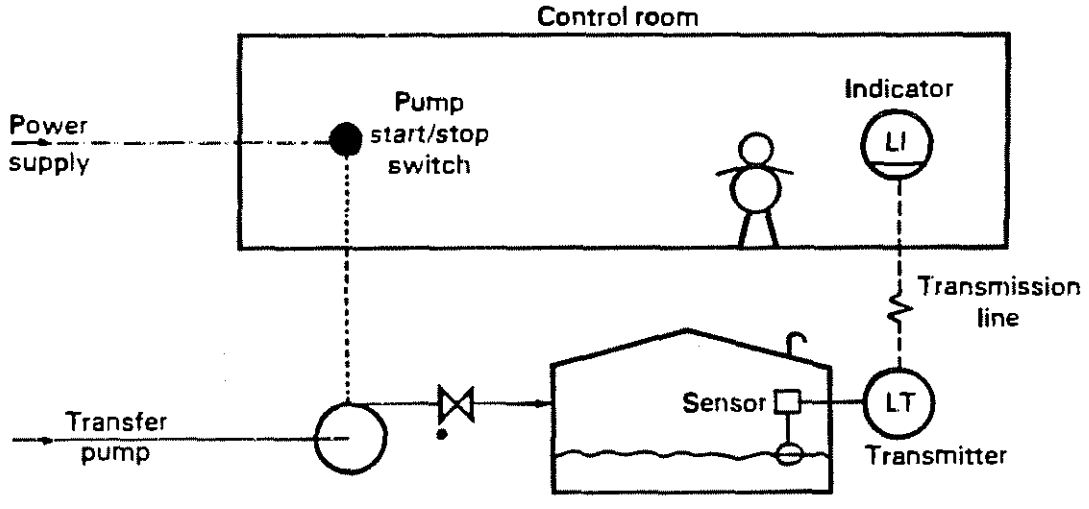
Whilst these results are in themselves significant, the potential problems having been clearly overlooked by the designers, the fuller account in reference (8) shows that a major risk was identified when the study proceeded into the plant section from the settling tank to the reactors.

5. FAULT TREE ANALYSIS

The principles of Fault Tree Analysis (FTA) are illustrated by a simple example involving the potential overfilling of a product storage tank (loss of containment event) in a refinery tank farm.

The operating system as shown in Fig. 4 consists of a tank being filled, a transfer pump which can be started and stopped from the control room, and a hand-operated valve in the tank inlet. The level measuring system includes a level transmitter (LT) at the tank-side and a level indicator (LI) located in the control room.

Fig. 4 Fault tree example – operating system



In practice, the operating systems described above would include an overflow line with a block valve (both not shown) and additional safety features e.g. different line-up, automatic pump shutdown, automatic valve shut-off, a high level alarm etc. These have all been omitted in the example for the sake of simplicity. Consequently considerations such as fractional dead time and test frequency for protective equipment have not been taken into account.

During the filling operations an abnormally high level occurs which leads to the overflow of the tank, through the vent. A fault tree shown in Fig. 5 illustrates the causative events and failure pathways, for this situation. The conditions for loss of containment, which lead to overflow and which is described in fault tree terminology as the "top event" are:

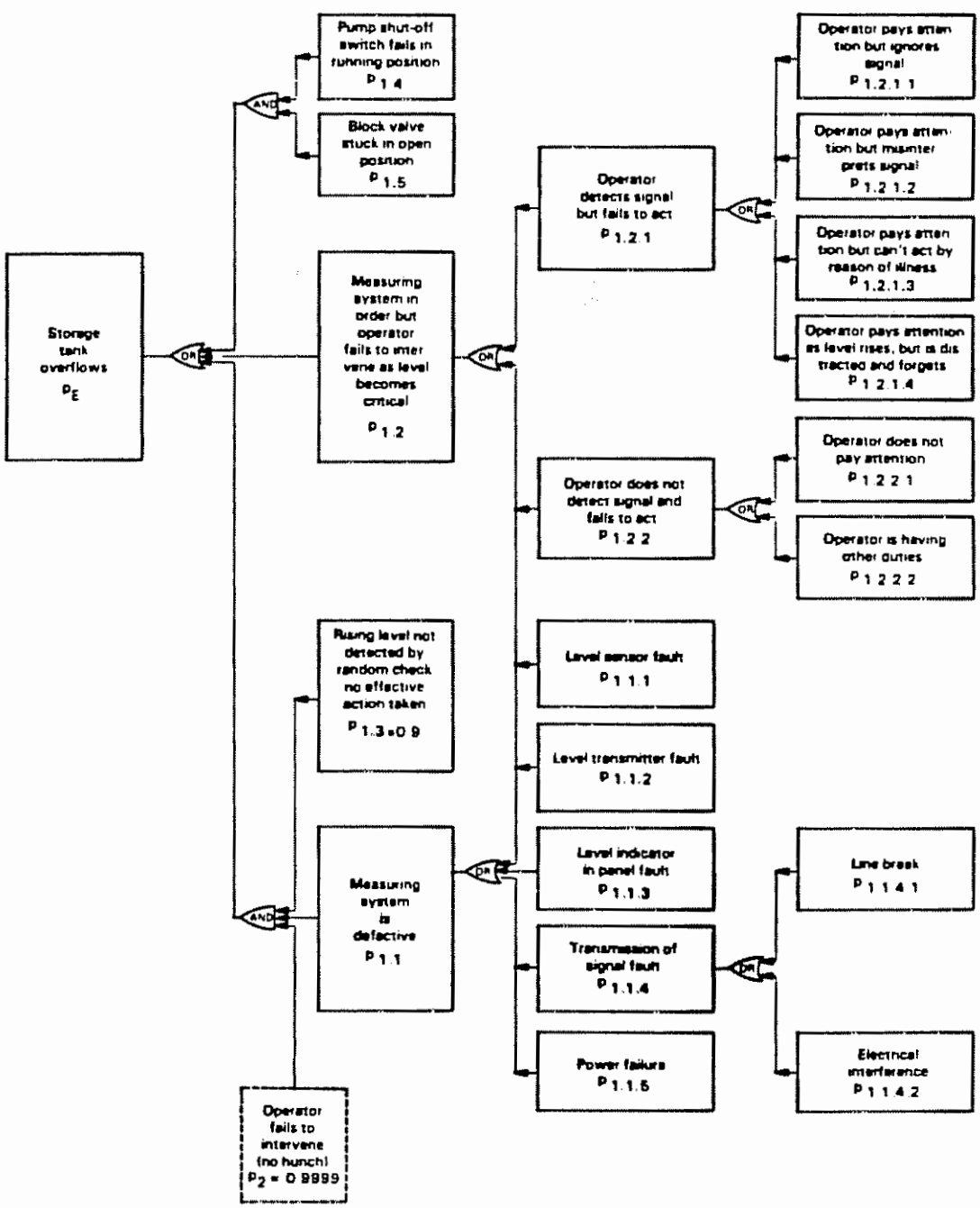
i) the level measuring system is defective before or during the high level phase, thereby giving the operator almost no chance to recognise the rising level and to stop the flow into the tank before overflow;

ii) the level measuring system functions and gives the correct signal but, either the operator ignores it and does not act to stop the rising level, or

iii) the operator does recognise the signal and attempts to switch off the pump and close the block valve: but he is not effective in stopping the level rising before the tank overflows.

The "top event", designated by p_E in Fig. 5 is traced back through all possible causative events p_1 $p_{1.1}$ etc. to causative events ($p_{1.1.4.1}$, $p_{1.2.3.2}$ etc.) This figure shows the failure pathways in the form of a fault tree of sequential events.

Fig. 5 Fault tree – illustrative flow scheme and assigned probabilities



The probability of the tank overflowing, P_E, can now be calculated, using the "tree" for the example of Fig. 5, bearing the following in mind:

a) the probabilities of events preceding an OR must be added;

b) the probabilities of events preceding and AND must be multiplied.

Thus:

$$P_E = P_{1.2} + P_{1.1} \times P_{1.3} \times P_2 + P_{1.4} \times P_{1.5}$$

$$P_{1.1} = P_{1.1.1} + P_{1.1.2} + P_{1.1.3} + P_{1.1.4.1} + P_{1.1.4.2} + P_{1.1.5}$$

$$P_{1.2} = P_{1.2.1} + P_{1.2.2}$$

$$= P_{1.2.1.1} + P_{1.2.1.2} + P_{1.2.1.3} + P_{1.2.1.4} + P_{1.2.2.1} + P_{1.2.2.2}$$

Note: The combination of probabilities shown above assumes that the events are mutually independent and their probabilities small.

The result of this calculation shows the probability or chance with which the tank could be expected to overflow. Instead of probabilities, frequencies (e.g. failures/year) could have been used. The "top event" would then have a frequency value. For instance "Overfilling can be expected once in .....years".

Using either probabilities or frequencies, the result could be used for comparison with results for similar systems or could be compared with a predetermined limiting value, as a first step towards deciding whether improvement was necessary. This can be aided by using other information such as operability and cost.

After such a comparison, the probability (or frequency) value of the top event may have to be improved. Closer examination of the fault tree will suggest possibilities. Earlier in the report the value of such an examination even of an unquantified tree is discussed (see section 4.2.1).

When typical data is used to quantify the tree, further information will be revealed. Suppose that the failure pathway $P_{1.2.1.2}$, $P_{1.2.1}$, $P_{1.2}$ is shown as making a significant contribution to the probability value for the "top event". This pathway starts with the event $P_{1.2.1.2}$: "Operator pays attention but misinterprets signal". The question should then be raised: "Why does the operator misinterpret the signal?". Can he see the instrument clearly and read it clearly? By this kind of analysis ways can be found to reduce the probabilities of causative events leading to the "top event", P_E (tank overflows).

Whether probability values are used or frequencies in both cases the values used should be derived from a reliable and consistent data base when comparing alternative designs.

6. FAILURE MODE AND EFFECT ANALYSIS

Failure Mode and Effect Analysis (FMEA) examines the behaviour and interaction of individual components in a plant or installation, to enable the consequences of their failure upon the safety of the operation to be assessed e.g. electrical system faults.

Part of the previous storage tank overfilling example is used to illustrate the method, namely the interruption of the transmission of a signal to the level indicator e.g. due to maintenance or construction work (fault designated $p_{1.1.4.1}$). From relevant information e.g. historical plant records and experience, the general probability of a signal transmission line in a specific area being interrupted is to be established as a first step:

Let the general probability be	5.2×10^{-4}	(p_i)
Will interruption be discovered by maintenance worker causing it?	Probability*	
	yes 0.97	
	no 0.03	(p_1)
If the answer is "no"	Probability*	
Will interruption be discovered by tank farm operator?	yes 0.1	
	no 0.9	(p_2)
If the answer is again "no"	Probability*	
Will other events identify the fault?	yes 0.05	
	no 0.95	(p_3)

Then probability for this chain of events leading to $p_{1.1.4.1}$ will be:

$$p_{1.1.4.1} = (p_i) \times (p_1) \times (p_2) \times (p_3)$$
$$= 5.2 \times 10^{-4} \times 0.03 \times 0.9 \times 0.95$$
$$= \underline{1.3 \times 10^{-5}}$$

Note: Only one sequence - the one leading to $p_{1.1.4.1}$ - has been considered in this example. In an actual analysis all other possible sequences have to be reviewed to ascertain that they cannot result in other "loss of containment" events.

---

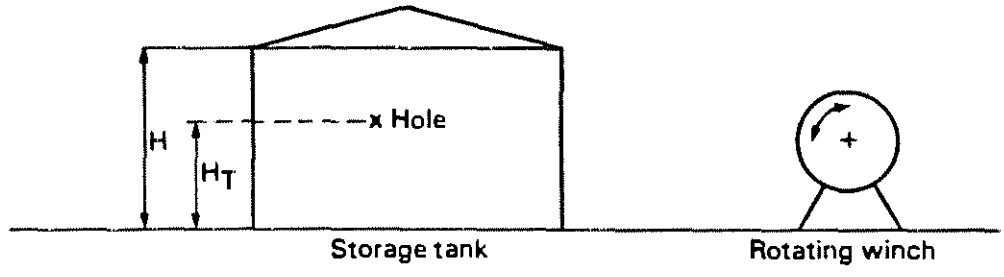
*Probability is estimated on the basis of actual plant circumstances.

7. RANDOM NUMBER SIMULATION ANALYSIS

7.1 Problem Definition

The example considers a rotating winch which disintegrates next to an oil storage tank of total height H and a fragment from the winch penetrates the shell of the tank at a height H_T above the base of the tank.

Fig. 6



What spill size must be expected?

7.2 Assumptions

- the disintegrating winch will generate a fragment of adequate size and kinetic energy to penetrate the shell of the tank;
- the fragment actually hits the tank and causes a hole big enough to permit the stored liquid to flow out of the tank;
- there is no interference by the operators of the installation to control the spill;
- the height of the point of impact (= hole) above ground is H_T which can assume a value between H and zero. It has the probability distribution shown in Fig. 7.
- the winch has no protective cover and it has been assumed that the probability of a "hit" is equal for the entire vertical extension of the tank wall except for the bottom part (5%) where a higher hit frequency is assumed due to fragments being reflected from the ground;
- the inventory level in the storage tank, H_I has, in the past shown a distribution pattern, typical for a storage tank (Fig. 8);
- no significant change in tank usage is expected in the future.

Fig. 7

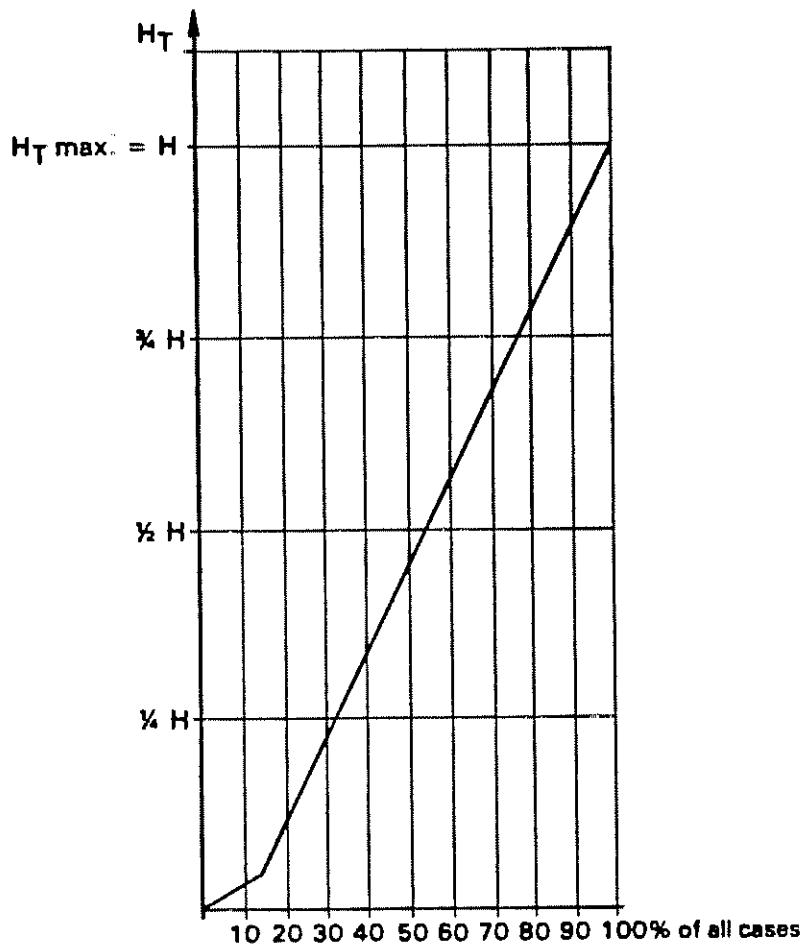
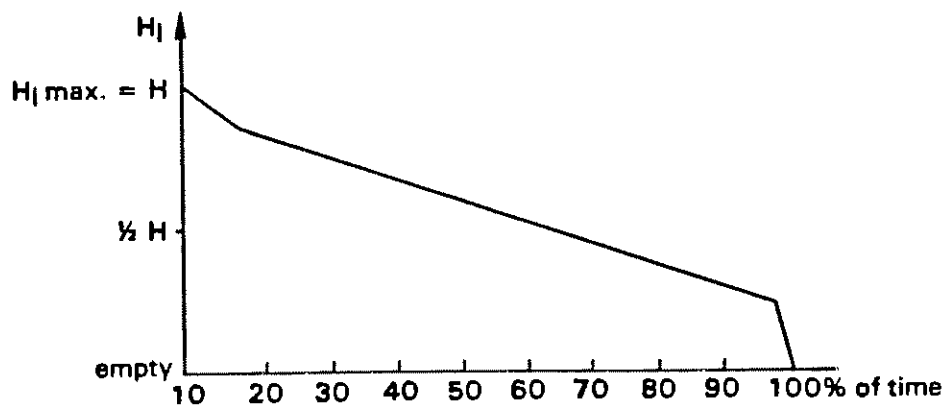

H_T
H_T max. = H
¾ H
½ H
¼ H
10 20 30 40 50 60 70 80 90 100% of all cases

Fig. 8


H_l
H_l max. = H
½ H
empty
10 20 30 40 50 60 70 80 90 100% of time

7.3 Procedure

It follows that the volume of a spill from a cylindrical tank will be approximately:

$$Q = r^2 \times \pi \times (H_I - H_T)$$

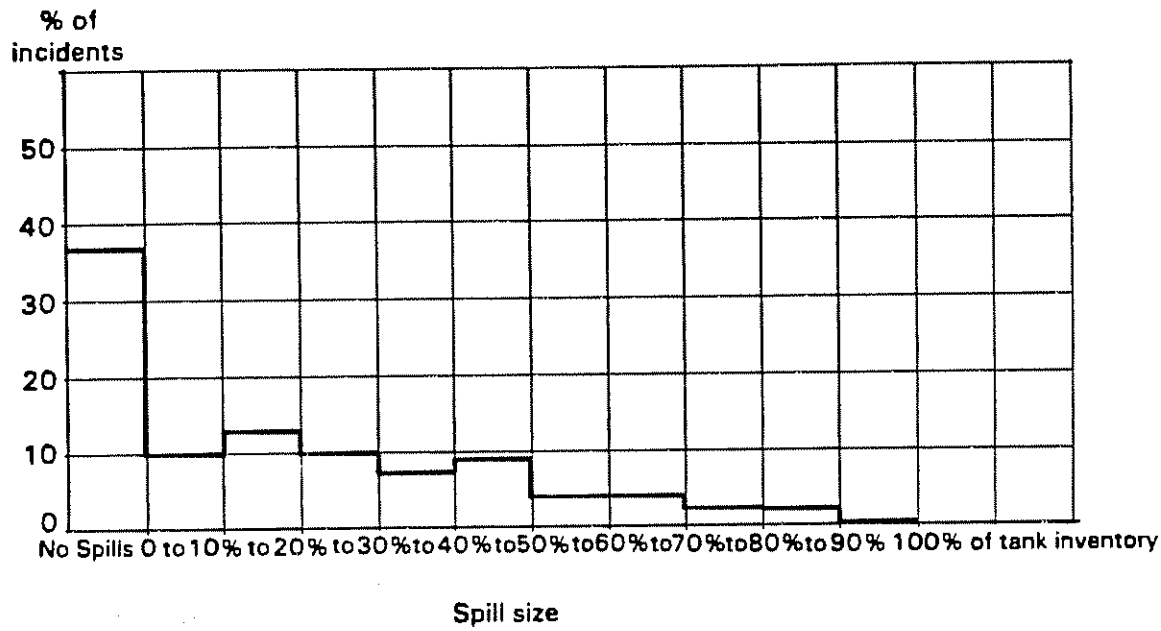
with r = radius of the tank and H_I and H_T ranging from 0 to H. Since the two variables i.e. the level of the inventory and the height of the hole from the ground, are independent from each other, a random number simulation analysis can be carried out.

Note: The distribution curves can have any desired discontinuities, multiple peaks etc. The volume of the spill has been calculated as described in section 4.2.3 selecting at random, varying values from the two probability distributions plotted above.
The results of repeated (=500) runs are shown in Table 3 and graphically in Fig. 9.

Table 3 Results of the simulation runs

Spill size	Per cent of cases	
	In category	Cumulative
No spill	37.00	
Spill less than 0.001 x H	0.25	37.25
Spills ranging from H multiplied by:		
0.001 to 0.01	0.75	38.00
0.01 to 0.1	9.25	47.25
0.1 to 0.2	13.25	47.25
0.2 to 0.3	9.75	70.00
0.3 to 0.4	6.50	76.50
0.4 to 0.5	9.00	25.50
0.5 to 0.6	4.50	90.00
0.6 to 0.7	4.50	91.50
0.7 to 0.8	2.75	97.25
0.8 to 0.9	2.25	99.50
0.9 to 1.0	0.50	100.00

Fig. 9 Percentage of incidents versus spill size



8. TECHNIQUES FOR HUMAN ERROR PREDICTION

8.1 Human Error Failure Rate Data

Human error failure rate data can be used as input to Fault Tree Analysis (FTA) and other quantitative hazard analysis techniques. Data covering a range of relatively simple tasks, relevant to the petroleum industry, are shown in Table 4. Human error failure rate data have been released by several authors. A concise description is given in (13).

Table 4 Human reliability

Task (under no stress or distraction)	Average No. of failures per 10,000 occurrences
Read technical instructions	82
Read electrical or flow meter	55
Inspect for loose bolts and clamps	45
Position multiple position electrical switch	43
Mark position of component	42
Inspect for bellows distortion	39
Install gasket	38
Inspect for rust and corrosion	37
Install "O" ring	35
Record a reading	34
Inspect for dents, cracks, and scratches	33
Read pressure gauge	31
Tighten nuts, bolts, and plugs	30
Connect electrical cable (threaded)	28
Inspect for air bubbles (leak check)	26
Install reducing adapter	25
Connect flexible hose	25
Lubricate bolt or plug	21
Position hand valves	21
Install nuts, plugs, and bolts	21
Lubricate "O" ring	21

Task (under no stress or distraction)	Average No. of failures per 10,000 occurrences
Fill sump with oil	19
Disconnect flexible hose	18
Install protective cover (friction fit)	17
Read time (watch)	17
Verify switch position	17
Close hand-valves	17
Install drain tube	17
Open hand-valves	15
Position two-position electrical switch	15
Verify component removed or installed	12
Remove nuts, plugs, and bolts	12
Install pressure cap	12
Remove protective closure	10
Remove reducing adapter	9
Remove pressure cap	8
Loosen nuts, bolts, and plugs	8
Remove drain tube	7
Verify light illuminated or extinguished	4
Install funnel or hose in can	3
Remove funnel from oil can	3

Attempts have also been made e.g. by A.D. Swain (13, 16) to rate the probability of human error against complexity of the operation Human error rates probably differ by one order of magnitude from those of protective equipment i.e. 10^{-2} for humans and 10^{-3} for protective equipment arranged in a system with "redundancy". Typical values for human errors in more complex tasks are shown in Table 5.

Table 5 Probability of operator failure to start corrective action (after A.D. Swain)

10^{-0}	Failure to operate second step of two closely coupled events, having failed to operate the first step.
	High stress time constrains: – available for action:
	0 to 1 minute, Probabilities of failing to act correctly 1
	up to 5 minutes .9
	up to 30 minutes .1
	Failure to detect state of e.g. valve, on general walk-round tour 0.5 if check-list used.
	Failure of non: routine, complicated operation.
10^{-1}	Personnel on different shift fail to check, e.g. plant item, .1 if required to do so by writen instruction or check-list.
	Failure of checker/monitor to recognise operator error, .1 if there is feedback, e.g. from annunciator, chart, etc.
	Operator is already reaching for wrong control, then fails to notice from, e.g. indicator lamp, that control is already at required state. If indicator shows control not at the desired level P = 1.
	Failure in non-routine operation when other duties present.
	Simple arithmetic error with self-checking.
10^{-2}	General error of omission, with no feedback display, e.g. failure to close valve after maintenance: 0.01 if special precautions, e.g. check-list, locking off, used.
	Failure in routine operation where some care is required.
	Error of omission of action embedded in a procedure.
	General error of commission, e.g. misreading label and hence selecting wrong switch.
10^{-3}	failure in routine, simple operations. Correct decision but wrong control selected when appearances are different.

8.2 Technique for Human Error Rate Prediction (THERP)

As a first step, this technique requires the establishment of a logical model covering the options a human being (e.g. an operator) encounters in the task under consideration. If, for instance, an event tree is used as a representative logical model, the branches of the tree in the diagram will show the success or failure probability of the various courses of action which are possible. Care must be taken to include all options, including "no-action taken" alternatives. In the following example after A.D. Swain (17) a flow chart diagram was established to illustrate the THERP technique (Fig. 10).

The situation is a steadily running plant. Analysis requires an estimate of the probability, with which the control room operator will not respond in a timely manner - say within 1 minute - to an alarm annunciator, when his attention is distracted by a second alarm.

The sequence in his response should be:

- recognition of the alarm
- deciding what to do
- start to take action.

Ideally it is assumed the operator would acknowledge the alarm by switching off the audio signal and then find which alarm window is lit in the annunciator panel. When he finds which alarm is flashing, he cancels the flasher and starts to take corrective action on the fault. The alarm remains lit - steadily - until the fault is corrected.

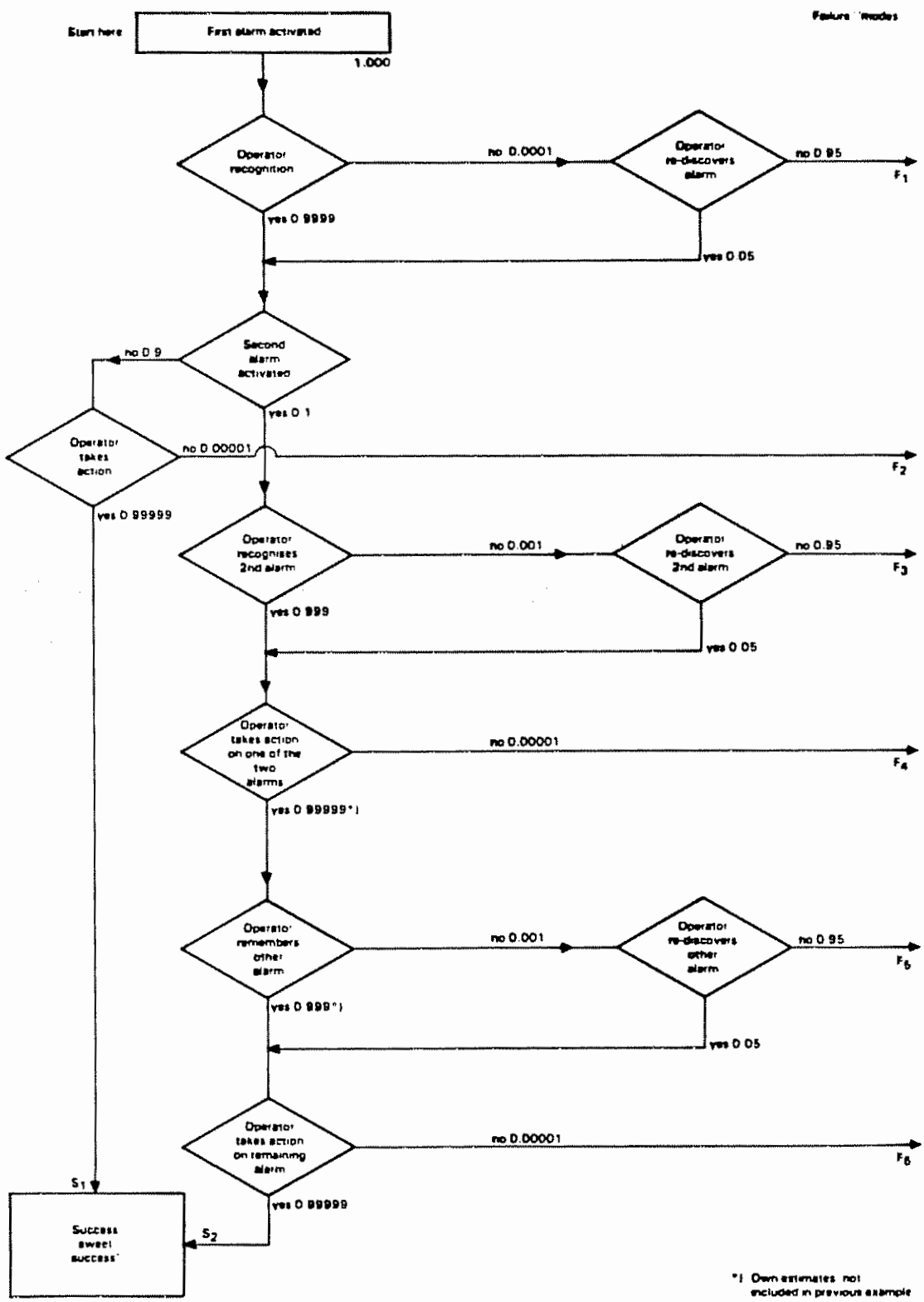
Experience indicates that for only one alarm indicating, the probability of the operator failing to act in this way is 10^{-4}.

Supposing, the operator is interrupted, as he recognises the first alarm, by a second alarm, before he can then decide what to do about the first. In a steadily running plant, this is somewhat unlikely. But to illustrate the THERP procedure, the example assumes a 10% chance of interruption.

Further, if the operator then fails to respond within the time of one minute required, the probability of failure increases from 10^{-4} to 10^{-3}. The longer he takes, the worse this probability becomes. This is because he increasingly tends to forget about the first alarm.

It could be that he will not detect the first alarm condition until he examines the panel on a routine scan, say one hour later, then realising that the window for the first alarm is still lit. In such circumstances the chance of him doing this, is estimated as 0.05.

Fig. 10 Flow diagram illustrating THERP technique



The THERP flow-chart shows these sequences and their estimated probabilities. It provides the basis for calculating the total failure probability and the necessity (or otherwise) to modify the system.

It can be seen that in this illustrative example, the probability that the operator will take the correct course of action is greater than 0.9997.

CALCULATION OF TOTAL FAILURE PROBABILITY

$$Pr\ (F) = F_1 + F_2 \ \ldots\ F_n = F$$

In example:

$F_1 = 0.95 \times 10^{-4}$

$F_2 = 10^{-5} \times 0.9 \times 0.9999$

$F_3 = 0.95 \times 0.001 \times 0.1 \times 0.9999$

$F_4 = 10^{-5} \times 0.999 \times 0.1 \times 0.9999$

$F_5 = 0.95 \times 10^{-3} \times 0.99999 \times 0.999 \times 0.1 \times 0.999$

$F_6 = 10^{-5} \times 0.999 \times 0.99999 \times 0.999 \times 0.1 \times 0.9999$

$F_1 = 0.95000 \times 10^{-4}$

$F_2 = 0.08999 \times 10^{-4}$

$F_3 = 0.94990 \times 10^{-4}$

$F_4 = 0.00999 \times 10^{-4}$

$F_5 = 0.94895 \times 10^{-4}$

$F_6 = 0.00998 \times 10^{-4}$

2.95881×10^{-4}

N.B.: The probability of success is:
$1 - Pr\ (F)$
(or 0.9997 in the above case)

9. STUDIES USING THE EPIDEMIOLOGICAL APPROACH

This technique can be applied to specific problems by analysing historical performance data on equipment failure e.g. involving fire. Examples of typical equipment to which this procedure can be applied are as follows:

- pumps (influence of failures of bearings, couplings, seals etc.);
- storage tanks (type of tank, tank service, effectiveness of fixed foam facilities etc.);
- furnaces (type of furnace, furnace services etc.).

From a study of previous records, using data bank sources (18, 19), the types of failure can be analysed and the design safety features reviewed.

An example of epidemiological analysis may be found in API RP2003, "Recommended Practice for Protection against Ignitions arising out of Static, Lightning and Stray Currents". Appendix D of this document contains an analysis of 115 fires during loading of petroleum products into tank trucks which were suspected to have resulted from electrostatic ignition. The reported data on the circumstances of these incidents enabled the significance of factors such as splash filling, switch loading, electrical bonding, loading line filter, etc., to be evaluated. This in turn contributed to the formulation of design and procedural recommendations for preventing electrostatic ignitions during tank truck loading operations.

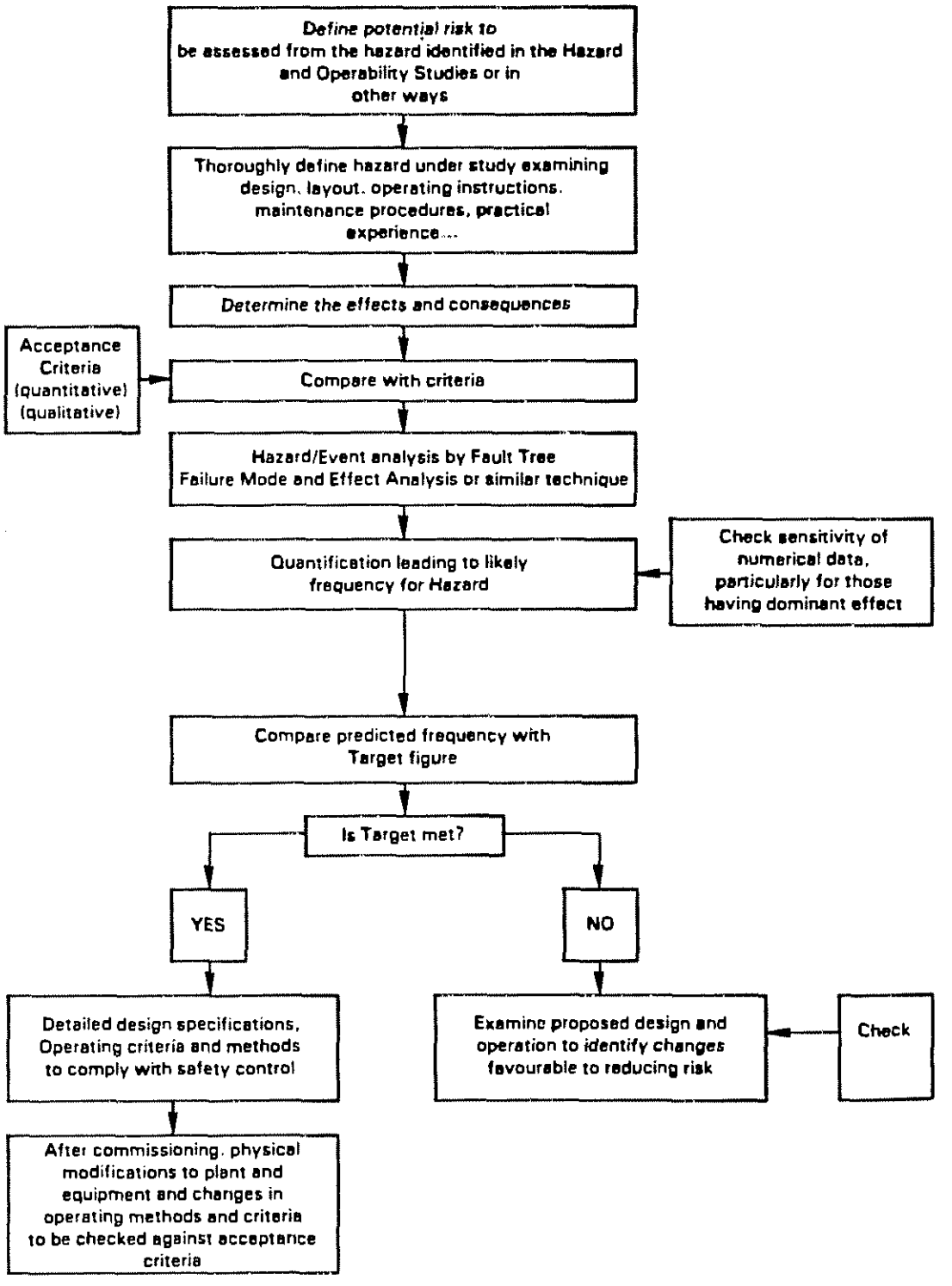
10. THE STRENGTHS AND LIMITATIONS OF THE ANALYTICAL PROCEDURES

Sections 4.1 and 4.2 of the report outlined the basic principles and applications of several qualitative and quantitative analysis techniques. A flow chart illustrating the procedure and logic sequence is shown in Fig. 11. The specific strengths and limitations of the methods are summarised in Table 6 below:

Table 6 Specific strengths and limitations of the various analytical procedures

Method	Used in petroleum industry	Strengths	Limitations	Comments
1 QUALITATIVE		-	-	Provide a more formalised and structured *approach to hazard identification*
1.1 Check-lists	Frequently	Straightforward, systematic conventional checking procedures	Effectiveness depends on thoroughness of check list preparation. May channel review into prescribed topics and inhibit creative analysis. Does not quantify or rank hazards	Particularly useful for checking compliance with standards etc
1.2 Hazard Indices				
Dow Fire and Explosion Index	Rarely	Can be used at an early stage of a project, and for audit of existing plant. Provides a criterion for safety design	Gives no credit for safety features already installed. Limited to fire and explosion hazards of process plant only	Developed primarily for fire and explosion for chemical processing industry
Mond Index	Rarely	Expands Dow Index to include consideration of storage and handling activities specific layout features and toxic materials in process. Uses some semi-quantitative factors	Still rather incomplete and requires experienced analysis	Mainly used in chemical processing industry
Instantaneous Fractional Annual Loss (IFAL)	Rarely	Enables estimation of physical damage from fire and explosion	Insurance orientated	Relatively new technique developed by the insurance business
1.3 Open-Ended Procedures				
Hazard and Operability Study (HAZOP)	Frequently	Systematic, comprehensive and flexible good method of identifying hazards and operability problems. Promotes exchange of ideas. Can be used semi-quantitatively	Requires use of study team with experience and judgement. Does not include detailed fault analysis. Not concerned with high hazard-low probability events	-
2 QUANTITATIVE		-	-	*Enable a numerical hazard analysis* to be carried out, which may incorporate probability estimates
2.1 Fault Tree Analysis (FTA)	Occasionally	Enables systematic construction of logic diagram of event sequences leading to specified failure. Versatile and useful qualitatively. Particularly suited to mechanistic options. Quantitatively enables more significant causative event sequences to be identified and ranked in order of priority	Time and rate dependent events not easily represented. Has to be applied selectively in complex systems for realistic use of *resources*. Choice of probability factors difficult and chain of events subject to bias of analyst. Event sequences may be overlooked	Starts from the failure event (top down)
2.2 Failure Mode and Effect (FMEA)	Less frequently	Enables all components and operating modes to be examined for results of failure. Very *rigorous and complete procedure*	Much more time consuming than FTA	Starts with individual components and operating modes to assess consequences of their failure ("bottom up")
2.3 Random Number Simulation (RNSA)	Limited	Based on logic model and enables failure events to be quantified in terms of a range of probabilities. Very flexible analytical tool. Conceptually more realistic than single numerical values	Identification of independent components difficult. Very detailed preparation and numerous repeated computations required	Usually requires access to data processing
2.4 Techniques for for Predicting Human Error (e.g. THERP)	Limited	Provides estimates of probability of human behaviour	Unpredictability of human reactions especially in abnormal circumstances	THERP provides input to *FTA, FMEA, etc*
2.5 Epidemiological Studies	Frequently	Examine past performance data for underlying failure rate relationships	Validity of conclusions very dependent on the quality of the data base, and statistical significance of anomalies found in a sample	Can be used for wide variety of purposes including input to other studies

Fig. 11 Flow chart – analytical procedures



concawe

methodologies for hazard analysis and risk assessment in the petroleum refining and storage industry

APPENDIX IV – TYPICAL PRACTICAL CHECK-LIST FOR RISK STUDIES

1. PLANNING A HAZARD ANALYSIS

- The objective of the analysis must be clear and explicit.
- The basis for the analysis must be defined and recorded.
- The hazard and cause types to be considered in the analysis must be defined.
- Make sure that there is agreement concerning access to information.
- Company employees, who may be involved or affected by the analysis, should be informed.
- Determine and define the form of publication, the readership and the distribution.
- The required standards of detail and certainty should be defined, and the standards for approval of the analysis set.
- Adequate allowance should be made for unforeseen hazards, or changes in priorities in the hazard analysis.

2. QUALITY OF HAZARD ANALYSIS

Hazard analyses differ widely in goal and circumstances. Not all analyses satisfy all requirements. In checking a hazard analysis the following points should be considered to the extent which is relevant.

- The basis for the analysis must be defined.
- The boundaries of the analysis must be defined in terms of plant limits and phases of operation.
- The methods used should be described adequately to allow the reader to repeat the analysis on a sample basis.
- The data for the analysis should be tested.
- The analysis should be repeatable using the same data.
- Specified threats to the plant from external sources should be included.
- The hazards arising from operation, maintenance or modification should be included.
- The possibilities of design error should be allowed for.

- The standards of plant management, maintenance and administration should be specified.
- The results should be compared with case histories of accidents in similar plant.
- The possibility of common cause (mode) and secondary failures should be considered.
- Operating and maintenance errors should be considered.
- The areas of uncertainty in the analysis should be described.
- The uncertain assumptions used in the analysis should be listed.
- Alternative assumptions should be investigated (sensitivity study).
- The results should be consistent with existing experience.
- Accident sequences should be described in sufficient detail for the reader to envisage and check the sequences.
- The analysis should be sufficiently detailed, and carried out in such a way that it satisfies its objectives.

concawe

methodologies for hazard analysis and risk assessment in the petroleum refining and storage industry

APPENDIX V – GLOSSARY OF TERMS

GLOSSARY OF TERMS

This glossary defines terms as they are used in this report. It includes some terms not mentioned in the report, but which may be encountered during wider reading on the subject.

Accident	Injury to a human being.
Accident rate	The number of reportable (definition may vary between countries and companies) accidents related to the number of persons working, or the total number of hours worked, or to units, produced in an installation, company etc. This enables, within limits, a comparison of the safety performance of various installations, companies etc. provided exactly the same definitions for the accident rate are used.
Bleve	See p. 18.
Common mode failure	The coincident failure of two or more independent components as the result of a single cause; of particular concern in an instrument system incorporating redundancy where an event causes coincident failure of two or more of the normally independent channels.
Criteria of acceptability	See section 5.2, p. 20.
Deflagration	The chemical oxidation reaction of hydrocarbon material in which the reaction front advances into the unreacted material at less than sonic velocity. A certain pressure rise will occur.
Demand	A disturbance or change in the process or plant outside normal design parameters which requires a response from a protective system.
Error	The deviation which can exist between the actual performance characteristic of a component, equipment or system, and the true or required value of such performance.

Error rate (human)	The frequency with which a human, e.g. an operator, makes an uncorrected mistake.
Event	In the context of risk, an event is an instantaneous happening and therefore having no duration.
Event tree	See section 4.2, p. 10.
Explosion	This is not a strictly scientific term but in the context of this report it refers to a rapid oxidation reaction usually involving hydrocarbons, leading to overpressure effects which cause blast damage. It does not include situations where there is a loud noise but without overpressure effects of any consequence. An explosion will mainly arise in the petroleum industry from the ignition of a hydrocarbon/air mixture within its explosive range and though it will probably be described as unconfined if it is outside a closed vessel, in practice it will nearly always be partially confined due to buildings and structures.
Failure	A condition of a component, equipment or system, in which the design intention is not met.
Failure mode	The manner in which a component, equipment or system fails as expressed by the consequences of failure. For example the "fail-safe" mode indicates that hazardous or otherwise harmful effects are minimal.
Failure rate	The frequency with which a component, equipment or system fails.
Fail-safe	See failure mode and section 4.2.2, p. 12.
Failure mode and effect analysis (FMEA)	See section 4.2.2, p. 12.
Fault tree	See section 4.2.1, p. 10.

Fireball	The phenomenon which may occur as the result of a deflagration of a vapour cloud which does not result in a blast wave. The burning cloud may rise due to buoyancy and will emit intensive radiation over a considerable area.
Hazard	A condition in the operation of a system with potential for initiating an incident or accident sequence.
Hazard analyses Hazard assessment	See section 2.1, p. 2.
Hazard and operability (HAZOP) study	See section 4.1.3, p. 9.
Incidence rate	See accident rate.
Loss of containment	The unintended release of process material hitherto retained within an enclosed space.
Lower/upper flammable limits	The proportion (usually expressed as a percentage) of hydrocarbon vapour in air below/above which combustion will not take place.
Liquefied petroleum gas	Light hydrocarbon material, gaseous at atmospheric pressure and temperature, but which can be held in the liquid state under pressure to facilitate storage and handling. LPG consists essentially of propane and butane.
Overpressure	In the context of this report, overpressure is the force exerted by the blast wave from an explosion. The "peak overpressure" is the excess over ambient pressure at a fixed point. A "peak reflected pressure" is generated if the blast wave strikes a flat surface. Note: The term overpressure has a different meaning which is used in the design of pressure relief devices for pressure vessels. In this case, overpressure refers to pressure increase in a vessel over the set pressure of its relieving device during discharge (Refer API definition of overpressure, API RP520—Part I, page 2).

Probability	A dimensionless measure of the likelihood of an event occurring. It is expressed numerically between 0 = impossible and 1 = certain.
Protective system	The equipment and procedures intended to respond to the onset of abnormal conditions so as to minimise damage, loss or injury.
Redundancy	The performance of the same overall function by a number of identical but independent means.
Reliability	The ability of components, equipment or systems to perform according to predetermined standards.
Risk	The probability of the realisation of potential for loss, damage or injury.
Risk Analyses Risk Assessment	See section 2.1, p. 2.
Synergistically	The working together, in a close way, of otherwise independent factors, such that their combined effect is greater than the sum of their individual effects.
Top event	An undesirable event taken as the starting point for the construction of a fault tree.
Unconfined vapour cloud explosion	The rapid combustion which occurs when a flammable vapour cloud formed in the open, following a major loss of containment, is ignited. Blast effects are produced.