INVESTIGATION OF NEAR-MISS EVENTS IN THE PROCESS INDUSTRIES USING HAZARD ANALYSIS METHODS.

By M.S FAIDI

MASTER OF PHILOSOPHY

UNIVERSITY OF EDINBURGH

1989

To my father may God bless his soul, my mother, my wife, my daugter,my brothers and sisters.

ABSTRACT

At the end of the 19th century and at the begining of the 20th century natural gas was only used as a source of heat. It was only during the late 50´s that, with the development of plastics, a new utilisation of natural gas was introduced. During the 60´s and the 70´s world demand for natural gas has considerably grown and its price has gone up allowing exporting countries like Algeria to develop their potentials of production.

Hassi R´Mel gas field is the 4th largest reservoir in the world with proved reserves of 3000 billion cubic meters of gas. Five natural gas processing plants have been installed with a daily production of 60 million cubic meters to answer the demand of both the national and international markets. The latest plant constructed by JGC (Japan Gas Corporation) was the MPP 4 (Module Processing Plant 4).

The primary objective of the study was to learn about the different techniques of hazard analysis and give a description and a review of some of them. To illustrate the study two examples of near-miss events were investigated.

ACKNOWLEDGEMENTS

I am most grateful to the Algerian government for their financial support.

I am also very grateful to Dr Dougal Drysdale, my project supervisor, for his continued support, encouragement, interest and guidance throughout the course of the work.

Thanks are certainly due to Dr E. Marchand for helpful discussions, to all the staff and students of the Unit of Fire Safety Engineering for being friendly and, to the typist for being patient in typing this thesis.

My thanks go especially to my wife and parents for their moral support.

DECLARATION

It is declared that all work and results in this thesis have been carried out and achieved by the author himself, and the thesis has been composed by him under the supervision of Dr D.D. Drysdale, unless otherwise stated.

Mohamed Said Faidi

Edinburgh

December 1989

TABLE OF CONTENTS.

CHAPTER I.

INTRODUCTION.

1. INTRODUCTION.

At the end of the 19th century and at the begining of the 20th century natural gas was only used as a source of heat. It was only during the late 50´s that, with the development of plastics, a new utilisation of natural gas was introduced. During the 60´s and the 70´s world demand for natural gas has considerably grown and its price has gone up allowing exporting countries like Algeria to develop their potentials of production.

Hassi R´Mel gas field is the 4th largest reservoir in the world with proved reserves of 3000 billion cubic meters of gas. Five natural gas processing plants have been installed with a daily production of 60 million cubic meters to answer the demand of both the national and international markets. The latest plant constructed by JGC (Japan Gas Corporation) was the MPP 4 (Module Processing Plant 4).

2. OBJECTIVE OF THE STUDY.

The primary objective of the study was to learn about

the different techniques of hazard analysis and give a description and a review of some of them. To illustrate the study two examples of near-miss events were investigated.

3. REASONS FOR THE STUDY.

The growth of the nuclear and aerospace industries in the mid 50´s and the 60´s necessitated the development of techniques which would assure the reliability and safety of the new and complex systems which were being designed. It was recognized that although learning from mistakes was of great value, methods for identifying and assessing the frequency and consequence of failure were needed if accidents involving large loss of life and capital were to be avoided.

It was not until the late 60´s that ICI led the way in applying and developing new techniques to help counteract the increasing risk associated with the large single stream chemical plants which were constructed to minimize production costs.

The effect of accidents at Feyzen and Flixborough was to give the discipline Loss Prevention Engineering a much needed boost. It brought an increased awarness of the shortcomings of the traditional design methods which omitted to pay close attention to the risk inherent in the processes that were being planned.

By the late 70's regular courses in hazard analysis were being run by several universities; some in conjunction with the professional institutions.

In common with other industries, oil companies have learnt from their experience of accidents. By investigating the causes, guidance is given and processes are modified in order to reduce the likelihood of hazard reccuring.

4. SUMMARY OF INVESTIGATION TECHNIQUE.

Four methods of hazard analysis were used to study the near miss-events which occured in certain parts of the process where the potential risk is the greatest.

The four methods selected were:

a)The Mond Index

b)Fault Tree Analysis

c)Cause Consequence Analysis, and

d)Failure Mode and Effects Analysis.

These methods represent different type of analysis being:

a)Points Scheme (Mond Index)

b)Event Orientated Analysis (FTA and CCA), and

c)Component Orientated Analysis (FMEA).

The analyses are qualitative and to some extent subjective being dependent on:

   a)The knowledge of the system studied

   b)The ease with which the methods can be applied,
     and

   c)The time taken to carry out the study.

5. LAYOUT OF THESIS.

In order to present the results of the study clearly, the analyses of the near-miss events occuring in the MPP 4 are to be found in Chapters 4 and 5.

Appendix A1 contains a list of the abreviations used throughout the text.

Chapter 2 reviews the development of risk analysis in the process industries.

A short review of the generic types of hazard analysis and some details about the methods in each type is given in chapter 3.

Appendices C1, C2, C3 and C4 present a detailed review of the different methods of analysis used in this study.

Chapter 6 presents some conclusions and recommendations. Their aim is to provide the engineer with the advice he requires in order to make the most of investigating

near-miss events.

A detailed description of the process, piping and instrumentation diagrams are contained in appendices B1 and B2.

CHAPTER II.

RISK ANALYSIS.

1. INTRODUCTION.

In the past thirty years the rapid growth of industrial activities has resulted in many new problems related to environmental protection, energy, resource conservation and safety. Industry has been continually developing its design methods and operating techniques in order to overcome these problems. The process industries, which operate chemical, petrochemical and petroleum refining plants, handle a wide range of flammable and toxic materials wich are potentially hazardous. These industries have had an exellent safety record when compared with industry as a whole. Nevertheless the few major incidents which have occured have made public aware of the hazards involved.

In this period rapid developments were occuring in other fields of new technology, such as the use of atomic energy for power generation and in the aircraft and aerospace industries. Here little relevant experience for assessing the safety aspects of new designs was available from the past and this led to the development of quantitative risk analysis techniques for decisions in the area of

reliability and safety.

As a result, interest in the use of quantified risk analysis techniques for assessing the safety of process plants has grown considerably in Europe, both within industry and within national authorities.

The terms used in systematic safety analysis and assessment are not rigidly defined. They are interchangeably used by different authors.

To provide more understanding of the way I shall use terms Hazard Analysis, Risk Analysis, Reliability Analysis and the like, this chapter discusses what each term commonly means. Several methods of analysis are also briefly described.

2. RELIABILITY ANALYSIS.

The reliability of a component, device or system is defined as the probability that an item will perform a required function under stated conditions for a stated period of time.

Reliability analysis is the term given to the methods used to determine the reliability of a component. For example, historical records of failure rates could be used to determine the reliability of each component of a system when it is being studied. The interactions of the

components are then investigated and functional dependency diagrams are drawn to illustrate them. From this a mathematical model of the ways in which the system will fail is constructed; usually by drawing a fault tree.

The main objective of reliability analysis is to indicate methods of ensuring that the unavailability of the system is minimized and kept to an economically acceptable level.

3. HAZARD ANALYSIS.

Hazard is the term used to describe the existance of a condition or a set of conditions which may result in the occurrence of an event which will cause loss of life, injury to the public, the operating personnel or damage to the plant.

The inherent characteristics of a petrochemical plant make the whole complex a hazard. The nature of the hazardous events that may occur provide the analyst with the basis upon which to compare plant with plant, or units within a plant with similar units. As a result, it can be said that one plant or unit is more hazardous than another.

Hazard Analysis is to a certain degree a misuse of the term hazard, since the analysis concentrates on the ways in which hazardous events occur because of the hazard

identified as being inherent in the plant. ·

For example, a pressure vessel is a hazard. Because it operates at a pressure there is a chance that the it will rupture. A vessel that operates at a pressure of 150 bar is thought to be more hazardous than a vessel that operates at a pressure of 15 bar. The probability of rupture will be similar given that both vessels are designed according to the same mathematical relationships. However, the consequences that may result are more serious if the 150 bar vessel ruptures, since more energy will be released. When comparisons are made they include the perception of the probability of occurrence and that of the possible consequences. Hence, the 150 bar vessel is said to be more dangerous than the other. It is also well known that the consequences resulting from 100 individual vessel ruptures will not be identical.

If loss of life is to be considered, the probability that a person is in the vicinity of the vessel, and the probability that this person will be killed when the rupture occurs must be taken into account.

The risk is the sum of all possible consequences with the probability of rupture. The term risk is applied also to the possible consequences of the occurrence of a natural calamity, an earthquake for example.

Hazard analysis is the method or methods which

identifies hazards, and analyses hazardous events. Simple
events which may lead to the occurrence of a hazardous
event are identified and their relationship is
investigated. These simple events may themselves be
hazardous! They are at the least undesirable. The hazard
analysis can be purely qualitative, or the probability of
occurrence of hazardous events may be quantified.

In a hazard analysis external events are not taken into
consideration. It only processes hazardous events which
may happen in the system being studied. Where external
events which may cause the top event are considered, a
risk analysis is carried out. For example, if the
occurrence of an explosion in a gas plant was being
studied, the possibility of a sabotage would be excluded
in a hazard analysis, but included in a risk analysis.

Hazard analysis does not investigate the consequences
that may be caused by hazardous events. Some authors make
no distinction between hazard and risk. They perceive
hazard as being an assessment of probability and the
extent of the consequences of hazardous events. However,
the word hazard is not used in this sense in the text.

The degree of hazard, and the hazard potential, are
terms used to describe the product of probability of
occurrence and consequence. They are synonymous with risk.
They are solely used in connection with a specific item or
plant, and therefore do not include the risk associated

with external events. These terms are used sparingly in the text. Where they are used, it is because the author of the method of analysis being discussed uses the term.

4. HAZARD IDENTIFICATION.

4.1 Hazard Identification.

Before an assessment of hazardous events can take place, the hazard associated with the system or process being studied must be identified (see chapter 3).

The quality of the analysis depends on the successful identification of all the hazards inherent in the system. A technique used commonly to identify potential hazards is a checklist. Checklists provide a means for ensuring that a process conforms to existing codes and standards of good practice. The checklist is valuable but restricted when considering a new process which utilizes new technology.

Hazard Indices are methods designed to give a quantitative indication of the potential for hazardous incidents associated with a given plant. Their most efficient use is in ranking processes against each other and thus directing attention to the worst cases. Standards and codes of practice have evolved from many years of experience in processing hazardous materials. Application of these practices can protect against a large number of hazards previously encountered and contribute

significantly to designing a plant capable of safe operation. The inherent weakness is that codes are not specific and lag behind new technologies.

Fundamental methods of hazard identification such as Hazard and Operability Study (HAZOP), and Failure Mode and Effects Analysis (FMEA) have been developed as a result of the increasing complexity of plants. They are aimed at two particular out-comes. Firstly, there is the identification of serious incidents which may result directly in danger to employees or the public, or in a financial loss. These incidents are usually known as the "Top event". Secondly, the fundamental methods can be used to identify the underlying root causes which can lead to the top event. Another advantage is that if the review takes place during the design phase of the project, particularly with HAZOP, operating problems are identified and can be rectified before the plant is commissioned.

Hazard identification has always been an integral part of the design and operational practice. However, it was to a large degree an informal process dependent on experience of those directly involved.

4.2 Comparative Methods.

These methods, such as used by Exxon Chemicals (1), use engineering codes and practices as the standards against which the acceptability of the design is evaluated.

An important advantage of these methods (or checklists) is that the lessons learned over many years of experience are incorporated in the company's practices and thus are available to be used at all stages in the design and construction of the plant. The main task of the hazard identification study is to ensure that the company's practices, and therefore its past experience, have indeed been incorporated in the design.

4.3 Fundamental Methods.

4.3.1 Hazard indices.

Hazard indices such as that developed by the Dow Chemical Company (2) and extended by Lewis (3) are methods which are designed to give a quantitative indication of the potential for hazardous incidents associated with a given design of plant.

4.3.2 Hazard and operability studies.

The most widely known of these is that published by H.G.Lawley of ICI (4) and later published by Kletz under the title "HAZOP & HAZAN: Notes on the Indentification an Assessment of Hazards"(5).

4.3.3 Failure modes and effects analysis.

Failure modes and effects analysis (6) is based on identifying the possible failure modes of each component of the system and predicting the consequences of the failure.

4.3.4 Fault tree analysis.

Fault tree analysis works from a chosen 'top event', such as 'fire in reboiler', and then considers the combination of failures and conditions which could cause the event to occur. Both failure modes and effects analysis and fault tree analysis are useful aids to hazard identification as they both structure and document the analysis. However, because they involve very detailed analysis of components and operations, their use on the process industry is mainly limited to identification of special hazards where they form the basis of quantification of risks.

4.3.5 Event tree analysis.

Event trees which work from a chosen 'bottom event' consider the developments which may follow the top event of a fault tree. However, they can also be useful for helping to establish the various sequences of events which may lead from a failure of a piece of equipment through to the release of flammable or toxic material from the plant.

4.3.6 Common-cause failure analysis.

In fire prevention problems, things may not be independent. Dependencies exist with regard to failure. To identify these and categorize these, is the subject of common-cause failure analysis.

A common-cause failure is a secondary cause of failure which can develop more than one component malfunction. Analysis of such causes is directed towards the cause of the component failure rather than the specific event which causes this failure.

4.4 Ease Of Application.

Hazard identification is an important part of the safety assessment of a plant. The depth of the study and the technique to be used has to be chosen to suit the situation. When the process is concerned with hazardous reactions or toxic materials the hazard identification must begin at the research stage and be continued through the pilot plant or process development stages of a project. Project approval procedures should include the requirements for potential hazards reviews at appropriate stages from the inspection of the project, through the project completion and during the life of the operating plant. The type and depth of studies should be determined by the needs at each stage.

4.4.1 Data availability.

Successful hazard identification depends upon having documentation to review which truly reflects the way the plant will be built and operated. The quality of the hazard study is improved by having the designer present his design to the study team.

4.4.2 Method selection.

The methods selected for hazard identification (or the combination of methods) should be the methods which best fit into the other design and hazard control activities of the particular organisation. For example, where the process is an assembly of previously used equipment modules operating within previously accepted limits, companies who have well documented engineering and design practices, will find it appropriate to use a comparative method similar to that of Exxon Chemicals (checklists). Where significant new technology is involved either in terms of process equipment or previously unknown reactions or process conditions, the fundamental methods such as Hazop would generally be prefered.

4.4.3 Report.

The report of the hazard identification study to senior management should be sufficiently detailed to communicate the concerns of the study team. It also should adequately describe how each hazard was controlled but not attempt to

show the precision of the survey by listing how the identification has been carried out.

4.4.4 Team methods.

It has been noticed, when using team methods for hazard identification, both for new projects and existing plant, that in addition to attaining safer design, the operating performance is also improved by the better understanding and motivation of the operating and maintenance people who have participated in the studies.

4.5 Future Developments In Hazard Identification.

Hazard identification procedures are probably the best developed element of risk analysis. Thus the future will probably not see much fundamental development of the methods. One area which may be explored is the automation of hazard identification based on computer modeling of the plant. However, the complexity of logic involved and the degree of 'experience' which would need to be built into the system suggest that we are still several years away from having a tool powerful enough to significantly help the analysts.

5. WHAT IS RISK ANALYSIS?

Risk analysis investigates the possible consequences of a hazardous event, as well as determining its causes. In

this way it differs from hazard analysis which does not investigate consequences. Risk analysis considers risk from all sources. For example, a risk analysis of a module in Hassi R'Mel field would include the consequence of a plane crash (an airport existing on the field), an earthquake or of a process fire or explosion.

Risk analysis can be summarized by three questions.
    -What can go wrong?
    -What are the effects and consequences?
    -How often will it happen?

The first and basic step of hazard identification (the first question) is purely qualitative and is often called a safety study. Such a study may reveal aspects of the plant or installation which require more consideration. It is then necessary to answer the next two questions in order to complete the risk analysis. The results of the analysis are used for judgement about the acceptability of the risk and for decision making.

Qualitative answers are often given to the second question. However, recent developments have involved the application of quantitative techniques for obtaining answers to this question and the third one.

Unlike hazard analysis, risk analysis considers events which are initiated by external events, and predicts the probability and the extent of the consequences.

Risk analysis is the more comprehensive of the two methods and often includes the lost production due to plant downtime, thus necessitating a complete reliability study of all systems on the plant.

6. CONSEQUENCE ANALYSIS.

Consequence analysis is a very large subject. Cause-consequence diagrams are constructed by defining a critical event, and then both defining the consequence events and paths which flow from the critical event and defining cause events for the critical event and logical relations between the cause events. The areas which merit further work in this field are seen to be:

6.1 Two Phase Flow Release.

Methods of estimating two phase flow releases from equipment and piping and for determining the subsequent vaporisation of the released material are still not satisfactory. More work is required in this field.

6.2 Heavy Gas Dispersion.

Considerable work has been done in the field of heavy gas dispersion. However, many assumptions still have to be made concerning terrain and topography. Further work will be necessary, both in wind tunnels and on ground, if a

better understanding of dispersion in actual situations is to be achieved.

6.3 Explosions.

The situations which lead to flame acceleration, so that ignition of a gas cloud gives an explosion rather than a flash fire, are still not understood. Work should proceed towards a better understanding of the phenomena since this could lead to the development of revised plant design and layout concepts in order to minimise the possibility of an explosion if there is a release of a flammable vapour or gas.

6.4 Toxic Gas Releases.

Prediction of injury caused by toxic gas releases is at an early stage of development. Injury assessments tend to be strongly focussed towards large numbers of injuries or fatalities, well above the level that has been experienced in past incidents. More consideration should be given to this problem.

6.5 Consequence Phenomena.

Experimental work on consequence phenomena has to be carried out on a large scale in order to establish scaling laws. Field experiments can be costly and require considerable resources. The present trend towards

cooperative research in this field should be continued.

7. QUANTIFICATION OF RISK.

7.1 Logic Diagrams.

Logic diagrams provide a valuable addition to traditional techniques for investigating failure mechanics. In particular, they allow a thorough understanding of an activity to be built up. This enables persons not familiar with that activity to bring an independent viewpoint to an established procedure or operation. It assists in identification of key areas and provide an aid to communication on how systems may fail and what effect modifications might have. However, the purely qualitative use of such tools does not give all possible information. Quantification can provide a clearer indication of the relative importance of the various causes of an undesired event. Quantification enables one to see more clearly the relative importance of an undesired event in the overall safety of a particular activity in which a number of such events is possible. It is in judging this importance that quantification can prove useful, giving clearer insight into performance of systems.

7.2 Data Sharing.

Information sharing schemes and data banks have a vital

role to play as long as problems and inhibitions regarding commercial confidentiality can be avoided. The problem of demonstrating very high reliability, i.e. obtaining a statistically meaningful sample for rare events, will always remain. Data collection may well proceed independently of quantitative risk analysis, as much of the data is useful in reliability studies.

7.3 Human Error.

Human error is often an important factor in the logic chain which leads to an unwanted event. Identification of the role that human error plays can in itself provide insight into the failure process (see section 9 of this chapter). Data on the probability of human error quoted in the literature, although based on a number of studies, is still arbitrary and uncertain. Human reliability is expected to remain largely intractable to quantification for specific cases.

7.4 Quantification Of Event Probabilities And Risks.

The quantification of event probabilities and risks contains many uncertainties. The quality of data is extremly variable, and errors can be made if the analyst is not fully aware of the theoretical basis of the relatively simple mathematical tools which are used. If an organisation is to use the techniques it must ensure that it has adequate resources and expertise to do the work.

8. ACQUISITION OF PROBABILITIES.

8.1 Mathematical Description of Component Behaviour.

The probability with which a component adopts its two possible states in practical work is taken to be either a constant value or is described by an exponential distribution.

If the behaviour of a component i is characterized by a constant probability, either its unavailability, U_i (the probability of being in a failed state), or its complementary value, the availability, $P_i = 1-U_i$, are indicated. If the description is in terms of an exponential distribution, the corresponding probability density function is:

$$F_i(t) = (1/T_i)\exp(-t/T_i) \qquad (t>0)\ (T_i>0) \qquad (1)$$

where T_i is the mean time to failure for component i.

Equation 1 yields upon integration over time t the unreliability (the probability that component i experiences its first failure up to time t):

$$Q_i(t) = 1-\exp(-t/T_i) \qquad (t>0)\ (T_i>0) \qquad (2)$$

In Equations 1 and 2, T_i is the mean time to failure for components of type i. This parameter is the inverse of the frequently used failure rate @, i.e., $@=1/T_i$, which gives the probability of failure in an infinitesimal increment

of time under the condition that the component has not failed before (see 8.2)

Constant failure probabilities are used for components which have to function on demand, such as interuptors, if their life time principally depends on the number of demands they have experienced. However, this is not always the case since the lifetime of components of this type is apparently more strongly influenced by factors which depend on the period of installation (such as corrosion). Thus, a description in terms of failure rates is usually preferred (7). Other fields of application for constant failure probabilities are the treatment of human error and of operational characteristics. In addition, they may be used for components subjected to maintenance whose unavailability is given by:

downtime /(downtime + functioning time)   (3)

In Equation 3 the downtime is the period during which the component is out of service, either because its failure has not been detected or because it is disconnected during its repair. In all other cases failure rates are generally used.

Failure rates are generally supposed to exhibit a time behaviour which can be described by the so-called "bathtub curve". At the beginning of component lifetime failures are relatively frequent (burn-in period). After that

follows a time interval with virtually constant failure rate. Toward the end of the lifetime another increase due to aging can be observed (8).

In addition to the quality of the components maintenance has an influence on system performance. Two basic types of maintenance may be distinguished: preventive and corrective. In preventive maintenance, periodic inspections are carried out which are meant to discover anomalies which have not yet led to a failure and remedy them before a failure occurs. Corrective maintenance implies repair or substitution of the component after its failure has occured. A mathematical maintenance description may be achieved using the theory of Markov processes or renewal theory (9).

The model for periodic inspection is valid under the following conditions:

* The lifetime of the component may be described by an exponential distribution
* The time between inspections is constant throughout component lifetime
* Failures are only detected on the occasion of an inspection
* The duration of the repair is negligible compared with the mean time to failure of the component
* After inspection the component is assumed to be "as good as new".

8.2 Reliability Data For Process Plant Analysis.

The reliability data should ideally have been obtained in a system which is similar to that under investigaion (similar components work under similar operating conditions). This goal may be satisfied in the case of specific types of nuclear reactors using the data compiled in Reference 1. On the other hand, the data obtained from the literature (10,11) do not supply component characteristics and give hardly any indication as to operation conditions. The knowledge of both is essential for making an adequate choice of reliability data in quantification of hazards.

8.3 Uncertainties.

Uncertainties exist in the estimation of reliability data. In the case of technical components these may be due to: differences in the performance of components on the same class and grouping together of similar but not identical components working under similar but not identical operating conditions; if data from the literature are used, values are necessarily selected from different sources without knowing whether component designs and operating conditions are comparable, and it is very probable that they are not. For this reason use of a statistical distribution for unavailabilities and failure rates is indicated instead of a single point value.

Usually a lognormal distribution is chosen for this purpose because it fits observed data reasonably well (7).

9. HUMAN ERROR.

Thus far only failures of technical components have been considered. Since technical systems, however advanced their level of automation, still rely on human intervention in some respects, a hazard analysis would be incomplete if this aspect were neglected. In modern process plants direct operator control is unusual. Automatic controllers generally ensure that process parameters are maintained close to nominal levels, except perhaps for start-up and shut-down, when an increased degree of human intervention is normally required. The operator's job therefore usually consists of a number of intermittent activities such as (12):

a) Operational tasks:

* Sequential control, starting pumps and motors, opening and closing valves etc., during start-up and shut-down, and batch processing operations

* More direct control of process parameters when control loops are not working

* Monitoring the plant for correct operation (compared with expected performance)

* Carrying out manual operations such as loading materials into hoppers and carrying out manually steered operations such as crane control

* Collecting and changing paper on chart recorders

* Completing plant production and operation log books

* Taking samples and operating instruments

* Alarm response and diagnosis of unusual plant conditions

* Reporting and following up equipment failures

b) Maintenance task:

* Adjusting manually controlled valves and pipe couplings for correct line up

* Adjusting set points for control loops and valve positions.

Human error quantification is, at present, only possible for the failure of an operator to carry out a planned intervention (e.g., opening a valve to increase the coolant flow when the temperature gets too high). Unplanned acts (playing around with buttons or changing positions of valve because of absent-mindedness or with the intention of causing harm) cannot be quantified. Even if this limitation is accepted, human error quantification still remains less exact than the quantification of the failure of technical components. Therefore, it may be recommended to calculate bounds for system reliability, assuming on the one hand perfect human intervention (U=0) and complete failure (U=1) on the other (13).

Human error is most frequently treated by the methods described in Reference 10. A human error is defined there

as an act outside tolerence limits. It is evident that the permissible interval of tolerance depends on the type of human act in question and on the circumstances under which it is carried out. The definition has to be made by the analyst in the light of these aspects. Usually the following kinds of human error are distinguished:

Error of omission: Faiure to perform a task or part of
                       a task
Error of commission: Performing a task incorrectly
Extraneous   act: Introducing some task which should
                       not have been performed
Sequential error: Performing some task out of sequence
Timing error: Failure to perform a task within the
                       allotted time or performing them too
                       early or too late.

The basis for the evaluation of human error is the identification of the acts to be carried out and their analysis. Important parameters to be established are the moment of the intervention, the time available for their realisation, the information at hand (instrument readings, knowledge of process behaviour, computerised information supply, etc.), and the possibility of correction if the initially required intervention has not been carried out. Ergonomic and environmental aspects have to be considered as well. In addition, it is important to take into account possible dependencies of human acts. These may be due to factors such as elevated stress which would affect several

consecutive acts realised by the same person or circumstances which would influence the action of two different persons trying to carry out the same act such as difficult access to the place of intervention.

The most widely used method for human error quantification is THERP (Technique for Human Error Prediction), which is discussed in detail in Reference 14. It is based on assigning error probabilities to simple tasks and breaking down more complicated tasks into simple ones, whose probabilities are combined according to the laws of probability in order to obtain the error probability of the complicated task. In addition, performance shaping factors (factors affecting these probabilities significantly) are taken into account by multiplying the base values, which apply to "normal" conditions, with them. In Reference 14 a great number of such performance shaping factors are discussed. In the present context only a few of the more important ones are commented upon:

9.1 Ergonomic Layout Of The Control Room.

An increase of failure probabilities is to be assumed if the arrangement, labeling, and design of the control mechanisms is such that error is enhanced. This may be the case, for example, if labeling of instruments and buttons is confusing or hardly legible or if stereotypes are violated (A stereotype is the expected reaction of a human

to an outside influence: for example, turning a button in a clockwise direction is associated with switching on).

9.2 Feedback Through Indicators And Alarms.

The probability of human failure is reduced, if feedback through indications and alarms which render the detection of probable error exists. The possibility of the discovery of an error is to be taken into account especially if the operator is warned immediately after committing it. This applies most of all if the system response to error is rapid.

9.3 Human Redundancy.

A further important way of detecting errors results from human redundancy, i.e., a decision of an act involves more than one person with adequate qualification. Redundancy is also assumed if a person's acts are controlled by another.

9.4 Pschycological Stress.

Stress is a very important factor for human performance. If it is too low, i.e., work is of routine type and considered as boring, error becomes more probable. If stress is very high, on the other hand, error again becomes very probable, reaching the value 1 for dangerous situations. This value should be adopted, for example, for interventions during a runaway reaction, if it implies

getting close to the reactor. Between these two extremes, there lies an optimal stress range which is assumed for control room work during normal operation, maintenance work, and testing.

9.5 Qualification And Training Of Operators.

Among other factors, appropriate qualification for work to be done is essential for avoiding errors. This implies neither under nor overqualification and includes general education and a specific understanding of the bases and procedures of the process in question. Another important aspect in this context is the training for emergency situations which helps to maintain an acceptable level of emergency response probability. This probability would otherwise decrease in the course of time.

9.6 Written Instructions.

A good explanation of what should be done in operating the plant both in normal and emergency conditions in written form tends to reduce the probability of human error.

Human error is treated in fault tree analysis by analogy with the failure of technical components. Its quantification, however, is much more complicated than that of the latter and requires the collaboration of experts from various disciplines such as engineering,

psychology, ergonomy, and statistics.

10. THE APPLICATION OF RISK ANALYSIS.

10.1 Some Limitations Of Quantified Risk Analysis.

A quantified risk analysis will have covered hazard identification, selection of risk senarios and quantification of the consequences and probabilities. Before we arrive at a judgement on its acceptability we have to consider the characteristics of the assessment of consequences and probabilities that have been carried out.

In many cases only very general data are available on equipment failure, for which statistical accuracy is often poor. In other cases there may be very little data available at all. This applies in particular to data on human failures. Data may have an accuracy no better than a factor of ten so that, when combined in a fault tree, they lead to incident frequencies that will have wider confidence limits although they may not necessarily be less accurate.

The lower the estimated probability of a hazard is, the wider will be the confidence limits of the calculated figure. Therefore, it is not possible to compare the frequencies of two catastrophic events at e.g. 10^{-5} and 10^{-6} per year and be confident about which event is more likely to happen.

The quantification of the effects and consequences of incidents also have large uncertainties associated with them. Methods of estimating dense gas dispersion and the effects of an ignition of flammable gas clouds are still at the development stage and the rest of the data will contain many assumptions.

The analytical models have been developed in an attempt to give a quantitative understanding of physical phenomena. In practice however, there are many uncertainties. A small event can lead to a major accident or only have a localised effect (for instance a release of flammable hydrocarbons).

The whole analytical exercise might be considered to be objective. However, it must be realised that because of the large body of assumptions, estimates, judgements and opinions involved, much of the input information is often subjective.

Because of these limitations considerable skill is needed to interpret the results produced by a quantified risk analysis. At the present state of development these techniques should only be used by those who understand their limitations and then only with caution.

10.2 Application In The Process Domain.

Qualitative methods for the identification of hazards have been used for many years by the process industries to ensure that their plants are adequately safe. It should be remembered that these methods are used to audit a design which should already meet the many codes of practice (both from the authorities and from the company) which cover most aspects of the engineering of the plant. Whilst a number of large companies have found benefit from the use of quantified risk analysis, it must be recognised that others in the process industry have not found it necessary. These companies, although well aware of the quantification methods, judge that the outcomes of quantitative risk analysis studies are not producing results on which they can rely or which contribute much to making a plant safer. They rely on identification procedures coupled with good engineering judgement, experience from actual practice and experiment, and regulations and guidelines. The availability of a large body of long term technical experience embodied in proven codes of practice obviates the use of quantitative methods.

Consequence calculations are becoming more widely used, particularly by companies handling large quantities of flammable or toxic liquefied gases. These can be useful for determining plant siting and layout. They can also be used by the people concerned with planning emergency procedures. However, there is always a possibility that too much weight is given to the largest possible

consequences if a judgement of the probability of the event occuring is not taken into account. If potential consequences are considered alone this may lead to unnecessary additions to a plant and excessive capital cost.

A company using quantitative risk analysis will use its own experience and judgement to define targets against which to compare the results. This comparison will assist them for example to decide on the degree of redundancy required in an instrument protection system for plant handling an exothermic reaction.

Not withstanding the problems that still exist in the use of quantitative risk analysis for safety decision making, definite advantages are available if it is used prudently, particularly where new technology is involved. Benefits are to be gained in obtaining a better insight into causes of potential plant failures. The quantification of these can help with an understanding of the relative importance of the causes and assist with the development of improved designs. For these reasons selective use of quantitative risk analysis "in house" as one of the tools to assist with decision making. Any organisation considering a move in this direction should ensure that it has adequate expertise to handle the analytical techniques properly.

10.3 The Way Forward.

Quantification of risk may support safety decisions about plant involving step changes of scale, complexity or technology. The need for this should become apparent when the initial process safety analysis is carried out.

Recent and continuing developments in the process industries are also influencing the development of quantitative risk analysis. For instance we have:

-computer technology

-large integrated process plant complexes

-the higher education requirements that are needed for people handling these new systems.

These will have an influence on the development of methodologies for analysing risk situations for people and the environment in which they live. Areas in which change can be expected are:

-A combination of reliability and risk studies with more multi-disciplinary analytical methods, including long term toxicological effects.

-Machine/operator relationship (e.g. ergonomics and training).

-Better exchange of data via data banks (computer networks).

-Better understanding of ways of dealing with uncerainties, where there is a lack of knowledge and data.

-A combination of quantitative risk analysis and

cost/benefit analysis as part of the decision process.

The position of quantitative risk analysis in the future will depend on how well the analytical methods can give answers which are needed. An important aspect will be their development into a form in which the results can be meaningfully communicated from the analysts to others, e.g. managers, politicians, the public.

However, even with these developments, quantitative risk analysis remain a small part of the total safety package. The main requirements for safe process plant will always be good engineering, well qualified personnel and good management.

11. REFERENCES.

1)Solomon C.H., The Exxon Chemicals Methods for Identifying Potential Process Hazards. I.Chem.E. Loss Prevention Bulletin No. 52, Aug. 1983.

2) Dow Chemical Company, Fire and Explosion Index, Hazard Classification Guide, 5th Edition, 1981.

3)Lewis D.J., The Mond Fire Explosion And Toxicity Index _ A Development of The Dow Index Presented at the AICHeE Loss Prevention Symposium Houston, April 1979.

4)Lawley, Chem. Eng. Process _Vol 18, No 5, P. 105-116, 1973.

5)Kletz, T. A., "HAZOP & HAZAN: Notes on the Identification and Assessment of Hazards", Loss Prevention, The Inst. of Chem. Eng., ISBN 0-85295-165-5, Rugby, U.K., 1983.

6)US Departement Of Defence, "Military Standard Procedures For Performing A Failure Mode, Effects And Critically Analysis", MIL-SDT-1629 A, Washington DC 20362, Nov. 1980.

7) Homke, P., Krause, H.W., Ropers, W., Verstegen, C., Schlenker, H.V., Huren, H., Dorre, D., and Tsekouras, A., (ZerverlassigkeitskenngroBenermittlung im Kernkraftwerk Biblis - AbschluBbericht), Rep. no. GRS-A-1030, Gesellschaft fur Reaktorisicherheit, Cologne, 1984.

8) Barlow, R.E. and Proschan, F., (Statistical Theory of Reliability and Life Testing - Probability Models), Holt, Rinehart, & winston, New York, 1975.

9) Cox, D.R., "Renewal Theory", Methuen, London, 1962.

10) Anyakora, S.N., Engel, G.F.H., and Lees, F.P., "Some data on reliability of instruments in the chemical plant environment", Chem. Eng., p.396, November 1971.

11) Skala, V., "Improving instruments service factors",

Instrum. Technol., p.27, November 1974.

12) Taylor, J.R., "A Background to Risk Analysis", Vol. 1-4, Riso Research Centre, Roskilde, Denmark, 1979.

13) Hauptmanns, U. and Sastre, H., "Safety analysis of a plant for the production of vinyl acetate", J. Chem. Eng. Jpn., 17(2), 165, 1984.

14) Swain, A.D. and Guttman, H.E., "Handbook on Human Reliability Analysis with Emphasis on Nuclear Plant Applications", NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, D.C., 1983.

CHAPTER III.

DESCRIPTION OF HAZARD EVALUATION PROCEDURES.

1. INTRODUCTION.

This chapter describes a variety of hazard evaluation procedures that are being used in the chemical and petrochemical industries. These procedures have been developed to identify the hazards that exist, the consequences that might occur as a result of the hazards, the likelihood that events might take place that would cause an accident with such a consequence, and the likelihood that safety systems, mitigating systems and emergency alarms would function properly and eliminate or reduce the consequences.

The different hazard evaluation procedures can be classified into four generic types:

> a)Point Schemes
>
> b)Checklists
>
> c)Component Orientated Technique, and
>
> d)Event Orientated Technique

Each type has its own purpose and function.

Each category contains several evaluation procedures some of which will be described in the following sections. References for each procedure are given at the end of this chapter.

2. POINTS SCHEMES.

A point scheme is a rapid tool in which each factor which increases or reduces the risk is assigned a score. The total score is then compared with a standard value which represents a predefined acceptable level of risk.

The best use of a points scheme is to identify areas which are more in need of attention than others. A review of a chemical works may indicate that the risk associated with one process is more significant than the risk from the other processes on the site.

2.1 The Mond Index.

This method has been developed from an initial approach used for insurance assessments by chemical organisations along the lines of identifying features of plant or other activities which have been historically associated with many incidents. Its primary aim is to roughly rank hazards of a wide ranging character on the basis that they are a function of:

    a) The activity carried out, and

    b) The nature of the materials being handled.

It is always assessed without any allowance for safety features and practices and hence gives as the first result obtained a measure of the hazard potential for a "worst case". A key advantage of the technique is that it can be applied at very early stages of design or development before decisions on equipment selection and layout have to be finalised. It does not require the availability of detailed piping and instrumentation diagrams for its use and is thus quite different to conventional hazard analysis where much detailed information is necessary.

Such an assessment made early in a development can identify problems so that they can be avoided and the results of the modified assessments by this method can form a major input to the preparation of Safety Cases and in carrying out emergency planning activities. This is because it enables a "worst case" assessment to be considered as recommended by Cassidy (see references).

The use of the "worst case" assessment is not a complete answer to the assessment of plant units especially where spacing requirements are concerned. Hence, a range of "offsetting" safety factors are incorporated in the second part of the Mond Index technique. These factors provide a mean of reducing the "worst case" potential to arrive at a result that represents the activity as is likely to be actually operated and maintained.

Many of the "offsetting" factors relate to features such

as training and experience plus safety features incorporated into the plant as a result of hazard studies (including fire protection and fire fighting). Included in them are consideration of general safety pratices for a site as a whole.

A direct benefit of the early use of the Mond Index technique is that it allows a relative assessment to be made of the hazard potential as "worst cases" for various parts of a whole plant/system so that more extensive hazard study and related activities can be allocated in proportion to relative unit hazard levels. Otherwise, such allocations of effort have to be based on judgements which may or may not be sound.

2.2 Instantaneous Fractional Annual Loss Method.

The Insurance Technical Bureau (ITB now part of the Loss Prevention Council) has developed a method of calculating the expected average loss from fire and explosion for plants handling flammable materials. The method is synthetic, calculating the course of the events leading to loss from data on the materials being handled, the main plant items, and the layout. This technique provides the insurance industry with the means of calculating insurance premiums in a more systematic way and in a manner that more accurately evaluates the financial risk that companies underwrite when insuring a plant.

IFAL is the average fractional loss per year which a system will sutain if it were to operate unchanged and in an unchanging environment for a very long time. The loss may be lives or money or whatever is the hazard of primary concern. IFAL is not just an index of hazard. It is a measure. It does not simply rank hazards as the Mond Index do. It rates them in absolute terms. The IFAL numbers can be manipulated arithmetically in calculations concerning expected loss. So far the technique is being used to rate the hazard of property loss from fire and explosion, but it should be adaptable to hazard resulting in loss of life or injuries to the personnel and public.

The IFAL is a function of the process hazards, the standard of engineering, and the way in which the process is managed.

Like the Mond Index, IAFL can be used to investigate changes in:

a)The layout of the plant

b)Measures taken to prevent hazardous events occurring, and

c)Protective systems which limit the damage plant that may occur.

However, it does not appear that its evaluation of preventive and protective measures is as developed as that in the Mond Index.

IFAL is basically empirical, the systematic mathematical procedure using available failure rate data. The difficulty of acquiring adequate reliable basic information is a weakness which hopefully will improve with time and effort (see chapter 2). The procedure is involving and time consuming, event with computer help. It needs expert handling.

3. CHECKLISTS.

A checklist is a summary of good design procedures and is an expression of senior design personnel who have collaborated to pass on their experience in the form of codes of practice and design rules. It can also high-light a lack of basic information or a situation that requires a detailed evaluation. The results obtained are qualitative. They vary with the specific situation, but generally they lead to a "yes-or-no" decision about compliance with standard procedures.

3.1 Preliminary Hazard Analysis.

A Preliminary Hazard Analysis (PHA), as described herein, is an analysis which is part of the U.S. Military Standard System Safety Program Requirements. The main purpose of this analysis is to recognise hazards early, thus saving time and cost which could result from major plant redesigns if hazards are discovered at a later

stage. Many chemical companies use similar procedure under a different name. It is generally applied during the concept or early development phase of a process plant and can be very useful in site selection.

PHA is a precursor to further hazard analyses. It is included in this description of the hazard evaluation procedures to provide a cost effective, early-in-plant-life method for hazard identification. Indeed, the PHA is really intended for use only in the preliminary phase of plant development for cases where past experience provides little or no insight into any potential safety problems, for example, a new plant with a new process.

The PHA focuses on the hazardous materials and major plant elements since few details on the plant design are available, and there is likely not to be any information available on procedures. The PHA is sometimes considered to be a review of where energy can be released in an uncontrolled manner. The PHA consists of formulating a list of the hazards related to:

* Raw materials, intermediate and final products, and their reactivity
* Plant equipment
* Interface among system components
* Operating environment
* Operations (test, maintenance, etc.)

* Facilities

* Safety equipment.

The results, which are qualitative, include recommendations to reduce or eliminate hazards in the subsequent design plant.

3.2 Process/System Checklists.

Checklists are frequently used to indicate compliance with standard procedures. A checklist is easy to use and can be applied to each stage of a project or plant development. A checklist is a convenient means of communicating the minimal acceptable level of hazard evaluation that is required for any job, regardless of scope. It is particularly useful for an inexperienced engineer to work through the various requirements in the checklist to reach a satisfactory conclusion. It also provide a common basis for management review of the individual engineer's work.

A checklist is intended to provide direction for standard evaluation of chemical or petrochemical plant hazards. It can be as detailed as necessary to satisfy the specific situation, but it should be applied conscientiously in order to identify problems that require further attention and to ensure that standard procedures are being followed. Checklists are limited to the experience base of the checklist author(s). They should be

audited and updated regularly.

Many organisations use standard checklists for controlling the development of a project from initial design through plant shutdown. The checklist is frequently a form for approval by various staff and management functions before a project can move from one stage to the next. In this way, it serves both as a means of communication and as a form of control.

3.3 Safety Review.

A Safety Review can vary from an informal routine function that is principally visual(walk-through on-site inspection), with emphasis on housekeeping, to a formal week-long examination by a team with appropriate backgrounds and responsibilities. The emphasis in this section is on the latter and it is sometimes referred to as "Safety Review". Such a program is intended to identify plant conditions or operating procedures that could lead to an accident and significant losses in life or property.

While this technique is most commonly applied to operating process plants, it is also applicable to pilot plants, laboratories, storage facilities, and support facilities. The comprehensive Safety Review is intended to complement other safety efforts and routine visual inspections. The Safety Review should be treated as a cooperative effort to improve the overall safety and

performance of the plant rather than as a feared interference with normal operations. Cooperation is essential. People are likely to become defensive unless considerable effort is made to present the review as a benefit to each participant.

The review includes interviews with many people in the plant: operators, maintenance staff, engineers, management, safety staff, and others, depending upon the plant organisation. Having the support and involvement of all these groups provides a thorough examination from any perspective.

The review looks for major risk situations. General housekeeping and personnel attitude are not the objective, although they can be significant indicators of where to look for real problems or places where real improvements are needed. Various hazard evaluation techniques, such as checklists, "what if?" questions, and raw material evaluations, can be used during the review.

At the end of the Safety Review, recommendations are made for specific actions that are needed, with justification; recommended responsibilities; and completion dates. A follow-up evaluation or re-inspection should be planned to verify the acceptability of the corrective action.

4. COMPONENT ORIENTATED ANALYSIS.

Failure Mode and Effect Analysis (FMEA) and Hazard and Operability Studies (HAZOP) are the principal component-orientated analysis techniques. In each method, the process under review is studied in detail and question "What if?", is used to identify hazards and investigate the way in which hazardous events occur.

Although a top down approach can be used in FMEA, both methods are more generally used to study a process from the bottom up. This causes the analyst to carry out a disciplined and comprehensive study of a process.

The major disadvantage of these methods is the time taken to carry out the study as they require the analyst to have a detailed understanding of the process. Therefore, these methods are often taught to design engineers and a team approach adopted when carrying out the analysis. This helps reduce the time required to complete the study. The team consists of design personnel and a hazard analyst may chair the study group.

4.1 "What If?" Analysis.

The "What If?" procedure is not as structured as Hazard and Operability (HAZOP) study and Failure Modes and Effects Analysis (FMEA). Instead, it requires the user to adapt the basic concept to the specific application. Very little information has been published on the "What If?"

method or its application. However, it is frequently referred to within the industry.

The purpose of "What If?" analysis is to consider carfully the result of unexpected events that would produce an adverse consequence. The method involves examination of possible deviations from the design, construction, modification, or operating intent. It requires a basic understanding of what is intended and the ability to mentally combine or synthetise possible deviations from design intent that would cause on undesired result. This is a powerful procedure if the staff is experienced; otherwise, the results are likely to be incomplete.

The "What If?" concept uses questions which begin "What If...?". For example:

* "What If" the wrong material is delivered?
* "What If" Pump A stops running during startup?
* "What If" the operator opens valve B instead of A?

The questions are divided into specific areas of investigation (usually related to consequences of concern), such as electrical safety, fire protection, or personnel safety. Each area is addressed by a team of two or three experts. The questions are formulated based on previous experience and applied to existing drawings and charts; for an operating plant, the investigation may

include questions for the plant staff (there is no specific order to these questions, unless the application provides a logical form or model). The questions can address any variation related to the plant, not just component failure or process variation.

4.2 Hazard And Operability (HAZOP) Studies.

The HAZOP study was developed to identify hazards in a process plant and to identify operability problems which, though not hazardous, could compromise the plant's ability to achieve design productivity. Thus, a HAZOP goes beyond hazard identification. Although originally developed to anticipate hazards and operability problems for new/or novel technology where past experience is limited, it has been found to be very effective for use at any stage in a plant's life from final design onwards. In addition, one variation of the HAZOP has been developed specifically to address preliminary design.

The approach taken is to form a multidisciplinary team that works together to identify hazards and operability problems by searching for deviations from design intents. An experienced team leader systematically guides the team through the plant design using a fixed set of words, called "guide words" (see Table 4.2), or uses checklists or knowledge. These guide words are applied at specific points or "study nodes" in the plant design to identify potential deviations of the plant process parameters at

those nodes. The nodes are usually specified by the team leader before the meetings. For example, the guide word "no" combined with the process parameter "flow" results in the deviation "no flow". The team then agrees on possible causes of the deviations (for example, operator error shuts off pump) and the consequences (for example, product contamination). If the causes and consequences are realistic and significant, they are recorded for follow-up action, which takes place outside of the study. In some cases, the team identifies a deviation with a realistic cause but unknown consequences (for example, unknown reaction product) and recommends follow-on studies to determine the possible consequences.

Guide Word	Property Word
No	Flow
Less	Temperature
More	Pressure
Reverse	Level
As well as	Concentration
Part of	Heat
Other than	Cooling

Table 4.2

4.3 Failure Modes And Effects Analysis (FMEA).

Failure Modes and Effects Analysis (FMEA) is a tabulation of the system/plant equipment, their failure modes, each failure mode's effect on the system/plant, and

a ranking for each failure mode (see Appendix C.2). The failure mode is a description of how equipment fails (open, closed, on, off, leaks, etc.). The effect of the failure mode is the system response or accident resulting from equipment failure, FMEA identifies single failure modes that either directly result in or contribute significantly to an important accident. Human/operator errors are generally not examined in a FMEA; however, the effects of mis-operation are usually described by an equipment failure mode. FMEA is not efficient for identifying combinations of equipment failures that lead to accidents. The FMEA can be performed by two analysts or a multidisciplinary team of professionals.

4.4 Human Error Analysis.

As the operator is the main component in any plant, his error could have a substantial influence on the safety of a system/plant. Human Error Analysis is a systematic evaluation of the factors that influence the performance of human operators, maintenance staff, technicians, and other personnel in the plant. It involves the performance of one of several types of task analysis, which is a method for describing the physical and environmental characteristics of a task along with the skills, knowledge, and capabilities required of those who perform the task. A Human Error Analysis will identifiy error-likely situations that can cause or lead to an accident. A Human Error Analysis can also be used to trace

the cause of a given type of human error. This type of analysis can be performed in conjonction with a Human Factor Engineering Analysis, a Human Reliability Analysis, or any of several types of system analysis.

5. EVENT ORIENTATED METHODS.

In contrast to FMEA and HAZOP, which start at the most detailed levels of a system and work up, event orientated methods are refered to as "top down" techniques.

An event of interest, for example a fire, is specifed as the top event and the events that cause the top event are identified. Events that may occur simultaneously, and alternative causes, are related in the form of a logic tree, so called because the final diagram looks like a tree.

Tveit (26) presents the following diagram to differentiate between FTA, CCA and ETA. See figure 5 below.
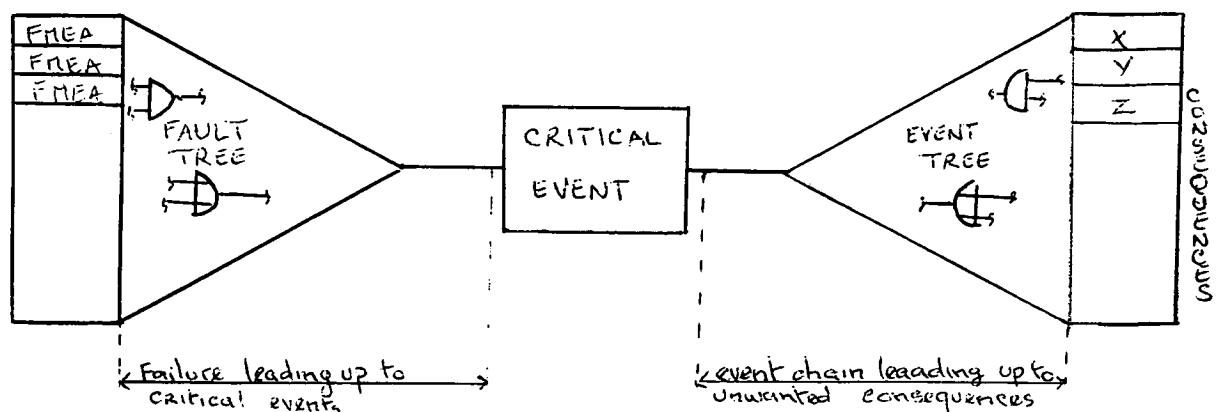
Fig. 5: Relation between FTA, ETA and CCA.

Fault Tree Analysis (FTA) is a deductive technique that focuses on one particular accident event and provides a method for determining causes of that accident event. The fault tree itself is a graphic model that displays the various combinations of equipment faults and failures that can result in the accident event. The solution of the fault tree is a list of the sets of equipment failures that are sufficient to cause the accident event of interest. FTA can include contributing human/operator errors as well as equipment failures.

The strength of FTA as a qualitative tool is its ability to break down an accident into basic equipment failures and human errors. This allows the safety analyst to focus preventive measures on these basic causes to reduce the probability of an accident. FTA is described in more details in Appendix C.3.

5.2 Event Tree Analysis.

Event tree analysis is a technique for evaluating potential accident outcomes resulting from a specific equipment system failure or human error known as an initiating event. Event tree analysis considers operator response or safety system response to the initiating event in determining the potential accident outcomes. The results of the event tree analysis are accident sequences; that is, a chronological set of failures or errors that

define an accident. These results describe the possible accident outcomes in terms of the sequence of events (successes or failures of safety functions) that follow an initiating event. Event tree analysis is well suited for systems that have safety systems or emergency procedures in place to respond to specific initiating events.

5.3 Cause-Consequence Analysis.

Cause-Consequence Analysis is a blend of fault tree and event tree analysis (discussed in the preceding sections) for evaluating potential accidents. A major strength of cause-consequence analysis is its use as a communication tool: the cause-consequence diagram displays the interrelationships between the accident outcomes (consequences) and their basic causes. The method can be used to quantify the expected frequency of occurrence of the consequences if the appropriate data are available. CCA is discussed in more details in Appendix C.4.

6. SELECTION OF HAZARD EVALUATION PROCEDURES.

Selecting a hazard evaluation for a particular purpose can be difficult. The different hazard evaluation procedures are different from each other in some ways and alike in others. There are many factors that characterise the need for the hazard evaluation that influence the selection of the procedure. This section addresses those

factors.

6.1 Factors Affecting Which Procedure is Selected.
6.1.1 Phase of Process/Plant Development.

Hazard evaluation should be a continuing process from process conception to plant shutdown and decommissioning. Each stage of process development has its own priorities for hazard evaluation, dependent mostly on achieving the best balance among:

a) Early identification to avoid costly redesign or construction modifications

b) Postponement of evaluation to await more detail

c) Avoidance of costly duplication of effort.

The best balance is usually achieved by using coarse screening evaluation procedures to identify major problems as early as possible and using more detailed and more costly procedures for more complete evaluations when the details on the final design and procedures are available. The complete and detailed evaluations made prior to startup can provide a useful baseline for evaluating the impact of any process/plant modifications that may be suggested during the operation phase.

6.1.2 Purpose of Hazard Evaluation.

The hazard evaluation process could be described as a number of steps, each of which has its own purpose. In

most cases each procedure will provide information for more than one step in the hazard evaluation process. Also, in many cases, the hazard evaluation step can be covered, to a greater or lesser extent, by more than one procedure.

"Worst case" conservative estimates of consequence levels can influence the choice of hazard evaluation procedure. A potential large release of flammable or toxic materials can justify a more complete and detailed search for events and combinations of events that could cause such a large release. Conversly, if there is high confidence of a low hazard level, a less exhaustive seach for causes may be in order.

6.1.4 Complexity of Process/Plant.

The degree of complexity can influence the choice of hazard evaluation procedure. A plant that incorporates several levels of protection through redundant controls, safety systems, mitigation systems, etc., needs an evaluation procedure that can identify, evaluate, and present the variety of accident event sequences that are possible. This is sometimes but not always a function of size. Simpler and smaller systems can be evaluated with simpler hazard evaluation procedures.

6.1.5 Familiarity With Procedures.

A very well done, simple procedure will provide better

results for decision making than a poorly done, more sophisticated procedure. Familiarity of staff with certain procedures is an argument for using them, provided that the limitations of the procedures are completely understood.

6.1.6 Information and Data Requirements.

Some of the procedures described in this thesis require more input data and information than others. If this information is not available, the results will not justify the use of those procedures. This is not as much as of a problem when the procedures are used to provide qualitative results as when quantitative results are required.

6.1.7 Time and Cost Requirements.

Time for analysis and cost of the evaluations should not be an absolute factor in the choice of hazard evaluation procedures. However, it is a factor which should be compared to the cost of hazard reduction opportunities which might obviate or reduce the cost of the analysis. Also, there may be other choices, such as not modifying a plant because of the cost of evaluating the modifications, or not continuing to operate a marginal plant.

6.2 Selection Of Hazard Evaluation Methods For The Study Of Near-miss Events.

For the purpose of this study, I have selected the four following methods:

a)Mond Fire and Explosion Index

b)Failure Mode and Effect Analysis

c)Fault Tree Analysis, and

d)Cause Consequence Analysis.

In the investigation of near-miss events Point Schemes have no direct impact. They are only used to spot the most dangerous areas of the plant or the unit under investigation so that more attention will be devoted to any incident occurring within the boundaries of this particular plant or unit. The Mond Index was chosen in preference the other methods because it is the more developed method.

The choice of the FMEA was based on the fact that this method can be used to help discriminate between minor problems and those which should be investigated in a more detailed manner.

Of all the event orientated methods, FTA has consistently been the most widely adopted technique. It quantifies the frequency of occurrence of the top event.

Finally CCA was chosen to study the consequences of top events already defined by FTA.

One of the objectives of this study was also to provide the Algerian industry with a method of investigation, which combines several methods, to study in a more detailed way the near-miss events that occur during the operation of chemical and petrochemical plants.

7. REFERENCES.

Cassidy, K., "The National and International Framework of Legislation for Major Industrial Accident Hazards" I. Chem. E. Symp. Series No. 110, pp. 401-413, May 1988.

Departement Of Defence, Military Standard System Safety Program Requirements, MIL-STD-882B, Washington, D.C., 1984.

King, C.F. & Rodd, D.F. "Design and maintenance of failure tolerant process" A.I. Chem. E. Journal Vol.18, p.257, 1983.

Kletz, T. A., "HAZOP & HAZAN: Notes on the Identification and Assessment of Hazards", Loss Prevention, The Inst. of Chem. Eng., ISBN 0-85295-165-5, Rugby, U.K., 1983.

Knowlton, R.E., "An Introduction to Guide Word Hazard and Operability Studies", CSChE Conference, 1982.

Knowlton, R.E., "An Introduction to Creative Checklist Hazard and Operability Studies", CSChE Conference, 1982.

Lees, F.P., "Loss Prevention in Process Industries.", P. 194, Butterworth & Co., 2nd Edition, 1983.

Lees, F.P., "The Hazard Warning Structure of Major Hazards.", Trans. I. Chem. E., Vol. 60, P. 211-221, 1982.

Lewis, D.J. "Hazard Control and Major Hazards (Fire, Explosion, Toxic Release)", The Institution of Chemical Engineers, Loughborough University of Technology, 23-27 Jannuary 1989.

Lihou, D., "Fault Trees From Operability Studies.", University Of Aston, Sep. 1980.

Martin-Solis, G.A., et al, "Fault Tree Synthesis for Design and Real Time Applications", Trans. IChem. E., Vol. 60, P. 14-25, 1982.

National aeronoutics and space administration, "Instructions for Preparation of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL).", NSTS 22206, October, 1986.

Neilsen, D.S., Platz, O., and Runge, B., "A Cause-Consequence Chart for a Redundant Protection System", IEEE Transactions on Reliability, 1984.

PRA Procedure Guide, "A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, Vol.1 and 2, U.S. Nuclear Regulatory Commission, Washington D.C, 1983.

"Procedure for Performing a Failure Mode, Effects and Criticality Analysis.", Dept. of Defence USA, MiL-STD-1629A, Nov. 1980.

Sax, N.I., "Dangerous Properties of Industrial Materials", van Norstrand Reinhold, New York, 1984.

Solomon C.H., The Exxon Chemicals Methods for Identifying Potential Process Hazards. I.Chem.E. Loss Prevention Bulletin No. 52, Aug. 1983.

Swain, A.D. and Guttman, H.E., "Handbook on Human Reliability Analysis with Emphasis on Nuclear Plant Applications", NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, D.C., 1983.

"Technical Manual for the Mond Fire and Explosion Index" ICI Mond Division, 1985.

Thomson, J.R. "Engineering Safety Assessment - An introduction", Longman Scientific and Technical, UK, 1987.

Tveit, O.S. et al, "risk Analysis of a Typical North Sea

Production Platform.", Offshore Technology Conference 1980, Paper No. 3905.

Whitehouse, H.B., "IFAL - A New Risk Analysis Tool" The Institution of Chemical Engineers, EFCE Publication Series No. 42, pp.309-322, (UMIST) Manchester, 22-24 April 1985.

Wickens, C.D., "Engineering Psychology and Human Performance", Charles E. Merrill Publishing Company, Columbus, Ohio, 1984.

CHAPTER IV.

MOND INDEX APPLICATION

1. INTRODUCTION.

This chapter describes the results of the application of the Mond Fire and Explosion Index to one of the three parallel trains or process lines of the HASSI R´MEL gas processing plant (MPP4).

The calculation of the Mond index was carried out according to the procedure presented in the review of the Mond index (Appendix C.1).

2. CALCULATION PROCEDURE.

To illustrate the procedure, this section will present the calculations applied to one of the three units which constitute a train.

Throughout this section reference should be made to sheets contained in section 5 at the end of this chapter. These calculation sheets show the value assigned to each factor, the values of the indices that were calculated and also the offsetting index values.

2.1 Division Of The Train Into Units.

Considering the operating pressure, the train or process line will be divided in two different units. A high pressure separation unit and a distillation unit. The latter could further be divided into two different parts. The reboilers or furnaces will be investigated as a unit apart since they are distant from the remaining equipment which constitute the distillation unit. Finally to show the importance that the area has on the calculation of the fire load, one of the vessels constituting the high pressure separation unit was investigated as a unit apart (see section 5 of this chapter).

The high pressure separation unit has been chosen for the remaining calculations. A paragraph will be devoted to the specific aspects encountered in the evaluation of the two other units.

2.2 Selection Of The Dominant Material (Section 4).

Methane being the main constituent in the raw gas (84% by wt), was selected as the key material in the high pressure separation unit.

2.3 Material Factor (Section 5).

The material factor B is calculated in terms of the heat of combustion in air at 25´C (excluding the heat of condensation of the water vapour. The technical manual (1)

gives the equation:

$$B = DHc * 1.8 / M$$

Where: DHc is the net heat of combustion in air at 25´C
in kcal/mol.

M is the molecular weight of the key material in
gm/mol.

For methane DHc = 212.79 kcal/gm mole (2).

In order to compensate for the assumption that the
processed gas is only methane, the average gas molecular
weight was used. M = 19 gm/mol.

$$B = 212.79 * 1.8 / 19 = 20.15$$

2.4 Special Material Hazards (Section 6).

In subsection 3, Mixing and Dispertion Characteristics,
the technical manual recommends that a factor of -20 be
used when the key material is methane.

The values used to account for Ignition Sensitivity
(subsection 6) are listed in Table 1 of the technical
manual. A factor of -5 is given for methane and a factor
of 0 for propane. The latter factor was used because the
presence of propane will make the gas more sensitive.

A factor of 20 is used in subsection 10, Other, to take account for the hazards introduced by the presence of liquid hydrocabons in the process stream.

The Special Material Hazards M, has the total value of 0.

2.5 General Process Hazards (Section 7).

The technical manual specifies that for process operations which only involves handling and physical changes and are carried out in closed systems with permanently installed pipework such as vessels, heat exchangers and columns, should be allocated a factor of 10. The value of P, which represents the General Process Hazards has the value of 10.

2.6 Special Process Hazards (Section 8).

The total value of 376 for S is made up of several factors.

Given an operating pressure of 140 bars (2058 psi) a factor of 96, read off from the graph Figure 4 in the technical manual was assigned to subsection 2, High Pressure.

Under the heading Corrosion and Erosion Hazards, subsection 5, the manual recommends a factor of 100 for an

internal corrosion rate of about 1 mm/year with erosion effects. The corrosion is mainly due to the presence of mercury (50 to 80 micro gm/Sm3) in the raw gas and the erosion to the velocity of the gas.

In subsection 6, Joints and Packing Leakage, a factor of 20 is used to take account of the leaks of minor nature occuring into pumps and, gland seals especially when they are permuted.

This unit operating rotating machines (turbo-expanders), there is a chance that vibrations will induces problems, like a joint failure, and result in a gas release into the unit. Subsection 7, Vibration and Load Cycling, is assigned a value of 20 to take account of this hazard.

If a release from the equipment of a small quantity of gas at high pressure occurs it will probably result in the formation of a flammable concentration in a large part of the surrounding atmosphere. A factor of 40 is assigned to subsection 10, Greater Than Average Explosion Hazard.

When gas escapes at high velocity from the containment system the build up of a static electrical charge often results. The discharge may release sufficiant energy to ignite a flammable mixture of the escaping gas. This hazard is enhanced by the presence of liquid in the containment system and further enhanced if the equipment is itself lined with insulating materials. A factor of 100

was adopted in subsection 14, where electrostatic hazards are taken into consideration.

2.7 Quantity Hazard (Section 9).

The volume of material present at any time in the unit is assumed to be 315 m3 and the average density of the gas is approximately 122 kg/m3. The factor Q which represents the quantity hazard was read off Figure 6 in the technical manual, and has a value of 65.

2.8 Layout Hazards (Section 10).

The highest point above the ground in this unit is situated at a height of 18 meters. The normal working area is 530 m2.

The most important feature for open process structures is the height at which significant quantities of flammable materials are contained in the unit. A factor of 50, taken from the table listed in subsection 3, Structure Design, was used.

The collapse of a unit due to explosion or weakness of the structure by fire may involve adjacent units this aspect is considered under the heading Domino Effects in subsection 4. For a unit height of less than 20 meters a factor of 0 is given.

Liquid hydrocarbons being processed along with gas, the drainage of the working area is of importance. In the case of containment rupture, pool formation has to be avoided. Because the grids intersect with the normal working area a factor of 50 was used in subsection 6, Surface Drainage.

The total value of L, Layout hazards, is 100.

2.9 Acute Health Hazards (Section11).

For a maximum liquid recovery the raw gas, entering the process line at a temperature of 60´C, is cooled down to -40´C by heat exchange and expansion. The effects that would have the material on the skin by contact, are evaluated in subsection 1, Skin Effects. For example, scalding (or freezing) would be the result of skin contact with the low temperature gas. A factor of 50 was assigned.

Subsection 2, considers the Inhalation Effects. The mixture of gas processed, does not contain any toxic component (e.g., hydrogen sulphide), and is a simple asphyxiant. No irreversible effects due to inhalation or contact with the gas have to be feared. A value of 10 was used.

The Acute Health Hazards T, Has a total value of 60.

2.10 Computation Of Indices (Section 12).

The computation of the various indices is shown on page 4 of the sheets at the end of this chapter. Tables in the technical manual give the different categories in which each index numerical value is classified.

The equivalent Dow Index has a value of 155.38. The availability of the other indices convertion of the Dow Index value into descriptive ratings or to use it to compare units, unnecessary. It is, however, a basic element of the Overall Risk Rating.

The Overall Risk Rating falls into the "Extreme" category with a value of 18,307. This is mainly due to the high values of the Aerial Explosion index and the Internal Explosion Index which respectively have values of 9,869 and 4.86. The corresponding categories are "Extreme" for the first and "high" for the latter. The Fire Load Index falls under the category "Light" with a value of 1.46 this is mainly due to the large area of the unit as it is demonstrated by the investigation of one of the vessels composing the unit.

2.11 Process Development By Hazard Factor Review (Section 13).

A review of the process was not carried out due to the lack of more precise information, the only literature being the operating manual for most of the factors. The values given to the factors in the previous stages are the

more optimistic available.

The values of the indices are the same as those in section 10.

2.12 Offsetting Index Values For Safety And Preventive Measures (Section 13).

The measures which attempt to prevent the occurence of a hazardous incident, and the measures which reduce the consequences of hazardous incident are taken into account in the following six subsections:

a)Containment Hazards.

The design and quality control of the pressure vessel warrants a factor of 0.8 to be applied under the factor, "Pressure Vessels". A factor of 0.75 is used to account for the design stress in the transfer pipelines. Under "Joints and Packing" are entered three factors (0.9, 0.9 and 0.95) to take account of the welded pipework, the type of flanges used, and the seal oil system protecting the turbo-expanders. All relief or emergency venting releases being piped to a flare stack and the liquids dumped by pipeworks to a burn pit, a factor of 0.85 is assigned to "Emergency Venting or Dumping".

b)Process Control.

The whole plant being fitted with a wide range of alarms, a factor of 0.9 is given to "Alarm System". A value of 0.8 is assigned to "Emergency Power Supplies". If the two high-tension lines, which can separately supply the plant with energy, fail, a gas turbine is automatically switched on to provide emergency power. A battery room provide power for the essential systems, such as air compressors, light and main control panel, for 24 hours should the turbine fail.

Under the heading "Inert Gas Systems" a value of 0.9 is given, inert gas being supplied to all parts of the process. It is used to inert the vessels before a startup.

During the design and the construction stages of the plant, number of hazards studies were carried out. The value assigned to "Hazard Studies Activities" is 0.95.

A very high performance shutdown system has been designed for this plant. Strict specifications were applied and the relay logic carefully checked. Many features such as very low or very high, liquid levels or gas pressures, low flow rates and the like initiate the plant shutdown. Under the heading "Safety Shutdown Systems", a factor of 0.7 is applied.

A computer in the main control room (MCR) is used to monitor the process and to close the wells by remote control which consequentely initiate the shutdown. The

computer does not control the process, but the shutdown could be initiated from the MCR, therefore, a factor of 0.85 is assigned to "Computer Control". The "Operating Instructions" for the plant are clear and comprehensive. Start-up, normal operation and routine and emergency shutdown are adequately covered. A value of 0.8 is given to this factor.

The plant supervision is very good over all the HASSI R´MEL complex. Strict security measure to keep out any unauthorised person, efficient de-matching and no-smoking system and good control of vehicle movement in hazardous areas are applied. All process operators are in constant contact with the MCR via two-way hand held radios. 0.81 is given to "Plant Supervision".

c)Safety Attitude.

The HASSI R´MEL management is very concerned with the employees and the equipment safety . No compromise is allowed between production factors and safety. Requirements for pressure equipment inspection are complied with, and dangerous events, including near misses are investigated, reported and the necessary actions taken. "Management Involvement" scores 0.81.

On the first day of their visit, all employees must attend the safety briefing given by the safety officer. This briefing covers various aspects of the complex safety

practices, and the plan for evacuation in the event of a major disaster. A value of 0.9 is given to "Safety Training".

A strict "permit to work" system is observed for maintenance and modification work, and no work could be done without the presence of a safety officer. The housekeeping on the plant is of high standard and preventive maintenance is carried out on a scheduled basis. Under "Maintenance and Safety Procedures" three factors (0.90, 0.97 and 0.90) are given.

d)Fire Protection.

Fixed Nozzle systems help to protect the equipment structures if a fire occurs and this warrants a factor of 0.9 being assumed under "Structural Fire Protection". Water curtains can be generated to isolate the unit from its neighbouring units. Under the heading "Fire Walls, Barriers and Similar Devices" 0.90 is assigned.

Since all instrument cables and electrical cables needed for unit control functions are fire resistant a factor of 0.85 is applied, and a factor of 0.98 takes account of the possibility to use the fixed nozzle system to provide external fire protection insulation to the equipment under the collective heading "Equipment Fire Protection".

e)Material Isolation.

All vessels and major pipelines within the plant are fitted with remotely operated isolation valves and an emergency pressure blow down system is provided. A factor of 0.72 is assigned to "Valve Systems".

f)Fire Fighting.

The break glass call points system which is linked directly to the works fire brigade, will activate the shutdown system. The works fire brigade is also connected to the communication system of the plant so that the fire brigade will have an early description of any hazardous event and will save precious time. "Fire Alarms"is given 0.90.

Throughout the plant, hand held, large and small trolley mounted fire extinguishers containing various fire fighting substances, are provided. Their positions are well marked so that the operatives can obtain an extinguisher quickly. Factors 0.90 and 0.85, are assigned to "Hand Fire Extinguishers".

A pressure decrease in the firewater ring will automatically start-up two electrical motor centrifugal pumps. Two diesel motor centrifugal pumps are kept on stand-by in the case of an electrical power supply system failure. The high pressure and flow rate obtained from the firewater ring score 0.75 under "Water Supply". A value of

0.95 has been assigned under "Water Spray or Monitor Systems" to take account for the hand setting of direction of the monitor guns.

Installed foam systems are provided throughout the unit with sufficient quantities of foam making compounds to start fire fighting and give the enough time to the fire brigade to bring the supplies. A value of 0.81 was assigned under "Foam and Inerting Installations".

Under the heading "Fire Brigade Attendance" a factor of 0.75 has been assigned to take account the number of works appliances with adequately trained crews that are ready for any eventuality at any time. The regular training of the operatives in the use of hand extinguishers, fixed equipment, and their involvement alongside the works fire brigade in fire fighting exercice score 0.80 under "Site Co-operation in Fire Fighting".

2.13 Final Offset Indices Calculations.

The offset Overall Risk Rating becomes 113 and is categorized "Moderate". The Fire Load and the Internal Explosion indices fall into "Light" category with respective values of 5.62E-2 and 0.25, whereas the Aerial Explosion index still of importance with a value of 379 and falls into "High" category.

3. SPECIFICITIES OF THE REMAINING UNITS.

The distillation unit and the furnaces constitute in fact one unit. Most of the factors that will be discussed in this section are common to the two units. The specific factors will be pointed out.

The key material chosen for the two units was propane. Its proportions in the process stream and its properties make of it the most dangerous material present in these units. B the material factor has a value of 21.50.

Under "Mixing and Dispersion Characteristic" the propane is given a factor of 0. Special Material Hazard, M, has a value of 20.

Special Process Hazard has a total value of 360. The reduction in pressure decreases the value of p under "high pressure" by 26, but the high temperature scores 20 under "high temperature flammable material".

The quantity of material in each unit has been determined separately. The distillation unit contains at any time approximately 160 tonnes and the furnaces 10 tonnes. Their quantity factors will respectively be 88 and 40.

The height and the working area are also specific for each unit and are equal to 50m and 665m2 for the distillation unit and 40m and 256m2 for the furnaces unit.

The heights determine the "Domino Effect" factor. The distillation unit has a factor of 150 and the furnaces unit a factor of 100. Under Layout Hazards the first one score 200 and the second 150.

Concerning the investigation of the vessel (D101) few factors are different from the ones previously determined in the investigation of the high pressure separation unit. These concern the Quantity Hazards K and Q with values of respectiveluy equal to 3.45 and 22, the working area N with a value of 18 m2 and the height with a value of 14 m.

The offsetting index values for safety and preventive measures are assumed to be the same for all the units.

4. COMMENTS.

The comparison the results obtained show that the division of the plant into units is the most important part of the investigation and has a direct impact on the final results. The larger the area the lower the fire load will be. In the case of the high pressure unit the fire load is equal to 1.46 whereas for the D101 the fire load is equal to 3.86. The difference is mainly due to the large area under the pipe tracks that has to be taken into account when calculating the indices for the whole unit whereas when calculating the indices for the D101 only the area under the vessel is considered. When interpretating

the results one must pay considerable attention to this fact to avoid any error of judgement.

5. REFERENCES.

1) "Technical Manual For The Mond Fire And Explosion Index" ICI Mond Division, 1985.

MOND INDEX 1985
****

LOCATION HASSI R'MEL

PLANT MODULE PROCESSING PLANT 4 (MPP4)

UNIT HIGH PRESSURE SEPARATION

MATERIALS NATURAL GAS

ADDITIONAL INFORMATION

COMMENT
NUMBER

PRESSURE = psig 2058   TEMPERATURE t= DEG.C   60
MATERIAL FACTOR (Section 5)

KEY MATERIAL OR MIXTURE : METHANE
FACTOR DETERMINED BY   :
MATERIAL FACTOR   : B= 20.15
                             RANGE   FACTOR
                                                 INITIAL   REVIEW

SPECIAL MATERIAL HAZARDS (Section 6)

	RANGE	INITIAL	REVIEW
1.OXIDISING MATERIALS	0 TO 20		
2.GIVES COMBUSTIBLE GAS WITH WATER	0 TO 30		
3.MIXING & DISPERSION CHARACTERISTICS	-60 TO 100	m - 20	
4.SUBJECT TO SPONTANEOUS HEATING	30 TO 250		
5.MAY RAPIDLY SPONTANEOUSLY POLYMERISE	25 TO 75		
6.IGNITION SENSITIVITY	-75 TO 150	O	
7.SUBJECT TO EXPLOSIVE DECOMPOSITION	75 TO 125		
8.SUBJECT TO GASEOUS DETONATION	0 TO 150		
9.CONDENSED PHASE PROPERTIES	200 TO 1500		
10.OTHER	0 TO 150	20	
SPECIAL MATERIAL HAZARDS TOTAL		M O	

GENERAL PROCESS HAZARDS (Section 7)

	RANGE	INITIAL	REVIEW
1.HANDLING & PHYSICAL CHANGES ONLY	10 TO 50	10	
2.REACTION CHARACTERISTICS	25 TO 50		
3.BATCH REACTIONS	10 TO 60		
4.MULTIPLICITY OF REACTIONS	25 TO 75		
5.MATERIAL TRANSFER	0 TO 150		
6.TRANSPORTABLE CONTAINERS	10 TO 100		
GENERAL PROCESS HAZARDS TOTAL		P 10	

MOND INDEX 1985
****

SPECIAL PROCESS HAZARDS (Section 8)

1.LOW PRESSURE(BELOW 15 PSIA)	50 TO 150			
2.HIGH PRESSURE	0 TO 160	P	96	
3.LOW TEMP.:1.CARBON STEEL +10C TO -25C	0 TO 30			
2.CARBON STEEL BELOW -25C	30 TO 100			
3.OTHER MATERIALS	0 TO 100			
4.HIGH TEMP.1.FLAMMABLE MATERIALS	0 TO 35			
2.MATERIAL STRENGTH	0 TO 25			
5.CORROSION & EROSION	0 TO 400		100	
6.JOINT & PACKING LEAKAGES	0 TO 60		20	
7.VIBRATION,LOAD CYCLING,ETC.	0 TO 100		20	
8.PROCESSES/REACTIONS DIFFICULT TO CONTROL	20 TO 300			
9.OPERATION IN OR NEAR FLAMMABLE RANGE	25 TO 450			
10.GREATER THAN AVERAGE EXPLOSION HAZARD	40 TO 100		40	
11.DUST OR MIST EXPLOSION HAZARD	30 TO 70			
12.HIGH STRENGTH OXIDANTS	0 TO 400			
13.PROCESS IGNITION SENSITIVITY	0 TO 100			
14.ELECTROSTATIC HAZARDS	10 TO 200		100	

SPECIAL PROCESS HAZARDS TOTAL   S   376

QUANTITY HAZARDS (Section 9)

MATERIAL TOTAL TONNES   K   38.5
QUANTITY FACTOR   Q   65

LAYOUT HAZARDS (Section 10)

HEIGHT IN METRES   H   18
WORKING AREA IN SQUARE METRES   N   530

1.STRUCTURE DESIGN	0 TO 200	50	
2.DOMINO EFFECT	0 TO 250	0	
3.BELOW GROUND	50 TO 150		
4.SURFACE DRAINAGE	0 TO 100	50	
5.OTHER	50 TO 250		

LAYOUT HAZARDS TOTAL   L   100

ACUTE HEALTH HAZARDS (Section 11)

1.SKIN EFFECTS	0 TO 50	50	
2.INHALATION EFFECTS	0 TO 50	10	

ACUTE HEALTH HAZARDS TOTAL   T   60

MOND INDEX 1985
****

PAGE NO. 3
FILE NO.

OFFSETTING INDEX VALUES FOR SAFETY & PREVENTATIVE MEASURES
****

A.CONTAINMENT HAZARDS (Section 16.1)
1-PRESSURE VESSELS   0.80
2-NON-PRESSURE VERTICAL STORAGE TANKS   0.75
3-TRANSFER PIPELINES A)DESIGN STRESSES
                     B)JOINTS & PACKINGS   0.90, 0.99 0.95
4-ADDITIONAL CONTAINMENT & BUNDS
5-LEAKAGE DETECTION & RESPONSE
6-EMERGENCY VENTING OR DUMPING   0.85

                    PRODUCT TOTAL OF CONTAINMENT FACTORS   K1= 0.39

B.PROCESS CONTROL (Section 16.2)
1-ALARM SYSTEMS   0.90
2-EMERGENCY POWER SUPPLIES   0.80
3-PROCESS COOLING SYSTEMS
4-INERT GAS SYSTEMS   0.90
5-HAZARD STUDIES ACTIVITIES   0.95
6-SAFETY SHUTDOWN SYSTEMS   0.70
7-COMPUTER CONTROL   0.85
8-EXPLOSION/INCORRECT REACTOR PROTECTION
9-OPERATING INSTRUCTIONS   0.80
10-PLANT SUPERVISION   0.81

                    PRODUCT TOTAL OF PROCESS CONTROL FACTORS   K2= 0.24

C.SAFETY ATTITUDE (Section 16.3)
1-MANAGMENT INVOLVEMENT   0.81
2-SAFETY TRAINING   0.90
3-MAINTENANCE & SAFETY PROCEDURES   0.9, 0.97, 0.9

                    PRODUCT TOTAL OF SAFETY ATTITUDE FACTORS   K3= 0.57

D.FIRE PROTECTION (Section 17.1)
1-STRUCTURAL FIRE PROTECTION   0.9
2-FIRE WALLS,BARRIERS   0.9
3-EQUIPMENT FIRE PROTECTION   0.85, 0.9

                    PRODUCT TOTAL OF FIRE PROTECTION FACTORS   K4= 0.67

E.MATERIAL ISOLATION (Section 17.2)
1-VALVE SYSTEMS   0.72
2-VENTILATION

                    PRODUCT TOTAL OF MATERIAL ISOLATION FACTORS   K5= 0.72

F.FIRE FIGHTING (Section 17.3)
1-FIRE ALARMS   0.9
2-HAND FIRE EXTINGUISHERS   0.9, 0.85
3-WATER SUPPLY   0.75
4-WATER SPRAY OR MONITOR SYSTEMS   0.95
5-FOAM & INERTING INSTALLATIONS   0.81
6-FIRE BRIGADE ATTENDANCE   0.75
7-SITE CO-OPERATION IN FIRE FIGHTING   0.80
8-SMOKE VENTILATORS

                    PRODUCT TOTAL OF FIRE FIGHTING FACTORS   K6= 0.24

MOND INDEX 1985
×××××××××××××××××

EQUATIONS
=========

__EQUIVALENT DOW INDEX (for initial assessment and review)__

$$D = B(1+M/100)(1+P/100)(1+(S+Q+L+T)/100))$$

__FIRE INDEX__

INITIAL ASSESSMENT AND REVIEW   F= BK/N

OFFSET   F*K1*K3*K5*K6

__INTERNAL EXPLOSION INDEX__

INITIAL ASSESSMENT AND REVIEW   E=1+(M+P+S)/100

OFFSET   E*K2*K3

__AERIAL EXPLOSION INDEX__

INITIAL ASSESSMENT AND REVIEW   A=B(1+m/100)(1+p)(QHE/1000)(t+273)/300

OFFSET   A*K1*K2*K3*K5

__OVERALL RISK RATING__

INITIAL ASSESSMENT AND REVIEW   R=D(1+(.2E*SQUARE ROOT(AF)))

OFFSET   R*K1*K2*K3*K4*K5*K6

INDICES COMPUTATION
====================

INDEX	__INITIAL__		__REVIEW__		__OFFSET__	
	VALUE	CATEGORY	VALUE	CATEGORY	VALUE	CATEGORY
D	155.38	—			155.38	—
F	1.46	LIGHT			5.62 E-2	LIGHT
E	4.86	HIGH			0.259	LIGHT
A	9,869	EXTREME			379	HIGH
R	18,307	EXTREME			113	MODERATE

87

MOND INDEX 1985
****

LOCATION HASSI R'MEL

PLANT MODULE PROCESSING PLANT 4 (MPP4)

UNIT LOW PRESSURE SEPARATION

MATERIALS NATURAL GAS

ADDITIONAL INFORMATION

COMMENT
NUMBER

PRESSURE = psig 420   TEMPERATURE t= DEG.C 263
MATERIAL FACTOR (Section 5)

KEY MATERIAL OR MIXTURE : PROPANE
FACTOR DETERMINED BY   :
MATERIAL FACTOR   : B= 21.5
                          RANGE   FACTOR
                                           INITIAL   REVIEW

SPECIAL MATERIAL HAZARDS (Section 6)

	RANGE		INITIAL	REVIEW
1.OXIDISING MATERIALS	0 TO	20		
2.GIVES COMBUSTIBLE GAS WITH WATER	0 TO	30		
3.MIXING & DISPERSION CHARACTERISTICS	-60 TO	100	m	0
4.SUBJECT TO SPONTANEOUS HEATING	30 TO	250		
5.MAY RAPIDLY SPONTANEOUSLY POLYMERISE	25 TO	75		
6.IGNITION SENSITIVITY	-75 TO	150		
7.SUBJECT TO EXPLOSIVE DECOMPOSITION	75 TO	125		
8.SUBJECT TO GASEOUS DETONATION	0 TO	150		
9.CONDENSED PHASE PROPERTIES	200 TO	1500		
10.OTHER	0 TO	150		20
SPECIAL MATERIAL HAZARDS TOTAL			M	20

GENERAL PROCESS HAZARDS (Section 7)

	RANGE		INITIAL	REVIEW
1.HANDLING & PHYSICAL CHANGES ONLY	10 TO	50		10
2.REACTION CHARACTERISTICS	25 TO	50		
3.BATCH REACTIONS	10 TO	60		
4.MULTIPLICITY OF REACTIONS	25 TO	75		
5.MATERIAL TRANSFER	0 TO	150		
6.TRANSPORTABLE CONTAINERS	10 TO	100		
GENERAL PROCESS HAZARDS TOTAL			F	10

MOND INDEX 1985
****

SPECIAL PROCESS HAZARDS (Section 8)

1.LOW PRESSURE(BELOW 15 PSIA)	50 TO	150		
2.HIGH PRESSURE	0 TO	160	P	60
3.LOW TEMP.:1.CARBON STEEL +10C TO -25C	0 TO	30		
2.CARBON STEEL BELOW -25C	30 TO	100		
3.OTHER MATERIALS	0 TO	100		
4.HIGH TEMP.1.FLAMMABLE MATERIALS	0 TO	35		20
2.MATERIAL STRENGTH	0 TO	25		
5.CORROSION & EROSION	0 TO	400		100
6.JOINT & PACKING LEAKAGES	0 TO	60		20
7.VIBRATION,LOAD CYCLING,ETC.	0 TO	100		20
8.PROCESSES/REACTIONS DIFFICULT TO CONTROL	20 TO	300		
9.OPERATION IN OR NEAR FLAMMABLE RANGE	25 TO	450		
10.GREATER THAN AVERAGE EXPLOSION HAZARD	40 TO	100		40
11.DUST OR MIST EXPLOSION HAZARD	30 TO	70		
12.HIGH STRENGTH OXIDANTS	0 TO	400		
13.PROCESS IGNITION SENSITIVITY	0 TO	100		100
14.ELECTROSTATIC HAZARDS	10 TO	200		

    SPECIAL PROCESS HAZARDS TOTAL   S 360

QUANTITY HAZARDS (Section 9)

    MATERIAL TOTAL TONNES   K 160

    QUANTITY FACTOR   Q 88

LAYOUT HAZARDS (Section 10)

    HEIGHT IN METRES   H 50

    WORKING AREA IN SQUARE METRES   N 665

1.STRUCTURE DESIGN	0 TO	200		50
2.DOMINO EFFECT	0 TO	250		150
3.BELOW GROUND	50 TO	150		
4.SURFACE DRAINAGE	0 TO	100		
5.OTHER	50 TO	250		

    LAYOUT HAZARDS TOTAL   L 200

ACUTE HEALTH HAZARDS (Section 11)

1.SKIN EFFECTS	0 TO	50		50
2.INHALATION EFFECTS	0 TO	50		10

    ACUTE HEALTH HAZARDS TOTAL   T 60

MOND INDEX 1985
****

OFFSETTING INDEX VALUES FOR SAFETY & PREVENTATIVE MEASURES
****

A. CONTAINMENT HAZARDS (Section 16.1)
1-PRESSURE VESSELS
2-NON-PRESSURE VERTICAL STORAGE TANKS
3-TRANSFER PIPELINES A) DESIGN STRESSES
                      B) JOINTS & PACKINGS
4-ADDITIONAL CONTAINMENT & BUNDS
5-LEAKAGE DETECTION & RESPONSE
6-EMERGENCY VENTING OR DUMPING

PRODUCT TOTAL OF CONTAINMENT FACTORS $K_1 = 0.39$

B. PROCESS CONTROL (Section 16.2)
1-ALARM SYSTEMS
2-EMERGENCY POWER SUPPLIES
3-PROCESS COOLING SYSTEMS
4-INERT GAS SYSTEMS
5-HAZARD STUDIES ACTIVITIES
6-SAFETY SHUTDOWN SYSTEMS
7-COMPUTER CONTROL
8-EXPLOSION/INCORRECT REACTOR PROTECTION
9-OPERATING INSTRUCTIONS
10-PLANT SUPERVISION

PRODUCT TOTAL OF PROCESS CONTROL FACTORS $K_2 = 0.24$

C. SAFETY ATTITUDE (Section 16.3)
1-MANAGMENT INVOLVEMENT
2-SAFETY TRAINING
3-MAINTENANCE & SAFETY PROCEDURES

PRODUCT TOTAL OF SAFETY ATTITUDE FACTORS $K_3 = 0.57$

D. FIRE PROTECTION (Section 17.1)
1-STRUCTURAL FIRE PROTECTION
2-FIRE WALLS, BARRIERS
3-EQUIPMENT FIRE PROTECTION

PRODUCT TOTAL OF FIRE PROTECTION FACTORS $K_4 = 0.67$

E. MATERIAL ISOLATION (Section 17.2)
1-VALVE SYSTEMS
2-VENTILATION

PRODUCT TOTAL OF MATERIAL ISOLATION FACTORS $K_5 = 0.72$

F. FIRE FIGHTING (Section 17.3)
1-FIRE ALARMS
2-HAND FIRE EXTINGUISHERS
3-WATER SUPPLY
4-WATER SPRAY OR MONITOR SYSTEMS
5-FOAM & INERTING INSTALLATIONS
6-FIRE BRIGADE ATTENDANCE
7-SITE CO-OPERATION IN FIRE FIGHTING
8-SMOKE VENTILATORS

PRODUCT TOTAL OF FIRE FIGHTING FACTORS $K_6 = 0.24$

MOND INDEX 1985
****

EQUATIONS
=========

EQUIVALENT DOW INDEX (for initial assessment and review)

$$D = B(1+M/100)(1+P/100)(1+(S+Q+L+T)/100))$$

FIRE INDEX

INITIAL ASSESSMENT AND REVIEW   F= BK/N

OFFSET   F*K1*K3*K5*K6

INTERNAL EXPLOSION INDEX

INITIAL ASSESSMENT AND REVIEW   E=1+(M+P+S)/100

OFFSET   E*K2*K3

AERIAL EXPLOSION INDEX

INITIAL ASSESSMENT AND REVIEW   A=B(1+a/100)(1+p)(QHE/1000)(t+273)/300

OFFSET   A*K1*K2*K3*K5

OVERALL RISK RATING

INITIAL ASSESSMENT AND REVIEW   R=D(1+(.2E*SQUARE ROOT(AF)))

OFFSET   R*K1*K2*K3*K4*K5*K6

INDICES COMPUTATION
===================

INDEX	INITIAL		REVIEW		OFFSET	
	VALUE	CATEGORY	VALUE	CATEGORY	VALUE	CATEGORY
D	229				229	
F	5.17	MODERATE			0.199	LIGHT
E	4.9	HIGH			0.26	LIGHT
A	50,519	EXTREME			1,940	EXTREME
R	115,110	VERY EXTREME			711	HIGH (GROUP I)

MOND INDEX 1985
****

LOCATION   HASSI R'MEL

PLANT   MODULE PROCESSING PLANT 4 (MPP4)

UNIT   FURNACES

MATERIALS   CONDENSATS

ADDITIONAL INFORMATION

COMMENT
NUMBER

PRESSURE = psig 420   TEMPERATURE t= DEG.C 263
MATERIAL FACTOR (Section 5)

KEY MATERIAL OR MIXTURE : PROPANE
FACTOR DETERMINED BY   :
MATERIAL FACTOR   : B= 21.5

		RANGE	FACTOR	
			INITIAL	REVIEW

SPECIAL MATERIAL HAZARDS (Section 6)

	RANGE		FACTOR INITIAL
1.OXIDISING MATERIALS	0 TO	20	
2.GIVES COMBUSTIBLE GAS WITH WATER	0 TO	30	
3.MIXING & DISPERSION CHARACTERISTICS	-60 TO	100	m 0
4.SUBJECT TO SPONTANEOUS HEATING	30 TO	250	
5.MAY RAPIDLY SPONTANEOUSLY POLYMERISE	25 TO	75	
6.IGNITION SENSITIVITY	-75 TO	150	
7.SUBJECT TO EXPLOSIVE DECOMPOSITION	75 TO	125	
8.SUBJECT TO GASEOUS DETONATION	0 TO	150	
9.CONDENSED PHASE PROPERTIES	200 TO	1500	
10.OTHER	0 TO	150	20

SPECIAL MATERIAL HAZARDS TOTAL   M   20

GENERAL PROCESS HAZARDS (Section 7)

	RANGE		FACTOR
1.HANDLING & PHYSICAL CHANGES ONLY	10 TO	50	10
2.REACTION CHARACTERISTICS	25 TO	50	
3.BATCH REACTIONS	10 TO	60	
4.MULTIPLICITY OF REACTIONS	25 TO	75	
5.MATERIAL TRANSFER	0 TO	150	
6.TRANSPORTABLE CONTAINERS	10 TO	100	

GENERAL PROCESS HAZARDS TOTAL   P   10

MOND INDEX 1985
****

SPECIAL PROCESS HAZARDS (Section 8)

1.LOW PRESSURE(BELOW 15 PSIA)	50 TO 150		
2.HIGH PRESSURE	0 TO 160	P	60
3.LOW TEMP.:1.CARBON STEEL +10C TO -25C	0 TO 30		
2.CARBON STEEL BELOW -25C	30 TO 100		
3.OTHER MATERIALS	0 TO 100		
4.HIGH TEMP.1.FLAMMABLE MATERIALS	0 TO 35		20
2.MATERIAL STRENGTH	0 TO 25		
5.CORROSION & EROSION	0 TO 400		100
6.JOINT & PACKING LEAKAGES	0 TO 60		20
7.VIBRATION,LOAD CYCLING,ETC.	0 TO 100		20
8.PROCESSES/REACTIONS DIFFICULT TO CONTROL	20 TO 300		
9.OPERATION IN OR NEAR FLAMMABLE RANGE	25 TO 450		
10.GREATER THAN AVERAGE EXPLOSION HAZARD	40 TO 100		40
11.DUST OR MIST EXPLOSION HAZARD	30 TO 70		
12.HIGH STRENGTH OXIDANTS	0 TO 400		
13.PROCESS IGNITION SENSITIVITY	0 TO 100		100
14.ELECTROSTATIC HAZARDS	10 TO 200		

SPECIAL PROCESS HAZARDS TOTAL   S 360

QUANTITY HAZARDS (Section 9)

MATERIAL TOTAL TONNES   K 10
QUANTITY FACTOR   Q 40

LAYOUT HAZARDS (Section 10)

HEIGHT IN METRES   H 40
WORKING AREA IN SQUARE METRES   N 256

1.STRUCTURE DESIGN	0 TO 200	50
2.DOMINO EFFECT	0 TO 250	50
3.BELOW GROUND	50 TO 150	
4.SURFACE DRAINAGE	0 TO 100	50
5.OTHER	50 TO 250	

LAYOUT HAZARDS TOTAL   L 150

ACUTE HEALTH HAZARDS (Section 11)

1.SKIN EFFECTS	0 TO 50	50
2.INHALATION EFFECTS	0 TO 50	10

ACUTE HEALTH HAZARDS TOTAL   T 60

MOND INDEX 1985
****

OFFSETTING INDEX VALUES FOR SAFETY & PREVENTATIVE MEASURES
****

A.CONTAINMENT HAZARDS (Section 16.1)
1-PRESSURE VESSELS
2-NON-PRESSURE VERTICAL STORAGE TANKS
3-TRANSFER PIPELINES A)DESIGN STRESSES
                     B)JOINTS & PACKINGS
4-ADDITIONAL CONTAINMENT & BUNDS
5-LEAKAGE DETECTION & RESPONSE
6-EMERGENCY VENTING OR DUMPING

PRODUCT TOTAL OF CONTAINMENT FACTORS $K_1 = 0.39$

B.PROCESS CONTROL (Section 16.2)
1-ALARM SYSTEMS
2-EMERGENCY POWER SUPPLIES
3-PROCESS COOLING SYSTEMS
4-INERT GAS SYSTEMS
5-HAZARD STUDIES ACTIVITIES
6-SAFETY SHUTDOWN SYSTEMS
7-COMPUTER CONTROL
8-EXPLOSION/INCORRECT REACTOR PROTECTION
9-OPERATING INSTRUCTIONS
10-PLANT SUPERVISION

PRODUCT TOTAL OF PROCESS CONTROL FACTORS $K_2 = 0.24$

C.SAFETY ATTITUDE (Section 16.3)
1-MANAGMENT INVOLVEMENT
2-SAFETY TRAINING
3-MAINTENANCE & SAFETY PROCEDURES

PRODUCT TOTAL OF SAFETY ATTITUDE FACTORS $K_3 = 0.57$

D.FIRE PROTECTION (Section 17.1)
1-STRUCTURAL FIRE PROTECTION
2-FIRE WALLS,BARRIERS
3-EQUIPMENT FIRE PROTECTION

PRODUCT TOTAL OF FIRE PROTECTION FACTORS $K_4 = 0.67$

E.MATERIAL ISOLATION (Section 17.2)
1-VALVE SYSTEMS
2-VENTILATION

PRODUCT TOTAL OF MATERIAL ISOLATION FACTORS $K_5 = 0.72$

F.FIRE FIGHTING (Section 17.3)
1-FIRE ALARMS
2-HAND FIRE EXTINGUISHERS
3-WATER SUPPLY
4-WATER SPRAY OR MONITOR SYSTEMS
5-FOAM & INERTING INSTALLATIONS
6-FIRE BRIGADE ATTENDANCE
7-SITE CO-OPERATION IN FIRE FIGHTING
8-SMOKE VENTILATORS

PRODUCT TOTAL OF FIRE FIGHTING FACTORS $K_6 = 0.24$

MOND INDEX 1985
****

EQUATIONS
=========

<u>EQUIVALENT DOW INDEX (for initial assessment and review)</u>

$$D = B(1+M/100)(1+P/100)(1+(S+Q+L+T)/100))$$

<u>FIRE INDEX</u>

INITIAL ASSESSMENT AND REVIEW $F = BK/N$

OFFSET $F*K1*K3*K5*K6$

<u>INTERNAL EXPLOSION INDEX</u>

INITIAL ASSESSMENT AND REVIEW $E = 1+(M+P+S)/100$

OFFSET $E*K2*K3$

<u>AERIAL EXPLOSION INDEX</u>

INITIAL ASSESSMENT AND REVIEW $A = B(1+a/100)(1+p)(QHE/1000)(t+273)/300$

OFFSET $A*K1*K2*K3*K5$

<u>OVERALL RISK RATING</u>

INITIAL ASSESSMENT AND REVIEW $R = D(1+(.2E*\text{SQUARE ROOT}(AF)))$

OFFSET $R*K1*K2*K3*K4*K5*K6$

INDICES COMPUTATION
===================

INDEX	INITIAL		REVIEW		OFFSET	
	VALUE	CATEGORY	VALUE	CATEGORY	VALUE	CATEGORY
D	201				201	
F	0.84	LIGHT			3.22 E-2	LIGHT
E	4.9	HIGH			0.26	LIGHT
A	18,370	EXTREME			705	VERY HIGH
R	24,729	EXTREME			152	MODERATE

LOCATION   HASSI R'MEL

PLANT   MODULE PROCESSING PLANT 4 (MPP4)

UNIT   HIGH PRESSURE SEPARATION VESSEL   D101

MATERIALS   NATURAL GAS

ADDITIONAL INFORMATION

COMMENT
NUMBER

PRESSURE = psig 2058   TEMPERATURE t= DEG.C 60°C
MATERIAL FACTOR (Section 5)

KEY MATERIAL OR MIXTURE : METHANE
FACTOR DETERMINED BY   :
MATERIAL FACTOR   : B= 20.15
                                 RANGE   FACTOR
                                                    INITIAL   REVIEW

SPECIAL MATERIAL HAZARDS (Section 6)

	RANGE		INITIAL	REVIEW
1.OXIDISING MATERIALS	0 TO	20		
2.GIVES COMBUSTIBLE GAS WITH WATER	0 TO	30		
3.MIXING & DISPERSION CHARACTERISTICS	-60 TO	100	m -20	
4.SUBJECT TO SPONTANEOUS HEATING	30 TO	250		
5.MAY RAPIDLY SPONTANEOUSLY POLYMERISE	25 TO	75		
6.IGNITION SENSITIVITY	-75 TO	150	0	
7.SUBJECT TO EXPLOSIVE DECOMPOSITION	75 TO	125		
8.SUBJECT TO GASEOUS DETONATION	0 TO	150		
9.CONDENSED PHASE PROPERTIES	200 TO	1500		
10.OTHER	0 TO	150	20	
SPECIAL MATERIAL HAZARDS TOTAL			M 0	

GENERAL PROCESS HAZARDS (Section 7)

	RANGE		INITIAL	REVIEW
1.HANDLING & PHYSICAL CHANGES ONLY	10 TO	50	10	
2.REACTION CHARACTERISTICS	25 TO	50		
3.BATCH REACTIONS	10 TO	60		
4.MULTIPLICITY OF REACTIONS	25 TO	75		
5.MATERIAL TRANSFER	0 TO	150		
6.TRANSPORTABLE CONTAINERS	10 TO	100		
GENERAL PROCESS HAZARDS TOTAL			P 10	

SPECIAL PROCESS HAZARDS (Section 8)

1.LOW PRESSURE(BELOW 15 PSIA)	50 TO 150		
2.HIGH PRESSURE	0 TO 160	P	96
3.LOW TEMP.:1.CARBON STEEL +10C TO -25C	0 TO 30		
2.CARBON STEEL BELOW -25C	30 TO 100		
3.OTHER MATERIALS	0 TO 100		
4.HIGH TEMP.1.FLAMMABLE MATERIALS	0 TO 35		
2.MATERIAL STRENGTH	0 TO 25		
5.CORROSION & EROSION	0 TO 400		100
6.JOINT & PACKING LEAKAGES	0 TO 60		20
7.VIBRATION,LOAD CYCLING,ETC.	0 TO 100		20
8.PROCESSES/REACTIONS DIFFICULT TO CONTROL	20 TO 300		
9.OPERATION IN OR NEAR FLAMMABLE RANGE	25 TO 450		
10.GREATER THAN AVERAGE EXPLOSION HAZARD	40 TO 100		40
11.DUST OR MIST EXPLOSION HAZARD	30 TO 70		
12.HIGH STRENGTH OXIDANTS	0 TO 400		
13.PROCESS IGNITION SENSITIVITY	0 TO 100		
14.ELECTROSTATIC HAZARDS	10 TO 200		100
SPECIAL PROCESS HAZARDS TOTAL		S	376

QUANTITY HAZARDS (Section 9)

MATERIAL TOTAL TONNES	K	3.45
QUANTITY FACTOR	Q	22

LAYOUT HAZARDS (Section 10)

HEIGHT IN METRES	H	14
WORKING AREA IN SQUARE METRES	N	18

1.STRUCTURE DESIGN	0 TO 200		50
2.DOMINO EFFECT	0 TO 250		0
3.BELOW GROUND	50 TO 150		
4.SURFACE DRAINAGE	0 TO 100		
5.OTHER	50 TO 250		50
LAYOUT HAZARDS TOTAL		L	100

ACUTE HEALTH HAZARDS (Section 11)

1.SKIN EFFECTS	0 TO 50		50
2.INHALATION EFFECTS	0 TO 50		10
ACUTE HEALTH HAZARDS TOTAL		T	60

OFFSETTING INDEX VALUES FOR SAFETY & PREVENTATIVE MEASURES
****

A. CONTAINMENT HAZARDS (Section 16.1)

1-PRESSURE VESSELS
2-NON-PRESSURE VERTICAL STORAGE TANKS   0.8
3-TRANSFER PIPELINES A)DESIGN STRESSES   0.75
                     B)JOINTS & PACKINGS   0.9,0.9,0.95
4-ADDITIONAL CONTAINMENT & BUNDS
5-LEAKAGE DETECTION & RESPONSE
6-EMERGENCY VENTING OR DUMPING   0.85

PRODUCT TOTAL OF CONTAINMENT FACTORS $K_1 = 0.39$

B. PROCESS CONTROL (Section 16.2)

1-ALARM SYSTEMS   0.9
2-EMERGENCY POWER SUPPLIES   0.8
3-PROCESS COOLING SYSTEMS
4-INERT GAS SYSTEMS   0.9
5-HAZARD STUDIES ACTIVITIES   0.95
6-SAFETY SHUTDOWN SYSTEMS   0.7
7-COMPUTER CONTROL   0.85
8-EXPLOSION/INCORRECT REACTOR PROTECTION
9-OPERATING INSTRUCTIONS   0.8
10-PLANT SUPERVISION   0.81

PRODUCT TOTAL OF PROCESS CONTROL FACTORS $K_2 = 0.24$

C. SAFETY ATTITUDE (Section 16.3)

1-MANAGMENT INVOLVEMENT   0.81
2-SAFETY TRAINING   0.9
3-MAINTENANCE & SAFETY PROCEDURES   0.9,0.97,0.9

PRODUCT TOTAL OF SAFETY ATTITUDE FACTORS $K_3 = 0.57$

D. FIRE PROTECTION (Section 17.1)

1-STRUCTURAL FIRE PROTECTION   0.9
2-FIRE WALLS,BARRIERS   0.9
3-EQUIPMENT FIRE PROTECTION   0.85,0.9

PRODUCT TOTAL OF FIRE PROTECTION FACTORS $K_4 = 0.67$

E. MATERIAL ISOLATION (Section 17.2)

1-VALVE SYSTEMS   0.72
2-VENTILATION

PRODUCT TOTAL OF MATERIAL ISOLATION FACTORS $K_5 = 0.72$

F. FIRE FIGHTING (Section 17.3)

1-FIRE ALARMS   0.9
2-HAND FIRE EXTINGUISHERS   0.9,0.85
3-WATER SUPPLY   0.75
4-WATER SPRAY OR MONITOR SYSTEMS   0.95
5-FOAM & INERTING INSTALLATIONS   0.81
6-FIRE BRIGADE ATTENDANCE   0.75
7-SITE CO-OPERATION IN FIRE FIGHTING   0.8
8-SMOKE VENTILATORS

PRODUCT TOTAL OF FIRE FIGHTING FACTORS $K_6 = 0.24$

****

EQUATIONS
=========

EQUIVALENT DOW INDEX (for initial assessment and review)

$$D = B(1+M/100)(1+P/100)(1+(S+Q+L+T)/100))$$

FIRE INDEX

INITIAL ASSESSMENT AND REVIEW   F= BK/N

OFFSET   F*K1*K3*K5*K6

INTERNAL EXPLOSION INDEX

INITIAL ASSESSMENT AND REVIEW   E=1+(M+P+S)/100

OFFSET   E*K2*K3

AERIAL EXPLOSION INDEX

INITIAL ASSESSMENT AND REVIEW   A=B(1+a/100)(1+p)(QHE/1000)(t+273)/300

OFFSET   A*K1*K2*K3*K5

OVERALL RISK RATING

INITIAL ASSESSMENT AND REVIEW   R=D(1+(.2E*SQUARE ROOT(AF)))

OFFSET   R*K1*K2*K3*K4*K5*K6

INDICES COMPUTATION
===================

INDEX	INITIAL		REVIEW		OFFSET	
	VALUE	CATEGORY	VALUE	CATEGORY	VALUE	CATEGORY
D	145.84	⟋	—		145.84	
F	3.86	LOW			0.148	LIGHT
E	4.86	HIGH			0.259	LIGHT
A	1484	VERY HIGH			57.02	MODERATE
R	10890	VERY HIGH			67.20	LOW

CHAPTER V.

FMEA, FTA AND CCA APPLICATION

1. INTRODUCTION.

This chapter describes the results of the investigation of two examples of near-miss events which occured during the operation of the HASSI R'MEL gas processing plant (MPP4).

The investigation was carried out according to the procedures presented in the reviews of the Failure Mode and Effects Analysis, the Fault Tree Analysis and the Cause-Consequence Analysis.

2.INVESTIGATION PROCEDURE.

The investigation procedure is a combination of three methods of analysis. The first one, FMEA, which was used to help discriminate between minor problems and those which require thorough investigation, the second one, FTA, was carried out to spot the root causes of the near-miss event and the third one, CCA, was developed to show the possible consequences of the event of interest.

To illustrate the procedure, this section will present the results of the application of the methods to two

separate near-miss events. One being production of foam in a hydrocarbons/glycol separation drum and the other being gas blow-by in a medium pressure separation drum.

Throughout this section reference should be made to the tables and diagrams presented at the end of this chapter.

This section has been written with the assumption that the reader is familiar with the MPP4, FMEA,FTA and CCA. Appendix B1 contains a detailed description of the MMP4 and Appendices C.2, C.3 and C.4 describe how FMEA, FTA and CCA are carried out.

2.1 FMEA Application.

In order to keep good safety records in a process plant, like the MPP4, each single deviation from the normal operating conditions should be investigated. Applying the FMEA to the device whose failure resulted in the event, help to distinguish between simple deviations and near-miss events.

2.1.1 Analysis approach.

The analysis was carried out in accordance with the procedure described in Appendix C.2.

Piping and Intrumentation Diagrams for this subsystem can be found in Appendix B1, and the completed FMEA sheets

are presented at the end of this chapter.

2.1.2 Objective of analysis.

The objective of the analysis was to identity those
events which require a thorough investigation.

2.1.3 Results of analysis.

Two separate devices have been analysed using the FMEA.
The first being a level transmitter and the second being a
glycol filter.

a)Level transmitter.

Device LT 108 is a level transmitter whose function
is to provide a signal to the level controller
(LC108), the high level switch (LSH 108)and the level
indicator (LI 108) (see LICA 108 on diagram P&ID 1.1
at the end of the chapter).

The ways in which it can fail are by giving a high
or a low signal (high in our case) which could be
caused   by   the   impulse line being blocked, a
miscalibration or an internal fault.

The operational mode considered in this analysis is
the operating mode.

The effects of the failure, on the local level, will be that a high signal is sent to level controller , the level control valve positioner (LCV 108) and the high level switch. On the next higher level the effects will be that the level control valve will open too far. At the end effect the rapid fall in liquid level in D 103 will lead to gas blowby to D104 Through the liquid line.

The more reliable ways of detecting the drop of level will be the low pressure alarm (PAL 113) fitted on the vessel (D 103) which in the event of a rapid fall in level will indicate the consequent fall in pressure, and the high level alarm (LAH 111) fitted on the downstream drum D104 which will indicate the consequent rise in level in that vessel (see P&ID 1/1).

To compensate for this failure, the operator in the main control room (MCR) must put the level controller on manual and close the valve controlling the level.

The severity class (see Appendix C.2) for this particular event will be 2 since it does disturb the process and could cause the shutdown system to be initiated and cause damage to the personnel or equipment.

This kind of event is frequent but could have

catastrophic consequences if it is not properly (or quickly) dealt with.

b)Glycol filter.

Device S.302 (see P&ID 2 at the end of this chapter) is a glycol filter whose function is to remove all impurities from the glycol solution coming back from the trains.

The failure mode could be a quick saturation of its beds due to poor quality of the molecular sieves, bad regeneration procedure, fluidization of the bed or to a malfunction of the pressure differential recorder (PdR 302 part of PdRA 302) which should give an alarm whenever the filter is saturated and needs to be regenerated.

The mode of operation under which the event happened was the operating mode.

The local effect of the failure is that the glycol is not properly filtered affecting, on the next higher level the regeneration unit particularly the distillation section (foaming in the column, cavitation of the bottom pumps etc.) which at the end will cause foaming in some parts of the main process.

The failure detection mode (when noticing all these

effects) is to compare the readings given by the pressure differential recorder (PdR 302) and the ones given by the pressure gauges at the inlet (PG 306) and the outlet (PG 307) of the filter.

The best way to compensate is to inject an anti-foaming agent and put both filters on operating mode while permutating the two regeneration units (45 and 46, see Appendix B2 P&ID A015) . Since this particular failure can be counteracted and controlled without major disturbance to the process it will be classified as class 3 severity.

2.2 FTA and CCA application.

To avoid repetitions due to the complementarity of the two methods, the fault trees and the cause-consequence diagrams will be discussed in this section at the same time.

The FTA investigated the causes and failure paths that result in the near-miss event while the CCA investigated the failure paths that lead to catastrophic events (e.g. fire or explosion).

2.2.1. Objective of analysis.

Two objectives were assigned to this analysis. The first one was to identify the concurrent failures necessary to

cause the near-miss event being considered and those which could lead to the worst consequences and,the second one was to show the importance of investigating near-miss events since these investigations are of many advantages, the most important being the gain of experience in safely operating the process.

The analysis was restricted to failures in the control system. The analysis was limited to the train and the glycol regeneration unit.

2.2.2 Analysis approach.

The fault tree analysis and the cause-consequence analysis investigating near-miss events were carried out in accordance with the procedures discussed in Appendices C.3 and C.4.

The events determined by the FMEA as being near-miss events were more deeply investigated by developing fault trees and a cause-consequences diagrams. Each event being at the same time the top event of the fault tree analysis and the starting point of the cause-consequence analysis. The following events were analysed:

    a)Gas blowby from D103
    b)Foaming in D106

2.2.3 Gas blowby.

The fault tree for gas blowby is shown in sheets FTA 1/1. P&ID A1004 in Appendix B2, P&ID 1/1 and P&ID 1/2 at the end of this chapter, show the interrelationship of the components making up the level control system.

If the liquid in the vessel falls below the outlet level allowing gas into the outlet pipe, gas blowby will occur. Generally, liquid is fed to a vessel which operates at lower pressure. Therefore, gas blowby may result in the downstream vessel being subjected to a pressure above its design pressure.

The level control valve on the liquid outlet must remain wide open so that the liquid outflow exceeds in inflow. The level must fall slowly to a sufficiently low level before the low pressure alarm PAL 113 will attract the operator attention.

To follow the rule of the "worst case" (see Chapter 3 section 6.1.2), it is assumed that the operator has insufficient time to rectify the situation, because no low level alarm is fitted on the vessel. The tree gives a pessimistic view because it is assumed that the delayed operation of the pressure alarm gives the operator insufficient warning but it stresses that the factor time plays a major role in the succession of events.

The downstream drum D 104 is protected against

overpressure by a wide variety of devices which initiate shutdown or relieve the excess pressure in the vessel. CCA1/1 and CCA 1/2 shows the relationship of the events which may cause the vessel to rupture and release hydrocarbons into the module. P&ID A1004 in Appendix B.2 shows the instruments in this section.

For rupture to occur, the vessel must be exposed to a pressure greatly in excess of its design pressure 37.7 Kg/cm2G. This can only occur if there is a source of overpressure and the pressure safety valves fail to relieve the excess pressure. In the case of gas blowby from D103, the D104 will be submitted to a pressure of 70 Kg/cm2G which is about 186% that of its own working pressure.

PSV 105 and HXC 108 are two pressure safety valves fitted to D104. An interlocking system prevents both valves from being locked off or on simultaneously.

The other events in the diagram show how the shutdown system protects D 104.

There are two methods of protection. The first is to isolate the train by closing PIC 139. Secondly, the pressure may be vented by HIC 107 A&B and PSV 104 opening, or should these valves fail to open the gas may be vented to the flare system via UZ 138 or UZ 135. The latter valves are situated on the discharge of K101 A&B. Both

valves open when shutdown is initiated.

In principle FTA and CCA can be used to quantify the hazard of having gas blowby, but in the case of the present work the lack of data makes it impossible.

2.2.4 Foaming.

The fault tree for foaming is shown in sheets FTA2/2.

Foaming occurs, in our case, as a result of the presence of small particles of impurity on the surface layer of liquid in the hydrocarbons/glycol separation drum D 106. This causes the liquid level to rise in appearance leading to a consequent response of the level control loop. The residence time of the liquid in the vessel being less than the one prescribed by the design, results in glycol being entrained with the hydrocarbons to the bottom part of the column C 101.

The fault tree shows that the improper operation of the glycol filter at the entrance of the glycol regeneration unit is the cause of foam formation in D 106.

If glycol is present in the bottom part of the column it will decompose since the temperature at the bottom of the column exceeds the glycol decomposition temperature. The residue (carbon) resulting will be pumped with the hydrocarbons to the furnace and will deposit and form a

layer which will reduce the heat transfer coefficient. The end result will be the formation of hot spots which lead to the rupture of the tube and in hydrocarbons being released in the furnace resulting in fire or explosion.

There are two methods of protection. The first is to inject an anti-foam agent into the glycol going to the trains. Secondly, permutate the two glycol regeneration units to be able to change the molecular sieves of the filters causing the problem.

3. DISCUSSION OF THE RESULTS.

The two near-miss events that have been chosen to illustrate the study of methods happened only when the MPP4 was in normal operating mode. Hazardous events that occur during startup and shutdown should also be investigated.

The analysis was restricted to considering the ways in which hydrocarbons could be released into the train as a direct consequence of near-miss events. The trees that have been drawn do not show that hydrocarbons can be released due to small leaks. For example, gas may escape from valve glands, instruments, fittings and flanges.

The fault tree drawn from API RP 14c which is contained in Appendix C.3, shows that mechanical deterioration due to corrosion can also be a factor in hydrocarbons being

released. This was not taken into account in this analysis.

3.1 Modeling operator intervention.

I have found it difficult to accurately represent the opportunities given to the operator to correct deviations from the normal operating parameters. The assumptions that I have made are pessimistic.

The analyst can work out what indications the operator will have given a particular set of circumstances. The operator may misinterpret these data and fail to prevent the fault condition from arising. Most analysts remodel the fault tree to take account of operator intervention after the basic structure has been decided.

3.2 Gas blowby.

Gas blowby may appear to be a serious problem, but this is not the case as high pressure switch and pressure safety valve protect the downstream vessel which is being subjected to high pressure as a result of gas blowby.

Rupture of the downstream vessel would only result if the pressure to which it was subjected was sufficient to cause rupture (more than 150% of the working pressure) and if the protection devices failed simultaneously.

At least two pressure safety valves are fitted to each

pressure vessel and to the discharge lines of the turbo-expanders. These valves are fitted with an interlock mechanism which prevents them from being locked off simultaneously. This of course also prevent the valves being locked on at the same time.

The interlock mechanism allows each valve to be tested and calibrated without lowering the standard of overpressure protection as the other PSV must be locked on before maintenance work can commence. There is much to commend this practice as it ensures that a valve can not be incorrectly locked off.

The cause-consequence diagrams and the fault trees show the protection afforded by the shutdown system. Although the risk inherent in processing gas are high, the shutdown system ensures that a minimum of four simultaneous failures are required to cause the rupture of equipment, the absence of common mode failure render this possibility very unlikely. No quantitative analysis could be carried out due to the abscence of data (nonavailable), but it seems likely that the probability of vessel rupture is small.

3.3 Foaming.

The main element shown by the analysis is the extent to which simple event like foam formation in a separation drum will lead. Foaming being a common occurrence the

build up of carbon in the furnace is likely to occur over a long period of time leading to the formation of hot spots. However, it is very difficult to account for time in both FTA and CCA.

4 COMMENTS.

The combination of the different hazard analysis methods (FMEA, FTA and CCA) render the investigation of near-miss events easier than if just one of these methods is used alone. The FMEA select which events should be studied in a deeper way. This allow time to be saved since those events which do not present substantial hazards will be identified at this stage. The FTA determines the root causes of the near-miss event, thus help understanding the different mechanisms which led to the top event. Finally, the CCA points out the weak parts of the process and gives an idea about the hazards behind the near-miss event under investigation.

In conclusion it appears that foam formation is more likely to cause a problem over a period of time than gas blowby. The quantification of these models was not conducted due to the lack of data. This emphasises the fact that there is a need to collect data on failure rates etc., which can be used in such studies.
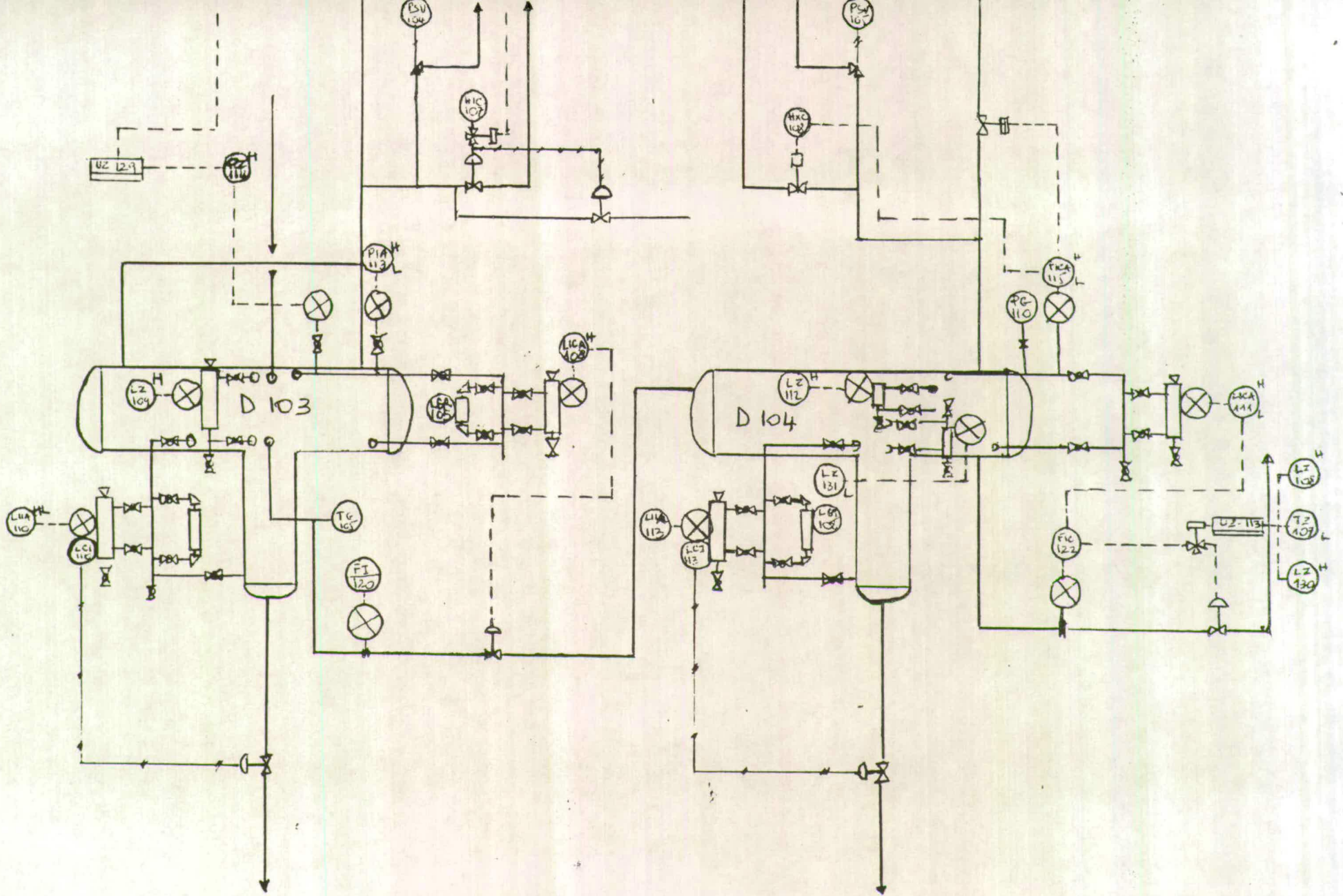
P&ID 1/1   D103 and D104
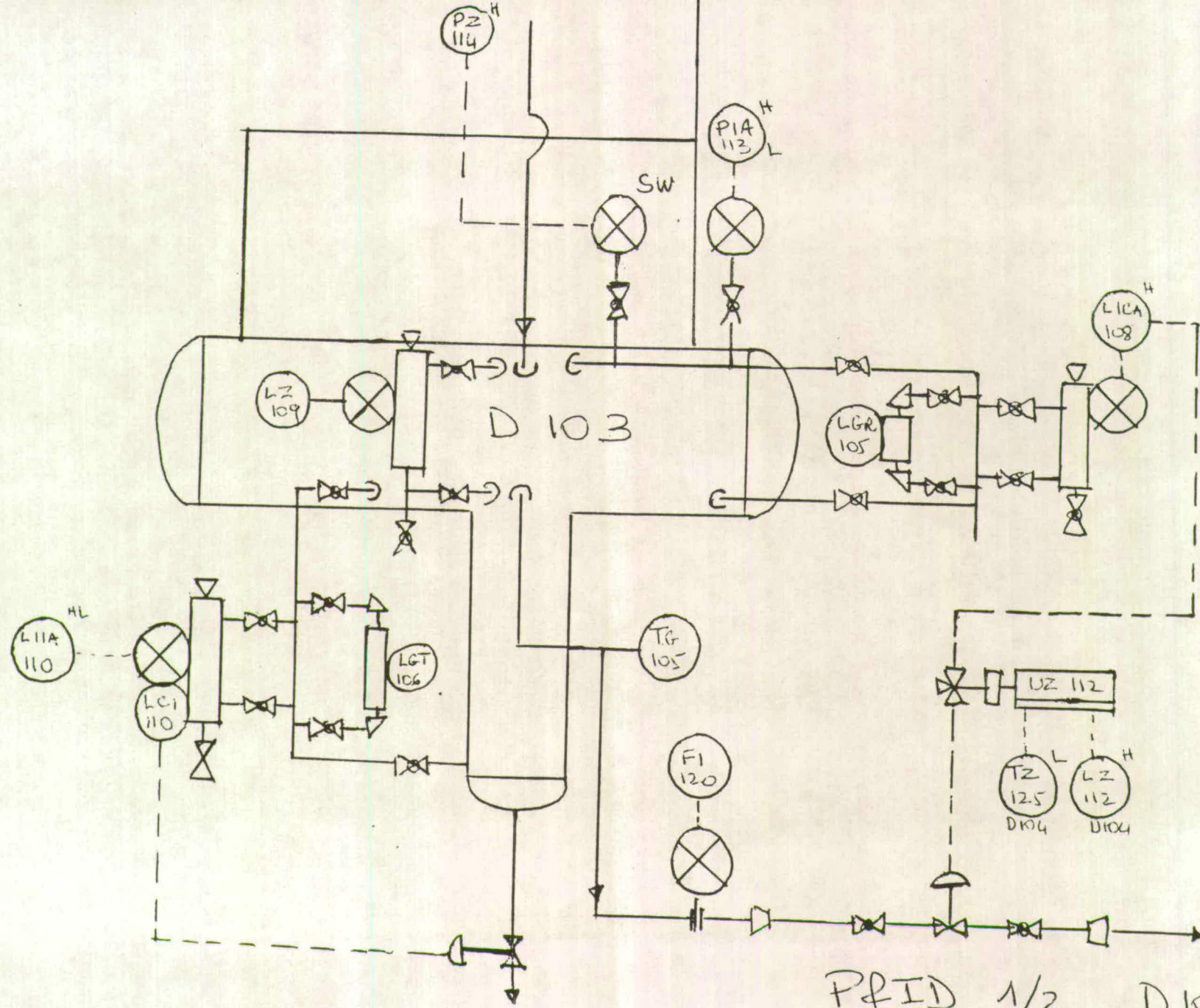
P&ID 1/2 D103
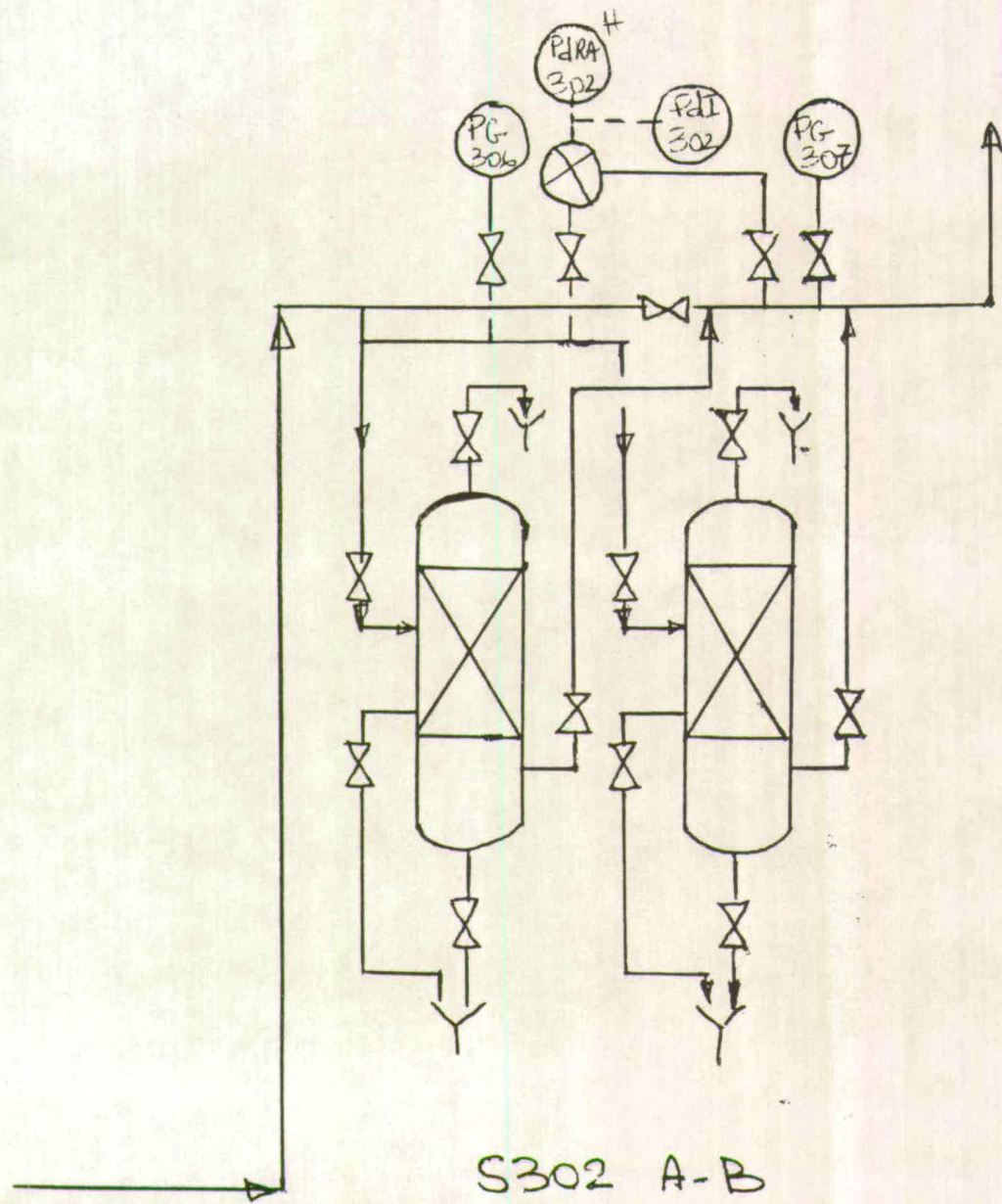
S302 A-B

P&ID 2   S302-AB

SYSTEM : GLYCOL REGENERATION UNIT

INDENTURE LEVEL : SUB-SYSTEM

REF. DRAWING : A1-015

MISSION : REMOVE IMPURITIES
FROM GLYCOL
SOLUTION

DATE 10/9/89

SHEET 1

COMPILED BY Faidi

identification number	item/functional identification (nomenclature)	function	failure mode and causes	operational mode	FAILURE EFFECTS			failure detection method	compensating provisions	severity class	remarks
					local effects	next higher level	end effects				
S 302 A-B	Glycol Filters	remove all impurities from glycol solution	QUICK SATURATION 1) bad regeneration 2) bad quality of molecular sieves 3) fluidization 4) PdR 302 miscalibrated	OPERATING	glycol badly filtred	-foaming in the regeneration column - P302 cavitates	FOAM FORMATION IN THE PROCESS	PdRA^h 302 gives warning when the saturation level is reached	1) put both filters on operation while starting up the unit	3	this fault may lead to large consequences if not properly dealth with

117

SYSTEM :

INDENTURE LEVEL :

REF. DRAWING :

MISSION :

DATE 10/9/89

SHEET 2

COMPILED BY Faidi

118

identification number	item/functional identification (nomenclature)	function	failure mode and causes	operational mode	FAILURE EFFECTS			failure detection method	compensating provisions	severity class	remarks
					local effects	next higher level	end effects				
LT 108	level transmiter	signal level to controlle. and alarms	HIGH SIGNAL 1) impulse line blocked 2) miscalibrated 3) internal fault	OPERATING	high signal to level controller, valve positioner and high level switch	level control valve open too far	liquid level drops	PAL113 signal dr p in pressure resuting from level falling	put controller on manual and close valve from MCR	2	if the level drops slowly the resuting pressure fail will not reach the pressure alarm. The event will not be noticed
			LOW or NO SIGNAL 1) impulse line blocked 2) miscalibrated 3) internal fault	OPERATING	low or no signal to other instruments	level control valve shut too far	level rises	LZH109 warns operator of extra high level. Compare indicator with level gauge	put controller on manual and open valve from MCR	2	

FTA 1/1 GAS BLOWBY

119

FTA 1/2 PAL . FAILS

```
                    ┌──────────┐
                    │   GAS    │
                    │ BLOWBY   │
                    └────┬─────┘
                         │
                    ┌────┴─────┐
                    │  OVER    │
                    │ PRESSURE │
                    │    IN    │
                    │  D 104   │
                    └────┬─────┘
                         │
                    ┌────┴─────┐
                    │  PIC 115 │
                    │  OPENS   │
                    │  100%    │
                    ├────┬─────┤
                    │YES │ NO  │
                    └────┴─────┘
```

positionner stuck   valve stuck   miscalibrated   internal fault

PIC 115 lifts over pressure — YES | NO

deviation corrected

internal fault   impulse line blocked   valve stuck   PAHH fails

HXC 108 OPENS — YES | NO

HXC 108 LIFTS OVER PRESSURE — YES | NO

deviation corrected

1
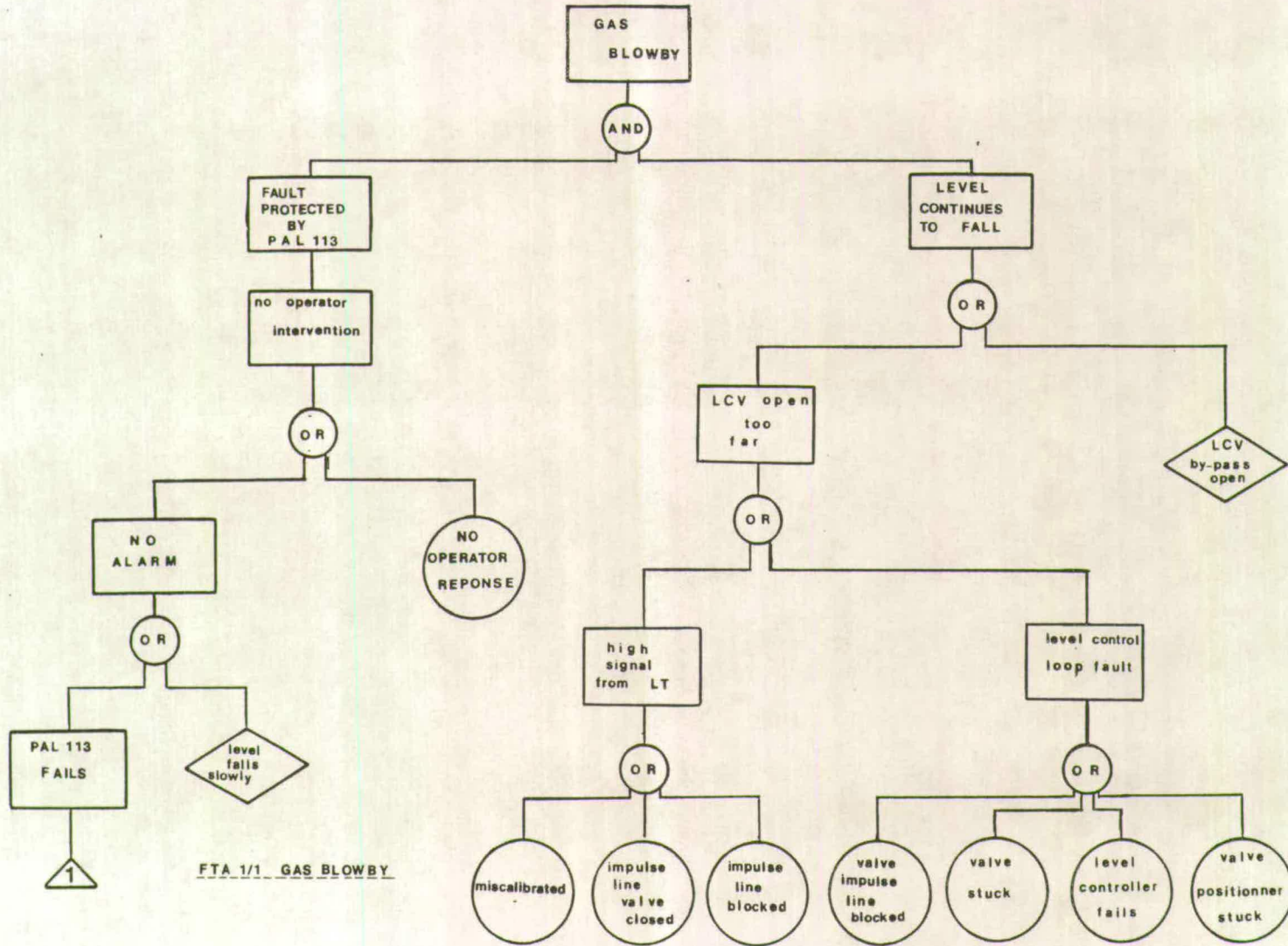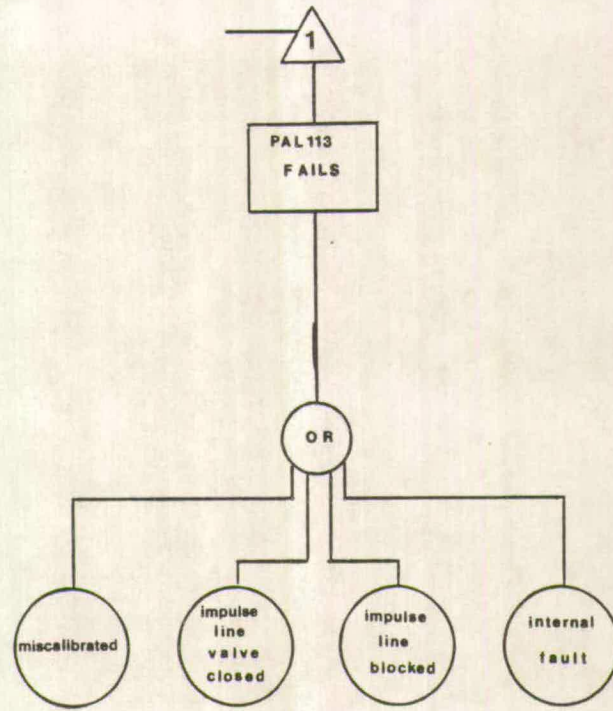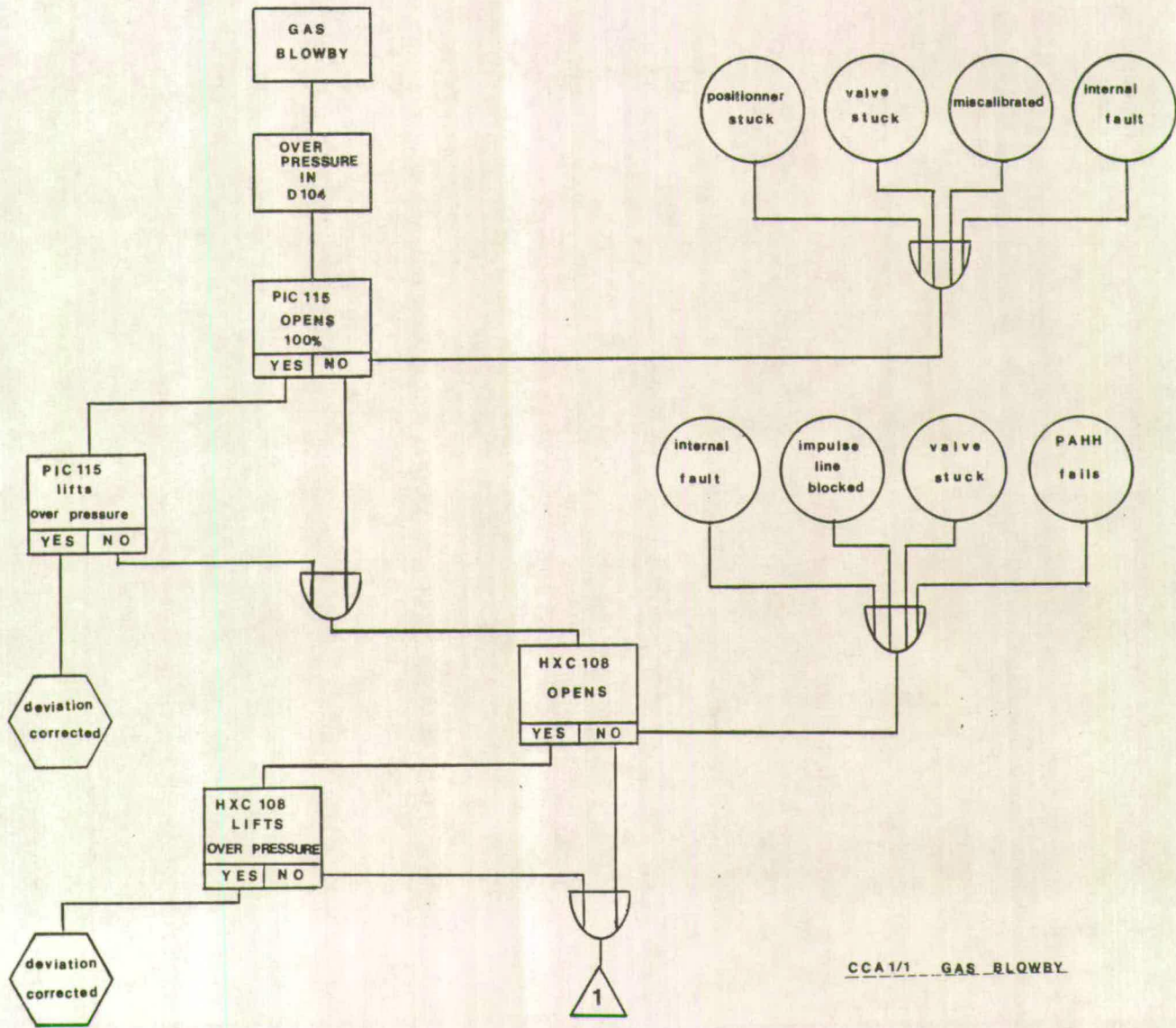
CCA 1/1   GAS BLOWBY
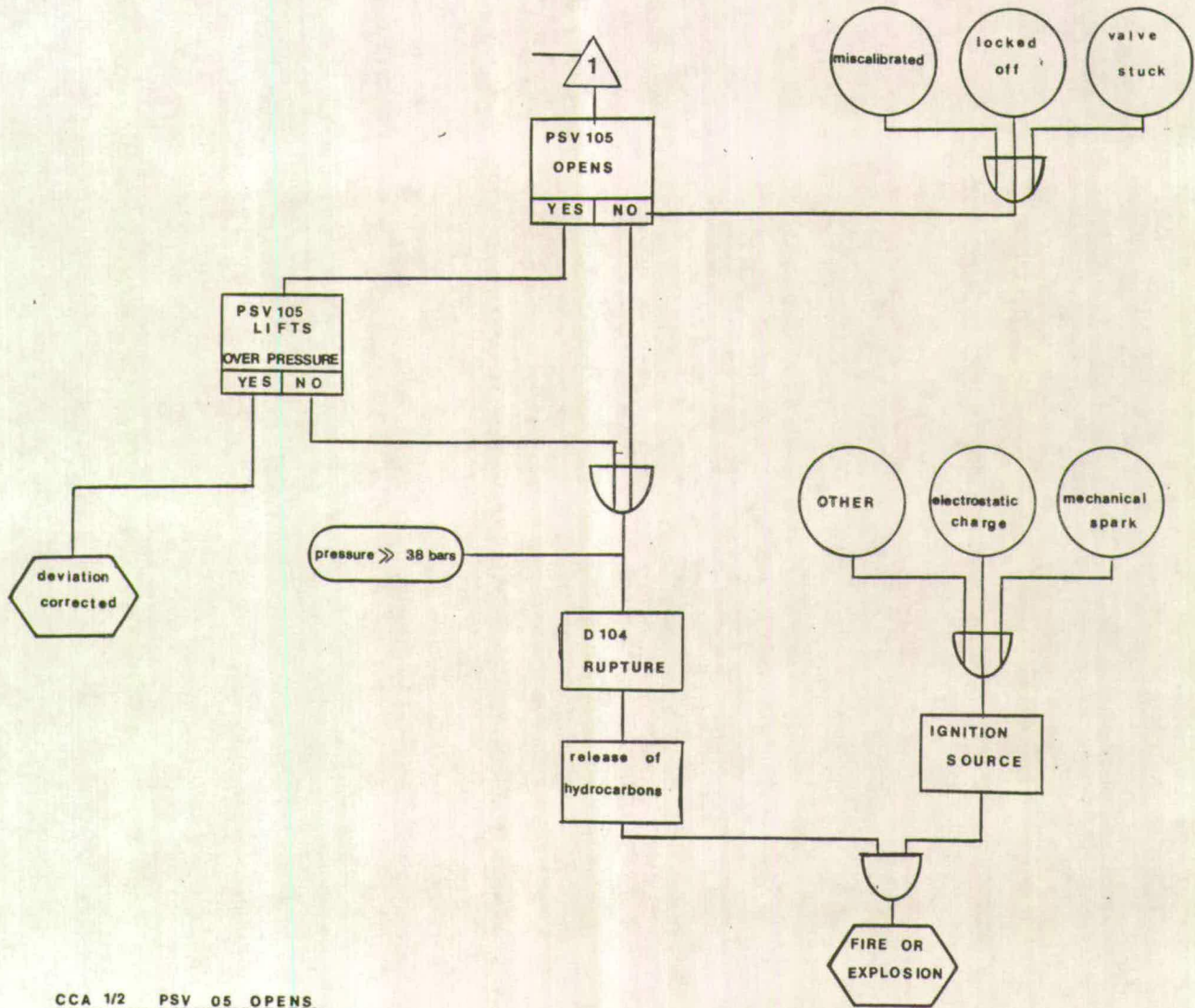
CCA 1/2   PSV 05 OPENS

FTA 2/1 LEVEL RISE

123

FTA 2/2 FOAMING

PUMP
FAILURE

OR

Pump shutdown
initiated

high
temperature
of motor
bearings

low
liquid
temperature
TZ 107
FAILS

OR

LZL 120
FAILS

LZL 122
FAILS

FTA 2/3 PUMP FAILURE

125

126
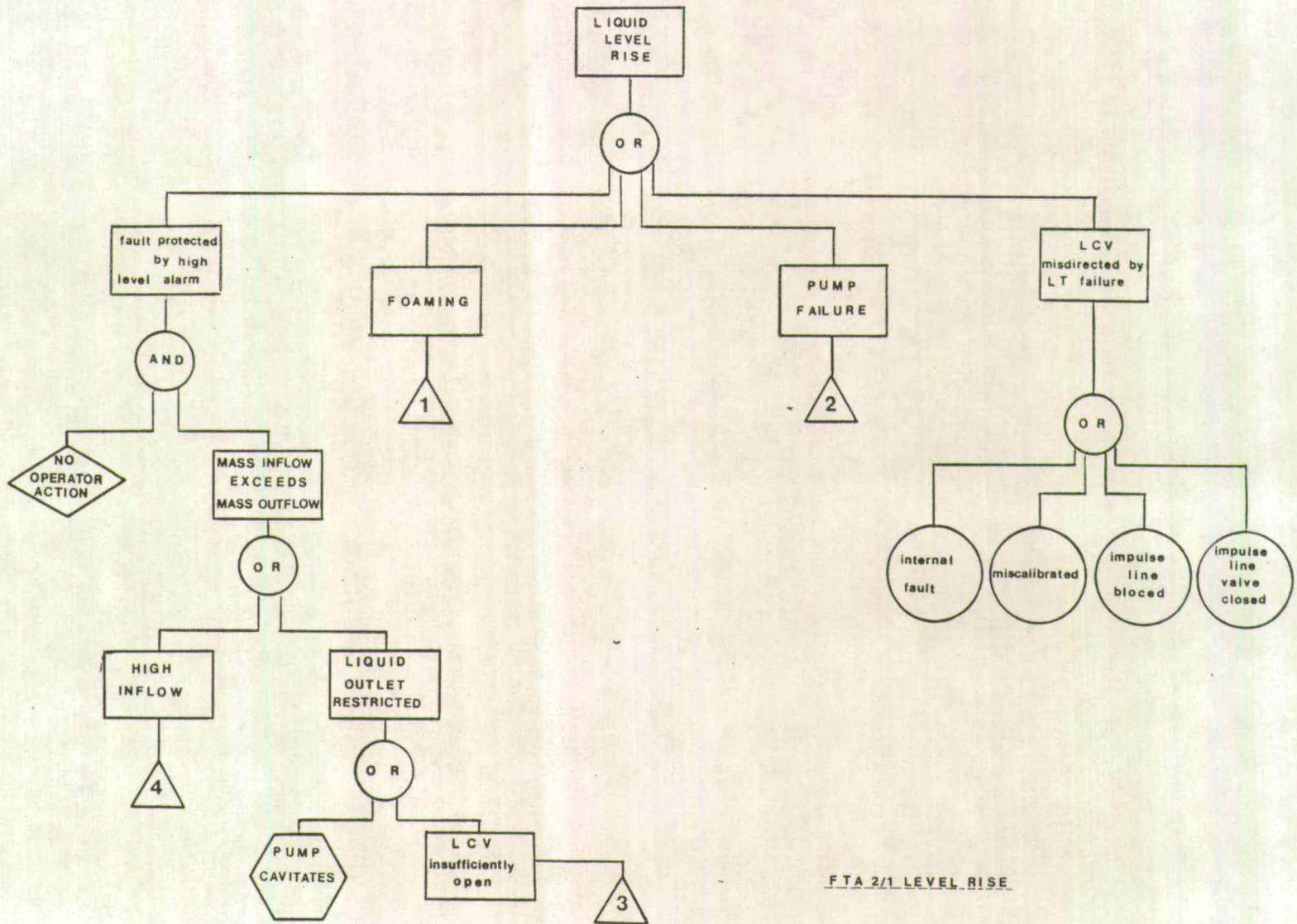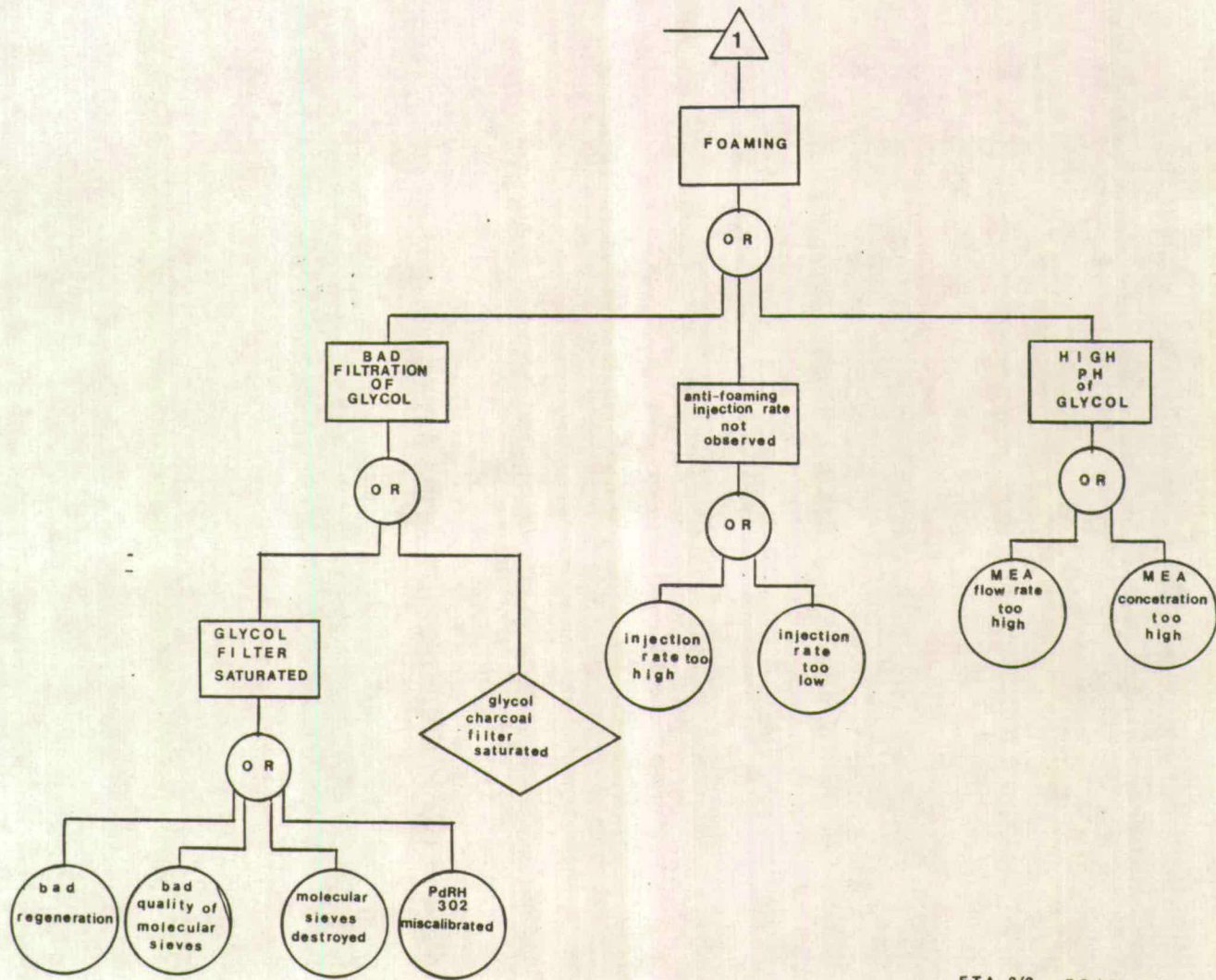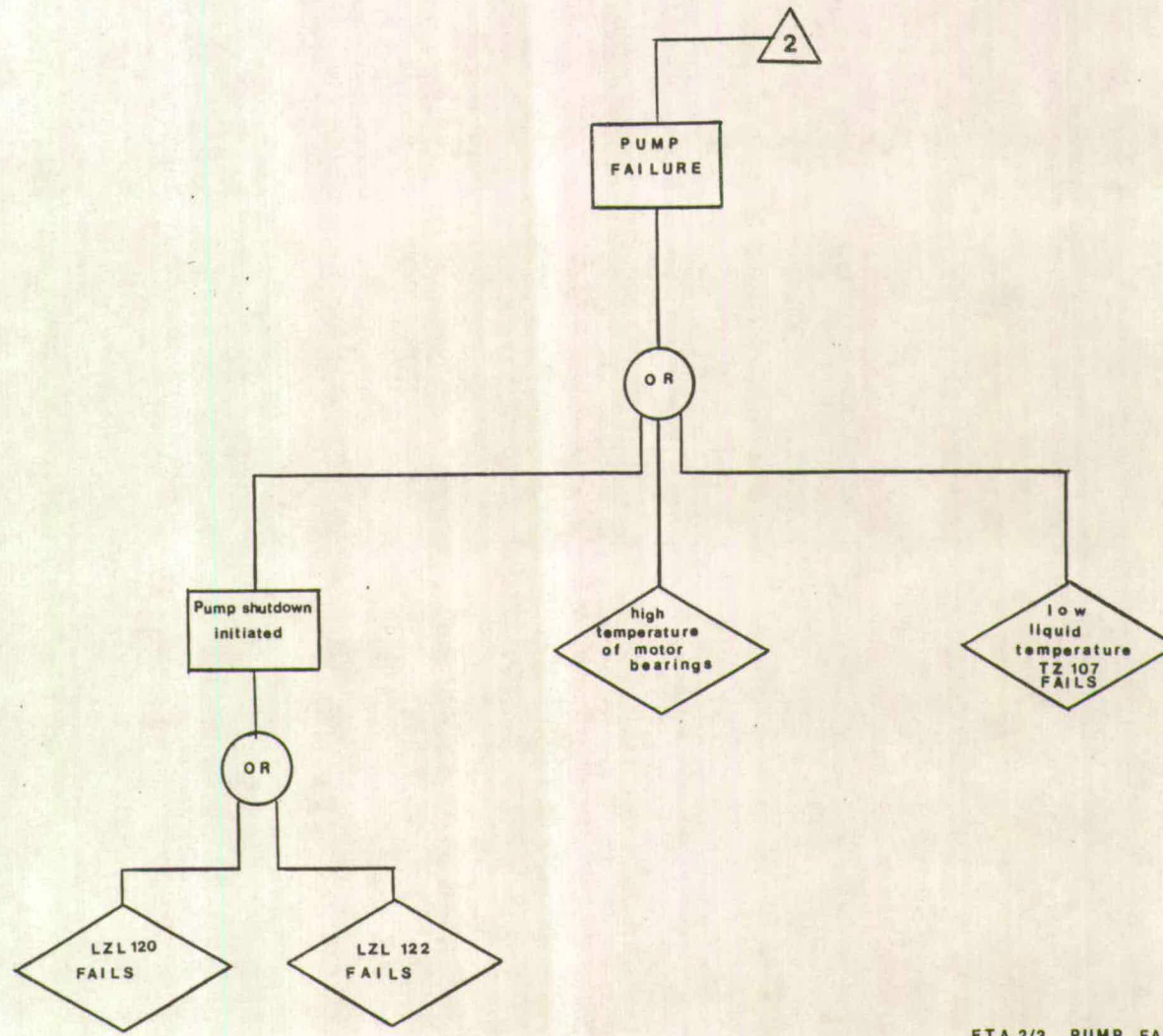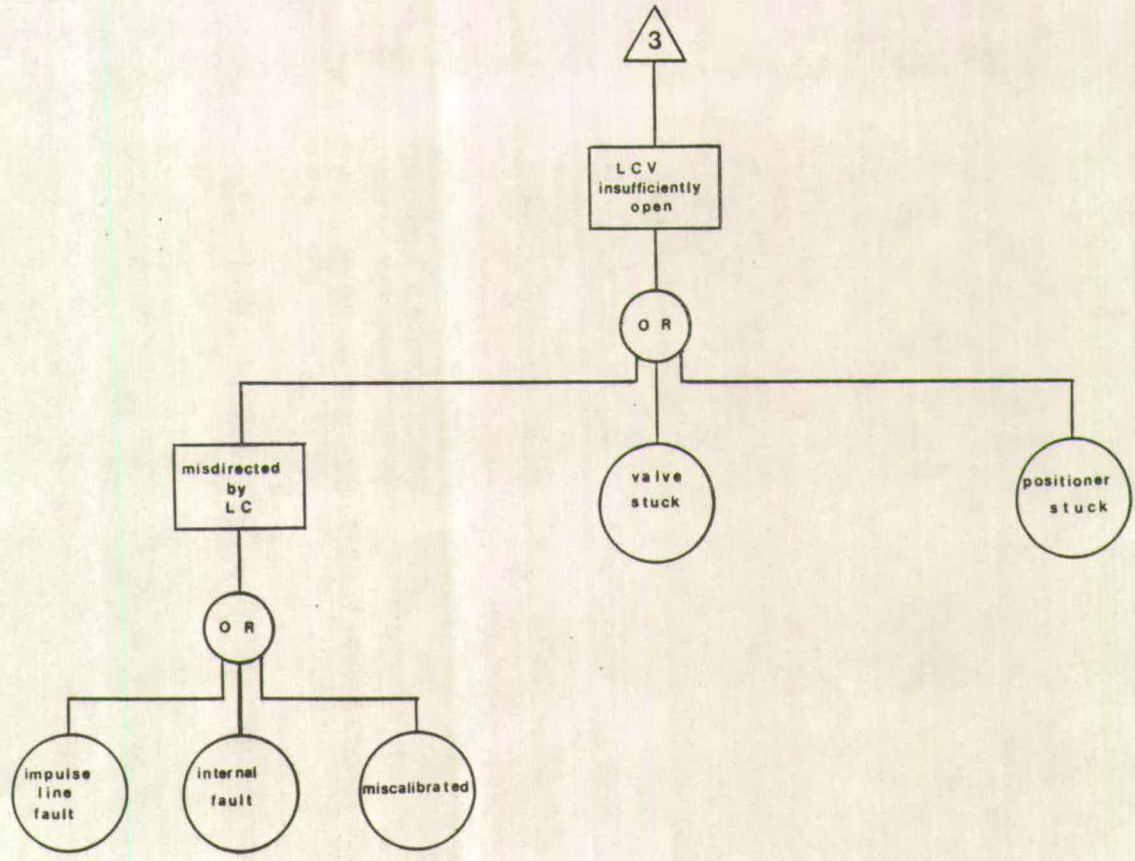
FTA 2/4 LCV insufficiently open
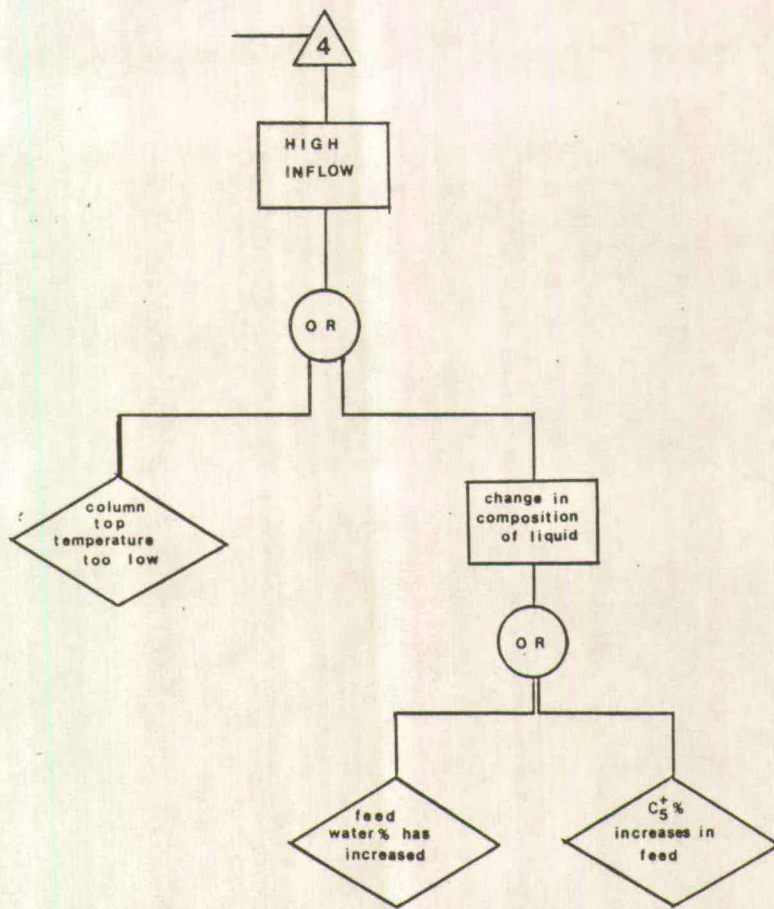
FTA2/5 HIGH INFLOW

CCA 2 FOAMING

128
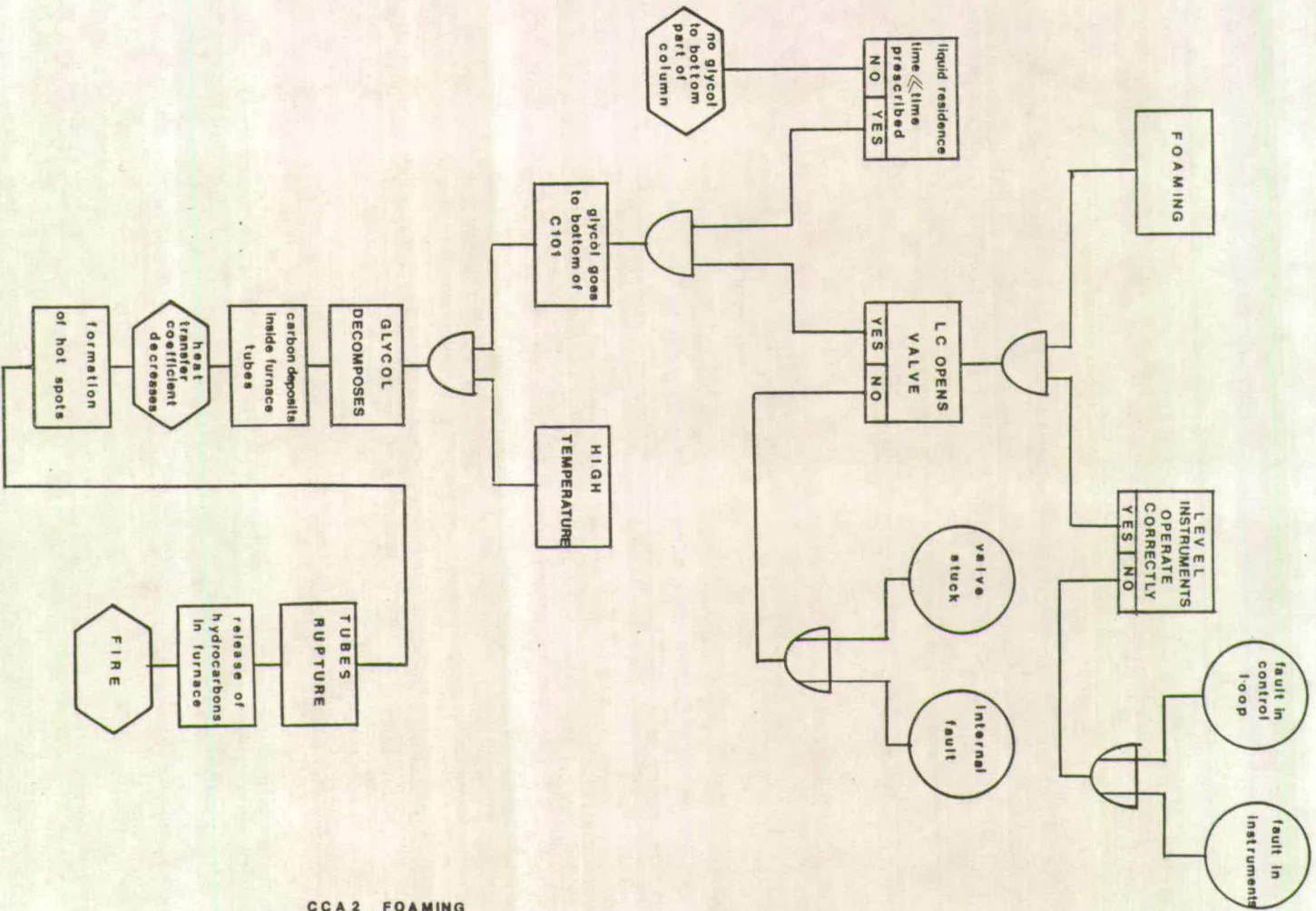
CHAPTER VI.

CONCLUSIONS.

1.INTRODUCTION.

The exploitation of industrial installations processing hazardous substances always presents some degree of unwanted and sometimes unforeseen hazards which if not controlled will result in catastrophic events.

Since the complete elimination of hazards is almost impossible, the only way to deal with them is to limit the frequency of their occurence by preventing as much as possible failures and consequently releases, and limit their eventual consequences. This can be achieved in a first step by the remote location of industrial installations with relation to populated areas. At the plant level, the layout of the different equipment and units contributes a great deal in preventing escalation of incidents. The second step is to devote more attention to the design, fabrication and inspection stages in order to avoid early errors which might be costly later on. The third step, which is the most important specificly in the context of the Algerian petrochemical industry is to avoid departures from the operating conditions during the operating stage (in order not to alter the integrity of the equipment), to have a high standard of training for

all personnel, to adhere to the established operating procedures, to check regularly the safety and control systems and investigate minor accidents, abnormal circumstances, and near misses. Similarly, maintenance operations and/or modifications should be carried out with caution.

As already mentioned, the two main objective of this study, were to learn about the different hazard analysis methods and to provide a way of investigating near-miss events.

The investigation of near miss-events should be conducted in a selective and progressive manner to concentrate the efforts (time and money) on the events that present a serious threat to life and/or property. The more an event is hazardous the deeper the study should go. For example, a leaking valve in the water treatment unit will not be given as much consideration as a leaking valve in the high pressure separation unit where hydrocarbons are released to the atmosphere. Applying the Mond Index to the whole plant gives indication on which unit sould be monitered with greater attention. The events occuring in this particular unit should be given more consideration with regard to the events occuring in the other units of the plant. This does not mean in any way that the latter should be ignored. The most important factor in applying the Mond Index is the division of the plant into blocks or units to be investigated separately. This factor

influences a great deal the final outcome (see Chapter 4).

The FMEA specifies the failure modes of the component, the effects of these failures at different levels of the system/process, and more importantly gives a ranking of the possible consequences of failures. Referring to the example given above, the position of the valve , its size, the amount and nature of material released, etc. will give a clear indication wheather a more detailed investigation is needed or not. The weakness of this method is that it is impossible to include the human factor in the analysis.

Finally, if required (see FMEA results) both FTA and CCA are carried out to determine the root causes of the incident and to show the possible consequences. If the analyst can assemble enough data, a quantification of the trees produced by the FTA and the CCA would give substantial information on the probability of occurence of such an event and its consequences. This will help deciding if more preventive and protective measures should be introduced in the process.

2.EVALUATION OF METHODS.

It is clear from the brief descriptions already given in Chapter 3 that most of the methods of hazard analysis are dissimilar except Fault Tree Analysis and Cause Consequence Analysis which complement one another and will

be evaluated under the same heading. Although the procedures are very different, the principles upon which the methods are based and the objectives of the techniques are alike. Each aims to identify aspects of the design which are unacceptable and require to be modified. Thus each aims to help to ensure the safety of the personnel and the plant.

The basis upon which the methods were evaluated is subjective, being based on "hands on" experience gained during their use in studying the near-miss events. The following criteria where chosen:

      a)The understanding of the process required

      b)The ease of application, and

      c)The time required to carry out the analyses.

2.1 Understanding Of The Process Required.

The first criterion upon which the evaluation was based was the understanding of the process which the analyst required before the analysis could begin. This is directly dependent on the level of detail into which the method itself goes.

The more detailed methods, like FTA and CCA, require a greater understanding of the system before the study can begin. The understanding required of the analysis technique to be used is discussed in subsection 2.2.

2.1.1 Mond Index.

The analyst needs to be acquainted with the general design parameters of the process being studied. As the method is a rapid ranking tool, the analyst can use approximations of various factors without seriously affecting the outcome. The detailed information that the Mond Index needs can be easily obtained from the design specifications.

2.1.2 FMEA.

The understanding of the process required by the analyst before an FMEA is begun is dependent on the indenture level at which the system is studied. At high levels, at for example the failure of whole systems, the analyst needs to understand how the system interacts with the other systems on the plant. Drawing functional dependency diagrams is a useful way of gaining this knowledge.

Where the failure of instruments is being studied, the analyst must know what types of devices are being used and the ways in which they can fail. The FMEA of the near-miss events required such knowledge. During the study I constantly refered to the operating manual.

2.1.3 FTA and CCA.

The analyst requires an intimate knowledge of the system

and the operating procedures used to control the process. The breadth of knowledge required is dependent on the top event or events which are to be investigated.

This understanding of the system can be gained by studying the piping and instrumentation diagrams (P&IDs), the design specifications, the operating procedures and the system description manual. Where an existing system is studied, a visit to the process and discussion with the operators are invaluable.

2.2 Ease Of Application.

The second criterion used to evaluate the methods of hazard analysis used in this study was the ease with which the techniques could be applied during the design phase of a plant project.

This criterion is based on the understanding of the method required before it can be used. It is also based on my experience of using each method in this study.

2.2.1 Mond Index.

In general, points schemes do not require the user to have a detailed understanding of the principles inherent in the approach they adopt. For example, the user does not need to understand why an index is calculated in the way it is. The analyst needs only to be conversant with its

use and can become so by proceeding step by step through the technical manual. However, when dividing the plant into unit much attention should be paid since this could influence the final results.

2.2.2 FMEA.

The most definitive document available on FMEA is the MIL-STD-1692A from which the procedure described in Appendix C.2 was written. Although many papers have been published on the use of FMEA in the nuclear industry by Taylor of Riso, the method has not been used extensively in the petrochemical industry.

The procedure described in Appendix C.2 was found to be readily applicable to the investigation of near-miss events. The standard forms which are completed ensure that the study is adequately documented. This also assists the review of the analysis by an independent analyst.

Appendix C.2 recommends that functional dependency diagrams (FDDs) be drawn for each sub-system studied. However I found that it was more helpful to redraw the piping and instrumentation diagrams (P&IDs) as these are themselves FDDs.

2.2.3 FTA and CCA.

An analyst must have a detailed understanding of FTA and

CCA before begining an analysis of a complex system. It is very easy to make logical errors which may be the result of an inadequate understanding of the process or of the techniques.

It is also difficult to model a dynamic system using a fault tree diagram as the state of the system is constantly changing. The use of inhibit gates helps to overcome this problem by allowing the analyst to specify the extent of the failure before the top event can occur.

The difficulty of modelling the system is lessened if the analysis is qualitative and is restricted to the study of failure paths. The assumptions that are made must be documented particularly those relating to the intervention of the operator to rectify faults.

2.3 Time Required.

In the following sub-sections estimates are given for the amount of time required to become familiar with the method of analysis and the system to be analysed, and thirdly for the time required to carry out the study.

2.3.1 Mond Index.

The application of the Mond Index can be learnt in two working days and experienced users would be able to carry out a calculation in less than an hour. This however

depends on having all the information required on hand when calculating the Index. A design engineer who is familiar with the technique would be able to carry out the calculation in the same time, perhaps even less as he is already acquainted with the design specification.

It can take longer to carry out an analysis of existing plant because the design information must be sought out first. These data are generally not readily available.

2.3.2 FMEA.

An FMEA is often used by an analyst to gain a better understanding of a system. The analyst need not therefore spend a lot of time to gain an understanding of the process before starting the analysis. Approximately three working days would suffice. He does however require to have a good background understanding of devices used in the system.

The description and FMEA procedure set out in Appendix C.2 explains the basic principles of FMEA. It would take about a week to become familiar with FMEA.

The amount of time required to carry out the analysis is dependent on the detail to which the analyst studies the process. I estimate that the analysis of a specific near-miss event would take one working day. A further day should be allowed for report writing.

Again I think that an engineer who is familiar with the method and the system could complete the study in less time.

2.3.3 FTA and CCA.

Like FMEA, there are few practical descriptions of how to carry out FTA or CCA. Appendices C.3 and C.4 bring together the basic principles that the engineer must be familiar with before attempting to carry out an FTA or CCA. It would take 7 working days to become familiar with each technique.

FTA and CCA require a thorough knowledge of the process which is to be studied. This takes a minimum of two weeks and further study of the system may be needed as the analysis is completed.

The objectives of the FTA and CCA will affect the amount of time the analysis would take to complete. If the analysis is qualitative four weeks should be sufficient. A quantitative study requires the collection of data and also requires greater accuracy of the trees and diagrams. This could take over seven weeks to complete. A point that is easily overlooked is that it takes quite some time to draw the trees or diagrams.

3. RECOMMENDED USE OF METHODS.

The scope and use of each method of analysis used in the study is discussed in the following sub-sections. Should an engineer wish to use an alternative method to those discussed here, the review of method analysis in Chapter 3 may be of some use.

3.1 Mond Index.

The Mond Index could be used to identify weakness in existing processes which require attention. It may however be more cost-effective for a company to develop a rapid ranking points scheme for its own use. This type of in-house scheme can be written so as to reflect company policy and can be used to review existing processes as well as those that are being designed.

It may be used to evaluate alternative protection strategies by assessing the way each mitigates the risk inherent to the process.

The Mond Index could also be used at the preliminary stages of design to compare alternative process designs. The chosen process would however require to be studied in more detail during the later stages of the design.

3.2 FMEA.

FMEA is a useful fundamental method of analysis whose

principles can be applied by the user to study the causes and effects of failures in any system or process. FMEA is a tool which enables the user to identify the hazards inherent in a process, and to assess the way in which these hazards may cause the occurence of hazardous events. FMEA can be oriented to the failure of equipment or consider the failure of the operator.

Although FMEA is a laborious method, if it is carried out during the design, the analysis should not delay the progress of the project. Care must be taken to review any modifications in the design as the conclusions of the FMEA may be annulled by these design changes.

FMEA is also a useful aid to more detailed analyses such as Fault Tree Analysis or Cause-Consequence Analysis. The FMEA can be used to help to discriminate between minor problems and those which require thorough investigation.

3.3 FTA And CCA.

FTA or CCA should be used to study problems which have been identified during less detailed analysis such as one carried out using FMEA.

FTA and CCA are time consuming and difficult, and the analysis may need to be carried out by an experienced analyst in preference to the design engineer. For example, the complexity of the system to be modelled may prevent the design engineer from carrying out the analysis as he

has neither the time nor the experience needed. Where a problem requires to be investigated using FTA or CCA, the analysis should be started at the earliest possible opportunity. An analysis which is begun at a late stage in the design may result in the project being delayed or modification having to be made during rather than before the construction phase. As the resulting financial penalties incurred are great, the engineer should ensure that the hazard analysis begins when the design process starts.

Where a quantitative analysis must be carried out, FTA or CCA are the obvious choice as these methods lend themselves to this form of analysis. It is a popular misconception however that fault trees or cause-consequence diagrams must be quantified. In many cases the decisions reached by a visual inspection of the diagrams by an experienced engineer are likely to be the same as those decisions which have a quantitative basis.

These are instances where the design engineer is required to justify the inclusion of additional safety measures to senior managment. Fault trees or cause-consequence diagrams can be used by the engineer to illustrate the value of the proposed measures. These diagrams can be readily understood by senior personnel who may be unfamiliar with the process.

Where the process system is to be controlled by

computer, the computer specialists also model the system. Considerable duplication of effort could be avoided if the hazard analyst were to work alongside the computer specialists.

4. QUANTITATIVE ANALYSIS.

There is considerable resistance by the Algerian petrochemical and gas industry in carrying out quantified hazard analysis. There are mainly two reasons.

-Firstly, quantified hazard analysis is restricted on the grounds that the models used are incomplete and that the basic failure rate data are unavailable or unapplicable. These reasons will steadilly diminish in importance as failure rate data are obtained, modelling tools improve, and computer controlled systems are developed.

-Secondly, the potential financial losses in the oil industry motivate most companies to ensure that the acceptable risks are kept to a minimum. In most cases where a problem has been identified, oil companies are prepared to spend money to rectify them. Every improvement in financial loss prevention has a commensurate effect on life safety.

Whilst such hostility to quantified hazard analysis remains in the oil industry, proponents of hazard analysis

should emphasize the value of qualitative analysis as a design tool. The introduction of these methods together with other developments will in time lead to an acceptance of quantitative techniques.

APPENDIX A

LIST OF ABREVIATIONS.

API   American Petroleum Institute

AS   Air Supply

ASH   Gas Detector

ATMOS.   Atmosphere

BL   Base Line

BNOC   British National Oil Corporation (now Britoil)

BP   British Petroleum Plc.

BV   Breather Valve

BW   Butt Weld

CCA   Cause Consequence Analysis.

CCC   Cause Consequence Charts.

C.INS   Cold Insulation

CW   Cooling Water

DG   Draft Gauge

DP   Dew Protection

ESS   Emergency Shutdown System

ETA   Event Tree Analysis

FC   Fail Closed

FDD   Functional Dependency Diagram

FDT	Fractional Dead Time
FMEA	Failure Mode And Effect Analysis
FO	Fail Open
FSV	Flow Safety Valve
FTA	Fault Tree Analysis
FTET	Fault Tree Event Tree
HAZOP	Hazard And Operability Study
HCV	Hand Control Valve
HH	Very High
H.L	High And Low
HSS	High Signal Selector
H.INS	Hot Insulation
ICI	Imperial Chemical Industries
IFAL	Instantaneous Fractional Annual Loss
LAH	High Level Alarm
LAHH	Extra High Level Alarm
LAL	Low Level Alarm
LALL	Extra Low Level Alarm
LCV	Level Control Valve
LGR	Level Glass Reflex
LGT	Level Glass Transparent
LI	Level Indicator
LL	Very Low
LSH	High Level Switch
LSHH	Extra High Level Switch
LSL	Low Level Switch

LSLL	Extra Low Level Switch
LSS	Low Signal Selector
LT	Level Transmitter

MANU.	Manual
MAX.	Maximum
MCR	Main Control Room
MFR.	Manufacturer
MIN.	Minimum
MISC.	Miscellaneous

NC	Normal Close
NFPA	National Fire Protection Association (USA)
NL	Normal Level
NRV	None Return Valve (also called FSV)

OPEC	Organisation Of Petroleum Exporting Countries

PAH	High Pressure Alarm
PAHH	Extra high Pressure Alarm
PAL	Low Pressure Alarm
PALL	Extra Low Pressure Alarm
PB	Push Button
PCV	Pressure Control Valve
PDCV	Differencial Pressure Control Valve
PDIC	Differencial Pressure Indicator And Controller
PDR	Differencial Pressure Recorder
PG	Pressure Gauge
PI	Pressure Indicator

PIC	Pressure Indicator And Controller
PP	Personnel Protection
PSH	High Pressure Switch
PSHH	Extra High Pressure Switch
PSL	Low Pressure Switch
PSLL	Extra Low Pressure Switch
PSV	Pressure Safety Valve
PSX	Pressure Switch
PT	Pressure Transmitter
P&ID	Piping And Instrumentation Diagrams
RL	Running Lamp

SAC	Safety Analysis Checklist
SAFE	Safety Analysis Function Evaluation Chart
SAT	Safety Analysis Table
SR	Split Range
SW	Switch

TLV	Threshold Limit Value
TW	Thermo Well

UCL	Unit Control Logic

VB	Vortex Breaker

XV	Shutdown Valve

APPENDIX B.1

PLANT DESCRIPTION

1.INTRODUCTION.

The Module Processing Plant (MPP) has been designed for the recovery of heavy hydrocarbons (condensates and LPG) from the raw gas coming from Hassi R'Mel gas field and producing treated gas (sale gas or reinjection gas).

The MPP is composed of three trains of treatment. They all have the same process equipment and the same daily production capacity of 60*10E6 Sm3 of treated gas per day (S stands for Standard, meaning 15'C/ bar absolute).

The liquid hydrocarbons recovered in the high pressure separation sections are separated into LPG and condensates in the fractioning section and then piped to central storage and transfer facilities (CSTF).

2.RAW GAS AND PRODUCTS SPECIFICATIONS.

2.1 Inlet Gas Specifications.

This plant has been designed to process a raw gas with the following specifications:

i) Composition.

Component	% Mol
N2	5.56
CO2	0.20
CH4	78.36
C2H6	7.42
C3H8	2.88
i-C4H10	0.62
n-C4H10	1.10
i-C5H12	0.36
n-C5H12	0.48
C6H14	0.59
C7H16	0.56
C8H18	0.45
C9H20	0.37
C10H22	0.27
C11H24	0.21
C12+	0.57
Total	100.00

ii) Water Content.

Saturated at 310 barG and 90°C

iii) Temperature.

Min: 45°C (Winter operation)

Max: 65°C (Normal operation)

iv)Pressure.

       Min: 100 bars G

       Max: 140 bars G

The actual flow rate of raw gas to the plant has not been stated precisely. However, the plant was designed to process 64.9*10E6 Sm3/day of raw material which will give the products listed in subsection 2.2

2.2 Products Specifications.

Under normal operating conditions the products will have the following specifications:

i)Sale Gas

    Composition.

Component	% Mol
N2	5.91
CO2	0.21
CH4	83.26
C2H6	7.90
C3H8	1.96
i-C4H10	0.26
n-C4H10	0.35
C5+	0.15
Total	100.00

Dew point:	-6°C (max) at 80.5 bars G
Water content:	50 vol.ppm (max)
Calorific value:	9350 Kcal/m3 (min)
	9450 Kcal/m3 (max)
	(evaluated at 15°C, 1bar A)
C5+ content:	0.5% mol (max)
Temperature:	60°C (max)
Pressure:	72 bars A

ii)LPG

| C2- content: | 3% mol (max) |
| C5+ content: | 0.4% mol (max) |

iii)C5+ (condensates)

Reid vapour tension:10 psia (max)

3.PROCESS DESCRIPTION.

This process is characterised by the utilisation of
Turbo-expanders for the maximum liquid hydrocarbons
recovery. The main advantage in using a Turbo-expander is
that the expansion will be isentropic and the temperature
obtained will be lower than the one which is obtained if
an adiabatic expansion, through a Joule-Thomson Valve
(JTV), is performed. The turbine recovers energy from the
gas and uses it to drive a compressor which will
recompress the product gas to the sale gas pressure. This
means that with the Turbo-expander the high pressure gas
will be expanded to lower pressures than with a JTV.

The low temperature gas (-40´C)from the Turbo-expander is used to cool the raw gas. No external refrigeration system is needed.

The water contained in the raw gas causes hydrate formation at low temperature which could raise the losses by friction in the heat exchangers or plug the tubes or canalisations. To avoid this happening, a solution of mono-ethylene glycol is injected at those points of the process where there is a risk of hydrate formation (mainly heat exchangers).

3.1 High Pressure Separation Section.

3.1.1 Generalities.

In this section the raw gas is cooled in order to condense its heavy constituents and to improve its qualities. It first passes through the aerorefrigerant (E101), then the gas/gas heat exchangers and finally the Turbo-expander.

The treated gas goes to the transfer section after being compressed in the compressor side of the Turbo-expander (K101) to the tranfer line pressure and the liquid hydrocarbons are sent to the fractioning section where they are separated into LPG and condensates.

3.1.2 Fluid circulation in the process.

The distribution drum (D001) divides the raw gas (mixed phase) collected from the wells into three equal streams. The stream entering each train is first cooled in the aerorefrigerant (E101) to 48.9 ´C , then it goes to the admission separation drum where the condensed liquids and the water are separated from the gas. The water is sent to the blow down section through the flare separation drum (D404) and the separator SPI (S409).

The gas from the admission separation drum (D101) is first cooled to -6.7´C in the gas/gas exchangers (E102 and E103) and expanded through the Joule-Thomson Valve PRC-108, then it heads for the final high pressure separation drum (D102) where it is separated from the liquid condensates and the hydrated glycol solution. To avoid hydrates formation in the gas/gas heat exchangers (E102 and E103), a solution of glycol is injected in the gas stream. Having absorbed the water, the glycol solution, separated from the liquid hydrocarbons in the final high pressure separator is sent under pressure to the glycol regeneration section.

The gas leaving the final high pressure separator (D102) is isentropically expanded in a turbo-expander (K101) in order to lower its temperature. The liquid hydrocarbons produced by this expansion are separated from the gas in the medium pressure separator (D103).

Glycol solution is injected at the turbo-expander suction to avoid hydrate formation and to remove the maximum amount of water from the gas. The hydrated glycol solution is then separated from the liquid condensates in the medium pressure separator and sent under pressure to the glycol regeneration unit.

The gas passes through the shell side of the gas/gas heat exchangers where it cools down the incoming raw gas, then heads for the transfer section as sale gas.

The liquid hydrocabons collected in the admission separator circulate towards the rich condensate separator (D105) where the light constituents are rectified (evaporated).The stabilised liquid will constitute the bottom feed of the de-ethanizer (C101).

The liquid hydrocarbons collected in the final high pressure and the medium pressure separators (D102 and D103) are sent the low pressure separator where the light constituents are rectified. The stabilized liquid will constitute the top feed of the de-ethanizer (C101).

The gas from the low pressure separator (D104) and the gas from the de-ethanizer reflux drum are mixed and sent to the shell side of the gas/gas heat exchanger (E103). Then joined by the gas from the rich condensate separator (D105), they head for the recompression section where

their pressure is raised to the sale gas pressure.

The gas from the rich condensate separator (D105) being at a relatively high temperature contains a large quantity of water and, therefore, will influence the gas water content if reinjected in the gas stream. For this reason it is recommended to use it as fuel gas.

3.1.3 Main control points.

The following variables constitute the main control points in this section:

a)The outlet gas temperature in the admission aero-refrigerant (E101):
This temperature is maintained at 48.9°C by the TIC-101 which varies the angle of the fan blades to control the amount of air flowing through the heat exchanger.

b)The pressure in the final high pressure separator (D102):
This pressure is maintained at a constant level by the PRC-108 since a pressure of 100 barG at the suction of the turbo-expander is required for a maximum liquid recovery.

c)The oulet temperature of the gas at the gas/gas heat exchangers (E102 and E103):

The outlet tube side temperatures are regulated by varying the shell side gas flow rate in response to the signals emitted by feedback from TRC-102 or TIC-124.

d)Raw gas flow rate.

It is the FRC-101 (Flow Recorder and Controller), which by varying the blades angle of the turbo-expander regulates the raw gas flow rate.

e)Pressure in the rich condensate separator (D105):

PIC-116 maintains this pressure at 32.4 barG.

f)Pressure in the low pressure separator (D104):

PIC-115 keeps this pressure at a constant value of 34.2 barG.

In order to protect the equipment from abnormal occurences, the high separation section has been fitted with pressure and temperature controllers calibrated at values that can not be changed:

-PICA-139 (admission separator D101):

Closes when the pressure reaches 150 kg/cm2.

-PIC-101 (admission separator D101):

Open when the pressure reaches 153 kg/cm2.

-PIC-114 (admission separator D101):

Open when the pressure reaches 153 kg/cm2.

-TIC-124 (gas/gas heat-exchangers E102):

Open shell side by-pass if the temperature is

lower than -40´C even if it receives the signal
"close" from the TRC-102 (tube side temperature
regulator). That will maintain the temperature
at a constant level.

3.2 Distillation Section.

3.2.1 Generalities.

The liquid hydrocarbons recovered in the high pressure
separation section are split up into LPG and condensate in
the debutanizer (C102) after being relieved from their
light constituents in the de-ethanizer (C101). The latter
consists of 28 trap trays, 12 in the upper section and 16
in the lower section separated by an accumulation tray. To
avoid hydrates formation in the column a glycol solution
is injected in the reflux line. The mixture collected in
the accumulation tray is sent to the hydrocarbons/glycol
separator where a total separation occurs. The liquid
hydrocarbons are then pumped back to the column under the
accumulation tray and the glycol solution send to the
glycol regeneration unit.

The feed enters the column at the 5th and the 21st
trays. The 6th and the 19th are designed to be used as
feed trays if the gas composion is to vary. The
debutanizer consists of 32 trap trays of which the 21st is
the feed tray.

3.2.2 Fluid circulation in the process.

i)De-ethanizer:

The liquid hydrocarbons from the low pressure separator (D104) is pre-heated in the reflux heat exchanger (E106) then feeds the column at the 5th tray.

The liquid hydrocabons from the rich condensate separator (D105) are pre-heated in the feed heat exchanger (E104) and enter the column at the 21st tray.

The gas leaving the column from the top passes through the reflux heat exchanger (E106), is partially condensed (T=-23'C) and then goes to the reflux drum where it is separated from the liquids. To avoid hydrate formation in the E106 and to remove the maximum amount of water, glycol solution is injected in the gas stream when it leaves the column.

The gas heads then for the recompression section while the pressure in the reflux drum (D107) is regulated by the PIC-123.

The hydrated glycol solution is sent under pressure to the glycol regeneration unit while the liquid hydrocarbons are pumped back, under flow control (FIC-127), to the first tray of the column by the P103. To avoid hydrate formation in the top section of the column, glycol solution is injected down stream from the

pumps discharge pipe.

The liquid descending from the top trays is collected in the accumulation tray from where it flows out under gravity to the hydrocarbons/glycol separator (D106). The hydrocarbons are separated from the glycol and pumped back to the column by the P102 under the accumulation tray. The glycol solution is sent under pressure to the regeneration unit.

A fraction of the liquid accumulated in the bottom section of the column is pressurised by the P101 and sent to the reboiler under flow control (FIC-136). The reboiler (H101) heats up the liquid to a temperature of about 240°C and vaporises it to 50% by weight. This mixture heads back to the bottom of the de-ethanizer. The remaining part of liquid will constitute the feed of the debutanizer. It flows away under the action of FIC-128 and LIC-117 (in cascade).

ii)Debutanizer.

The gas from the top is totally liquified in the reflux aero-refrigerant (E108) before entering the reflux accumulator drum (D108). A fraction of this liquid is pumped back to the first tray at the top of the column, by the P105, as reflux and its flow rate is controlled by the FRC-143. The remaining liquid is sent product LPG to the storage and transfer section.

If the LPG does not conform to the specifications (analysed in the gaseous phase by the chromatographe AR-101), the LIC-128 AV closes and the LIC-128 BV open so that the LPG will be sent to the off-spec storage sphere.

A fraction of the bottom product is sent under pressure (P104) to the reboiler. The flow rate is controled by the FIC-144. The liquid hydrocarbons after being heated to a temperature of 263´C and partially vaporised (50% wt) in the furnace are sent back to the bottom part of the column.

The remaining fraction is extracted as condensates, under level control by the LIC-126, and sent to the storage section after being cooled down to 48.9´C in the heat exchanger (E104) and the aero-refrigerant (E107).

3.2.3 Main control points.

The following variables constitute the main control points in this section:

i) De-ethanizer (C101).
    a)Pressure:
The pressure in the de-ethanizer is maintained at a value of 26.4 kg/cm2G by the PIC-123 which regulate the amount of vapours from the reflux drum (D107).

b)Top feed temperature:

The top feed temperature is a function of the amount of heat transfer occuring in the reflux heat exchanger (E106). The quantity of heat transfer is controled by the heat exchanger by-pass valve LIC-123V on the tube side which responds to the signal from the LIC-123. In other words, when the level in the reflux drum (D107) is low, the LIC-123 send the signal to close the LIC-123V. As a result the amount of heat transfer will rise leading to a rise in level up to the required value.

c)Bottom feed temperature:

The bottom feed temperature is conditioned by the amount of heat transferred in the bottom feed heat exchanger. This temperature is controlled by the TIC-104 which acts on the shell side by-pass. The prescribed value is maintained by opening or closing this valve.

d)Reflux flow rate:

The FIC-127 at the discharge of the pumps P103 regulate the reflux flow rate.

e)Flow rate to the reboiler:

The flow of liquids to the reboiler is regulated by the FIC-136 positioned at the discharge of the reboiler pumps P101.

f)Reboiler outlet temperature:

This temperature is controled by regulating the fuel gas flow rate with TRC-109.

ii)Debutanizer.

a)Pressure:

The following drawings explain the pressure regulation in the debutanizer.

Partial condensation in the D108.
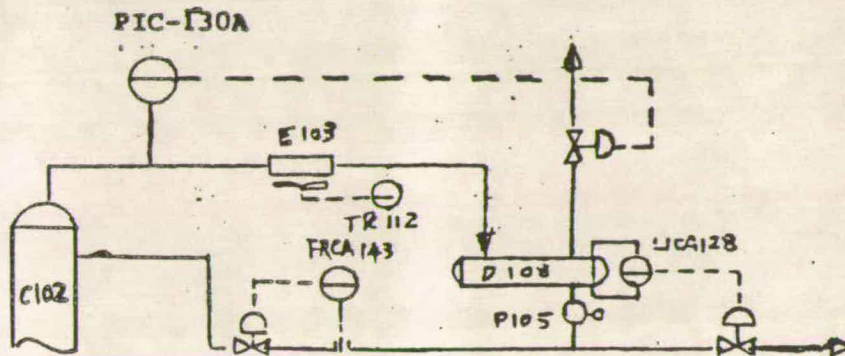
Total condensation in the D108.
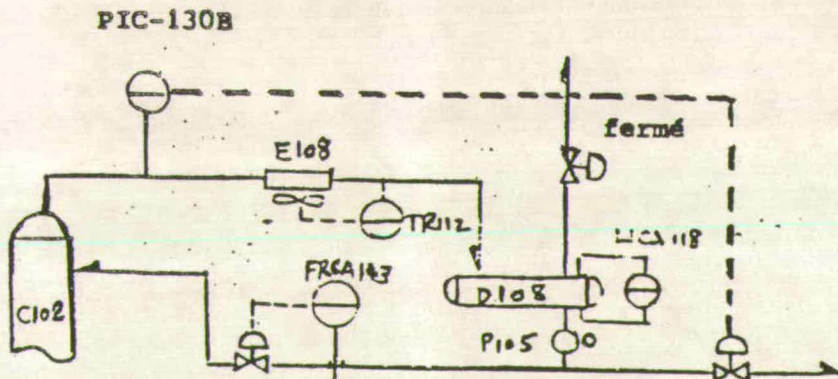
b)Reflux flow rate:

The FIC-143 at the discharge of the pumps P105

regulate the reflux flow rate.

c)Flow rate to the reboiler:

The flow of liquids to the reboiler is regulated by the FIC-144 positioned on the discharge line of the reboiler pumps P104.

d)Reboiler outlet temperature:

TRC-114 regulates the reboiler outlet temperature by acting on the fuel gas flow rate.

4. REMAINING SECTIONS.

In all process plants, beside the main production unit or units, there are the secondary or support unit. A brief description of these units which constitute the MPP 4 is given below:

4.1 Condensats degasification and LPG storage and transfer section.

Two spheres and three storage tanks, with a storage capacity of 48 hours production (LPG and condensates), are provided all with their support equipment (pumps, compressors etc.).

4.2 Glycol regeneration units.

Two glycol regeneration units are installed in the plant. On normal operation, one of the two is on

operating mode while the other is on standby. A unit
'storage of glycol' and a unit 'glycol injection pumps'
are respectively the upstream and the downstream units
with regard to the regeneration units.

4.3 Low pressure gases recompression section.

A compression system has been designed to recompress
all the low pressure gases produced in the low
temperature and pressure separation sections of the
trains, and the distillation sections of the trains.
This unit comprise two centrifugale compressors driven
by a gas turbines and with a daily compression capacity
of 5,000,000 Sm3 each. Under normal operating
conditions, one is on operation while the other is
maintained on standby.

4.5 Combustible gas unit.

The gases recuperated from the rich condensate
separation drum D105 have a high water content which
prevent from processing them with the gases from the
other stages of separation. The best way to use them is
as fuel gas. They are collected in the fuel gas unit and
sent back to different parts of the process.

4.7 Utilities.

The utilities are composed by:

-A water treatment section which provide the process with, cooling water (e.g. for pumps bearings), water for maintenance purposes and water for domestic use (showers, drink etc.).

-An air instrument and air service section which covers all the needs of the process in this area.

-Inert gas is also produced onsite in the inerte gas section.

-The electrical power section composed by two sub-stations which contain the electrical transformers and equipment switches.

-A flare and dumping sections with three high pressure, a medium pressure and a low pressure relief flares and a burn pit to burn eventually the liquid hydrocarbons.

APPENDIX B2.

LIST OF DIAGRAMS.

1. General Plot Plan.

2. Operational Flow Diagram.

3. Piping Symbols.

4. P&IDs for "Gas Admission" Section.

5. P&IDs for "High Pressure Separation" Section.

6. P&IDs for "Compressor Expander" Section.

7. P&IDs for "Low Pressure Separation" Section.

8. P&IDs for "Deethanizer" Section 1.

9. P&IDs for "Deethanizer" Section 2.

10. P&IDs for "Debutanizer" Section.

11. P&IDs for "Glycol Regeneration" Section.

General Plot Plan for Module Processing Plant IV — No. IV Module Processing Plant (Plan d'Implantation Général)

Operational Flow Diagram of Module Processing Plant

Symbol	English	French
	GATE VALVE	VANNE A PASSAGE DIRECT
	GLOBE VALVE	ROBINET A SOUPAPE
	CHECK VALVE	CLAPET DE RETENUE
	BUTTERFLY VALVE	VANNE A PAPILLON
	BALL TYPE COCK VALVE	ROBINET A BOISSEAU A BILLE
	NEEDLE VALVE	VANNE A POINTEAU
	ANGLE VALVE	VANNE D'ANGLE
	THREE WAY VALVE	VANNE A TROIS VOIES
	RELIEF OR SAFETY VALVE	SOUPAPE DE SURETE
	METERING COCK VALVE	VANNE MESURANTE A BOISSEAU
	LINE SIZE CHANGE (REDUCER)	EVASEMENT (REDUCTION)
	FLANGE CONNECTION	RACCORD A BRIDE
	HOSE CONNECTION	RACCORD POUR (TUYAU FLEXIBLE)
	NOZZLE WITH BLIND FLANGE	TUBULURE A BRIDE PLEINE
	RESISTANCE TEMPERATURE DETECTOR	DETECTEUR DE TEMPERATURE A RESISTANCE
	Y OR T TYPE STRAINER	FILTRE EN Y OU T
	CONICAL STRAINER	FILTRE CONIQUE
	LINE TRACE (ELECTRIC HEATER)	RECHAUFFAGE ELECTRIQUE
	OPEN DRAIN SYSTEM	SYSTEME DE DRAINAGE OUVERT
	RUPTURE DISC	DISQUE DE RUPTURE
	RESTRICTION ORIFICE	ORIFICE DE RESTRICTION
	CONTINUATION OF DRAWING	CONTINUATION DU PLAN
	FLOW ELEMENT – ORIFICE FLANGE	BRANCHEMENT POUR DEBITMETRE - BRIDE A ORIFICE
	FLOW ELEMENT – VENTURI	BRANCHEMENT POUR DEBITMETRE - VENTURI
	FLOW ELEMENT VOLUMETRIC	DEBITMETRE VOLUMETRIQUE
	FLOW ELEMENT AREA TYPE	ROTAMETRE
	FLOW ELEMENT (PITOT TUBE OR ANNULAR)	BRANCHEMENT D'UN TUBE DE PITOT OU ANNULAIRE
	SIGHT GLASS	VITRE DE REGARD
	GLYCOL DRAIN	VIDANGE DE GLYCOL
	PURGE CONNECTION	RACCORD POUR PURGE
	DIAPHRAGM OPERATED VALVE	SOUPAPE A DIAPHRAGME
	MOTOR OPERATED VALVE	SOUPAPE COMMANDEE PAR MOTEUR
	AIR MOTOR OPERATED VALVE	SOUPAPE COMMANDEE PAR MOTEUR A AIR
	SOLENOID OPERATED VALVE [1]	SOUPAPE A COMMANDE PAR SOLENOIDE [1]

Symbol	English	
	AIR CYLINDER OPERATED VALVE	S
	CONTROL VALVE WITH LIMIT SWITCH	V
	CONTROL VALVE WITH VALVE POSITION TRANSMITTER	V F
	MANUAL OPEN-CLOSE (SIDE HANDLE)	V
	MANUAL OPEN-CLOSE (TOP HANDLE)	V
	PRESSURE REGULATOR (SELF CONTAINED)	F
	PRESSURE REDUCING REGULATOR (DIRECT CONNECTED)	F
	DIFFERENTIAL PRESSURE REGULATOR OR DOUBLE DIAPHRAGM VALVE	F S
	FAILURE ACTION	D
	SEQUENCE CONTROL FUNCTION OR COMPUTING FUNCTION	F F
	LOCALLY MOUNTED FUNCTION	F
	PANEL MOUNTED INSTRUMENT AT MAIN CONTROL ROOM	I C
	PANEL MOUNTED INSTRUMENT AT UTILITY CONTROL ROOM	I C
	INSTRUMENT ON LOCAL PANEL	I
	INSTRUMENT TRANSMITTER	T
	PROCESS & UTILITY PIPING	T
	INSTRUMENT ELECTRICAL LEAD	C
	PNEUMATIC LINES (GAS OR AIR)	C
	INSTRUMENT CAPILLARY TUBING	T
	DRAIN TRAP	F
	FLOW ELEMENT TURBINE	D
	FLOW ELEMENT INTEGRAL ORIFICE	B
	SPECTACLE BLIND (NORMAL OPEN)	
	SPECTACLE BLIND (NORMAL CLOSE)	
	SAMPLE COOLER	I
	SPECIAL	
	CHOKE VALVE	V
	DIAPHRAGM VALVE	S

40-D001
BALLON DE DISTRIBUTION
(FLOW SPLITTER)
PRESS DE CAL = 248 Kg/cm2g
TEMP DE CAL = -28.8 / 76.6°C

H.P. TORCHE
622

MODULE IV
RESEAU COLLECTEUR DU GAZ
(GAS GATHERING SYSTEM)

H.P. TORCHE
626

(ELECTRIC HEATER)

SOURCE D'AIR INSTRUMENT
(INSTRUMENT)
(AIR SOURCE)
PANNE ELECTRIQUE
POWER FAILURE

D101 D101 D101

LL TRAIN STOP

22"-L001-F3

22"-L002-F3

22"-L003-F3

UZ-101

UZ-125 (UZ-125V TO CLOSE)
UZ-126 (UZ-126V TO CLOSE)

SIGNAL DE PIC 139
(SIGNAL FROM PIC 139)

DESSIN A1-002

DESSIN A1-002
TRAIN A

26-L019-F3   26-L019-F1

DO.01

1½-L216-F3

26-L020-F3   26-L020-F1   TRAIN B

36-L017-F3

26-L021-F3   26-L021-F1   TRAIN C

JONCTION DE LA LIAISON ALLANT ET
VENANT DU CIRCUIT DE SURCOMPRESSION
DU GAZ D'ALIMENTATION
(CONNECTION TO & FROM FEED)
(GAS BOOSTER SYSTEM)

1'-L016-F3

MISE EN ROUTE DU GAZ COMBUSTIBLE
(START UP FUEL GAS)

DESSIN A1-013

4-L015-F3

MPP I, MPP IV

4'-L014-D1
MISE EN ROUTE DU GAS COMBUTIBLE
(START UP FUEL GAS)

PIPE LINE WORK   MODULE
DESSIN NO. 75-A1-506

4'-P1118-6BAX

EXISTING | BY | EXISTING
         | JGC |

FOR CONSTRUCTION

La presente spécification est utilisée pour
construction à partir de la révision 6

FROZEN

DESSIN 0313.40-A1-001-B

Piping and Instrument Diagram of Module Processing Plant — Deethanizer Section-1

Piping and Instrument Diagram — Module Processing Plant, Low Pressure Separation Section

41/42/43 - D103 (C. INS)
SEPARATEUR DE MOYENNE PRESSION
(MEDIUM PRESSURE SEPARATOR)
PRESS. DE CAL = 91.4 Kg/cmG
TEMP. DE CAL = -45.5/93.3°C

41/42/43 - D104 (C. INS)
SEPARATEUR DE BASSE PRESSION
(COLD LOW PRESSURE SEPARATOR)
PRESS DE CAL = 37.7 Kg/cmG
TEMP. DE CAL = -53.0/93.3°C

41/42/43 - M101
MELANGEUR EN
LIGNE DE GLYCOL
(LINE MIXER)

41/42/43 - D105
SEPARATEUR DE CONDENSAT RICHE
(RICH CONDENSATE SEPARATOR)
PRESS DE CAL = 37.7 Kg/cmG
TEMP. DE CAL = -28.8/93.3°C

S103 A/B
FILTRE DE GLYCOL
(NO.3 GLYCOL INJECTION FILTER)

173

FOR CONSTRUCTION

FROZEN

DESSIN 0313.40-A1-004-B

This is a piping and instrument diagram (P&ID). The drawing is a full-page engineering schematic titled "PIPING AND INSTRUMENT DIAGRAM OF MODULE PROCESSING PLANT EXPANDER COMPRESSOR SECTION" prepared by JGC CORPORATION for SONATRACH, Hassi-R'Mel natural gas treatment plant.

Piping and Instrument Diagram (P&ID) — Module Processing Plant, Deethanizer Section.

Equipment labels:

- 41.42.43-S105 A/B — FILTRES DE GLYCOL (NO.5 GLYCOL INJECTION FILTER)
- 41.42.43-E 106 (C INS) — ECHANGEUR DE REFLUX DU DE-ETHANISEUR (DEETHANIZER REFLUX EXCHANGER) CALANDRE TUBE — PRESS DE CAL = 34.1 / 10.6 Kg/cm²G — TEMP DE CAL = -455/93.3 / -455/93.3 °C
- 41.42.43-P 103 A/B (C INS) — POMPE DE REFLUX DU DE-ETHANISEUR (DEETHANIZER REFLUX PUMP)
- 41.42.43-D 107 (C INS) — ACCUMULATEUR DE REFLUX DU DE ETHANISEUR (DEETHANIZER REFLUX ACCUMULATOR) PRESS DE CAL = 30.6 Kg/cm²G — TEMP DE CAL = -45.5/93.3 °C — HP TORCHE
- 41.42.43-H 101 — REBOUILLEUR DU DE-ETHANISEUR (DEETHANIZER REBOILER)
- 41.42.43-K 102 — SOUFFLANTE A AIR (PURGE AIR BLOWER)
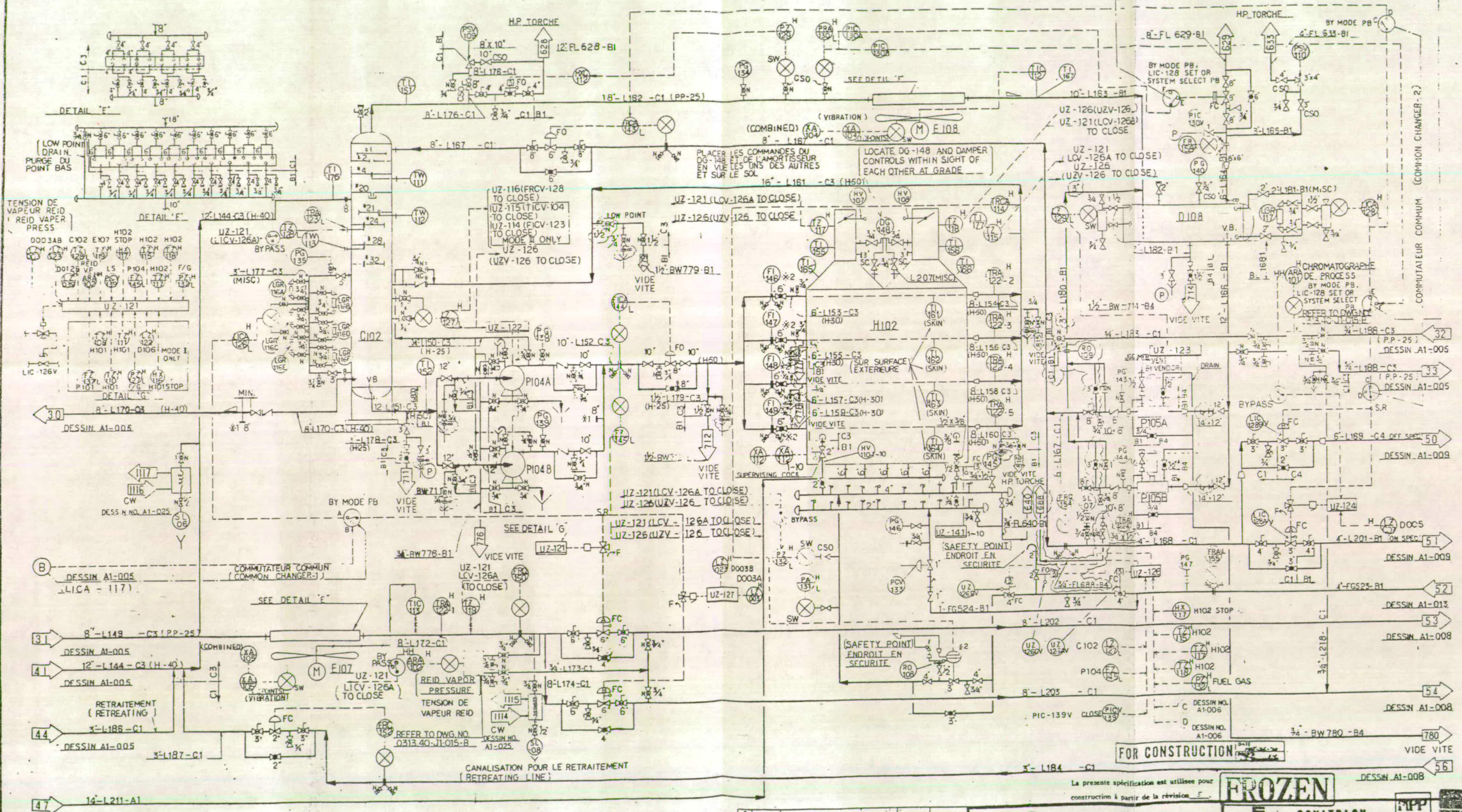
NOTE
(*1 WITH MINIMUM STOPPER)
AVEC DISPOSITIF EMPECHANT LA FERMETURE COMPLETE

FOR CONSTRUCTION

FROZEN

JGC CORPORATION
SONATRACH — DIRECTION PRODUCTION
MPP IV
HASSI-R'MEL: TRAITEMENT DE GAZ NATUREL (MODULE IV)
PIPING AND INSTRUMENT DIAGRAM OF MODULE PROCESSING PLANT DEETHANIZER SECTION-2
DIAGRAMME DE TUYAUTERIES ET D'INSTRUMENTS POUR MPP
SECTION-2 DE-ETHANISEUR

DESSIN N° 0313.40-A1-006 -B A1

Piping and Instrument Diagram — Module Processing Plant, Debutanizer Section (JGC Corporation / SONATRACH, Hassi-R'Mel, Traitement de Gaz Naturel, Module IV)

DESSIN NO. 0313.40-A1-007-B A1

Equipment legend (top):

45/46-E301A-F (H.INS)
ÉCHANGEUR DE CHALEUR DE GLYCOL
(GLYCOL HEAT EXCHANGER)
CALANDRE / TUBE
PRESS. DE CAL. 90 KG/CM²G / 98 KG/CM²G
TEMP. DE CAL. 160°C / 140°C

45/46-D301 (H.INS)
SEPARATEUR D'HUILE
(OIL SEPARATOR)
PRESS. DE CAL. 5.8 KG/CM²G
TEMP. DE CAL. 135°C

45/46-S302A.B (H.INS)
FILTRE DE GLYCOL
(GLYCOL FILTER)
PRESS. DE CAL. 5.8 KG/CM²G
TEMP. DE CAL. 135°C

45/46-C301 (H.INS)
COLONNE DE DISTILLATION
(GLYCOL STILL COLUMN)
PRESS. DE CAL. 3.5 KG/CM²G
TEMP. DE CAL. 160°C

45/46-P301A.B
POMPE DE GLYCOL FOND DE TOUR
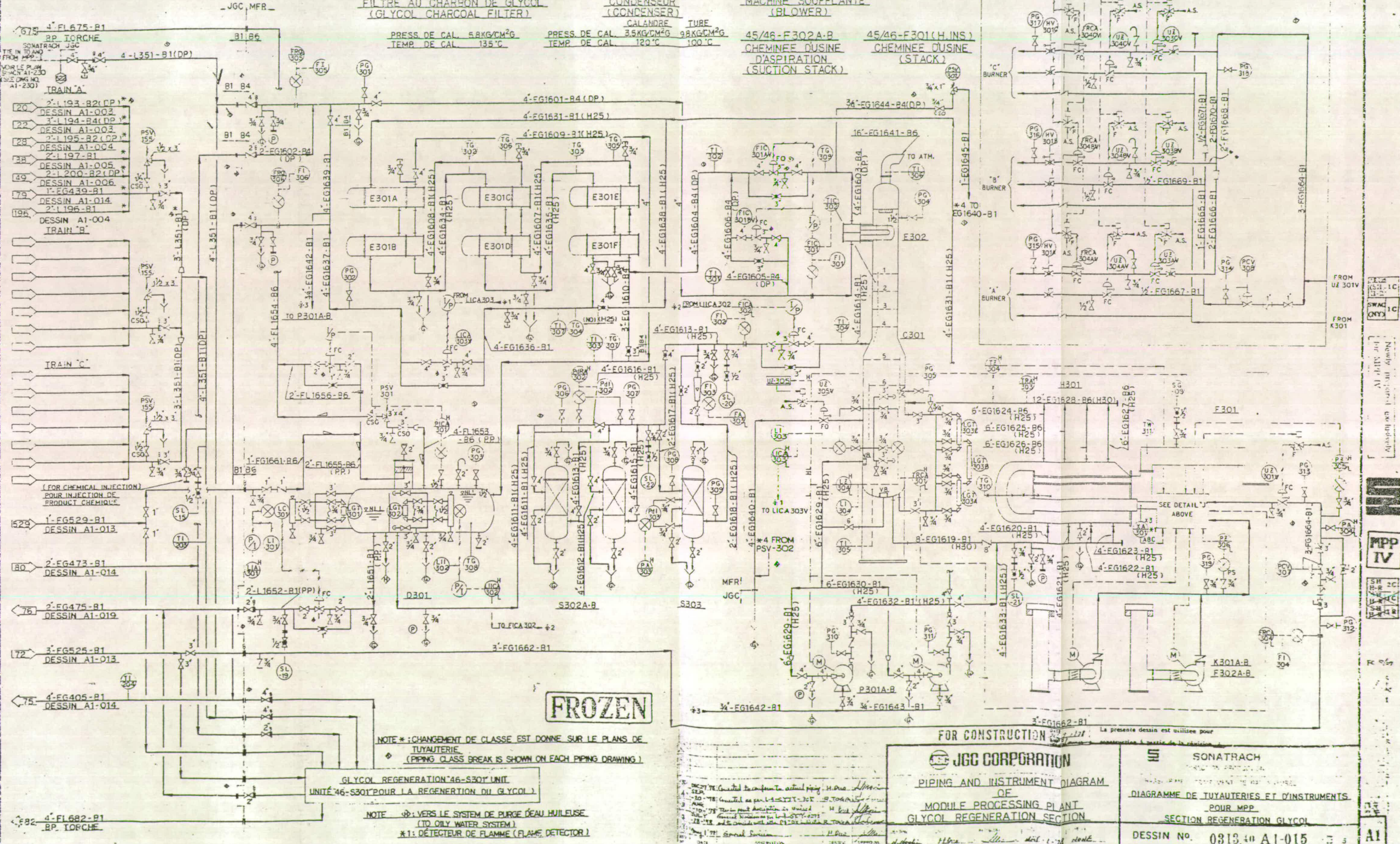(GLYCOL BOTTOM PUMP)

45/46-H301 (H.INS)
REBOUILLEUR
(REBOILER)
CALANDRE / TUBE
PRESS. DE CAL. 3.5 KG/CM²G / —
TEMP. DE CAL. 191°C / 200°C

45/46-S303 (H.INS)
FILTRE AU CHARBON DE GLYCOL
(GLYCOL CHARCOAL FILTER)
PRESS. DE CAL. 5.8 KG/CM²G
TEMP. DE CAL. 135°C

45/46-E302
CONDENSEUR
(CONDENSER)
CALANDRE / TUBE
PRESS. DE CAL. 3.5 KG/CM²G / 98 KG/CM²G
TEMP. DE CAL. 120°C / 100°C

45/46-K301A.B
MACHINE SOUFFLANTE
(BLOWER)

45/46-F302A.B
CHEMINEE D'USINE D'ASPIRATION
(SUCTION STACK)

45/46-F301 (H.INS)
CHEMINEE D'USINE
(STACK)

DETAIL "J"
BURNER CONTROL UNIT

FROZEN

NOTE * : CHANGEMENT DE CLASSE EST DONNE SUR LE PLANS DE TUYAUTERIE
◇ (PIPING CLASS BREAK IS SHOWN ON EACH PIPING DRAWING)

GLYCOL REGENERATION "46-S301" UNIT
UNITÉ 46-S301 POUR LA REGENERTION DU GLYCOL

NOTE ◇3 : VERS LE SYSTEM DE PURGE D'EAU HUILEUSE
(TO OILY WATER SYSTEM)
* 1 : DÉTECTEUR DE FLAMME (FLAME DETECTOR)

FOR CONSTRUCTION

JGC CORPORATION

SONATRACH

PIPING AND INSTRUMENT DIAGRAM
OF
MODULE PROCESSING PLANT
GLYCOL REGENERATION SECTION

DIAGRAMME DE TUYAUTERIES ET D'INSTRUMENTS
POUR MPP
SECTION REGENERATION GLYCOL

DESSIN NO. 0313.40 A1-015

MPP IV

ÉCHANGEUR DE CHALEUR DE GLYCOL
(GLYCOL HAET EXCHANGER)

CALANDRE	TUBE
PRESS. DE CAL. 9.0 KG/CM²G	9.8 KG/CM²G
TEMP. DE CAL. 160°C	140°C

SÉPARATEUR D'HUILE
(OIL SEPARATOR)
PRESS. DE CAL. 5.8 KG/CM²G
TEMP. DE CAL. 135°C

FILTRE DE GLYCOL
(GLYCOL FILTER)
PRESS. DE CAL. 5.8 KG/CM²G
TEMP. DE CAL. 135°C

COLONNE DE DISTILLATION
(GLYCOL STILL COLUMN)
PRESS. DE CAL. 3.5 KG/CM²G
TEMP. DE CAL. 160°C

POMPE DE GLYCOL
FOND DE TOUR
(GLYCOL BOTTOM PUMP)

REBOUILLEUR
(REBOILER)

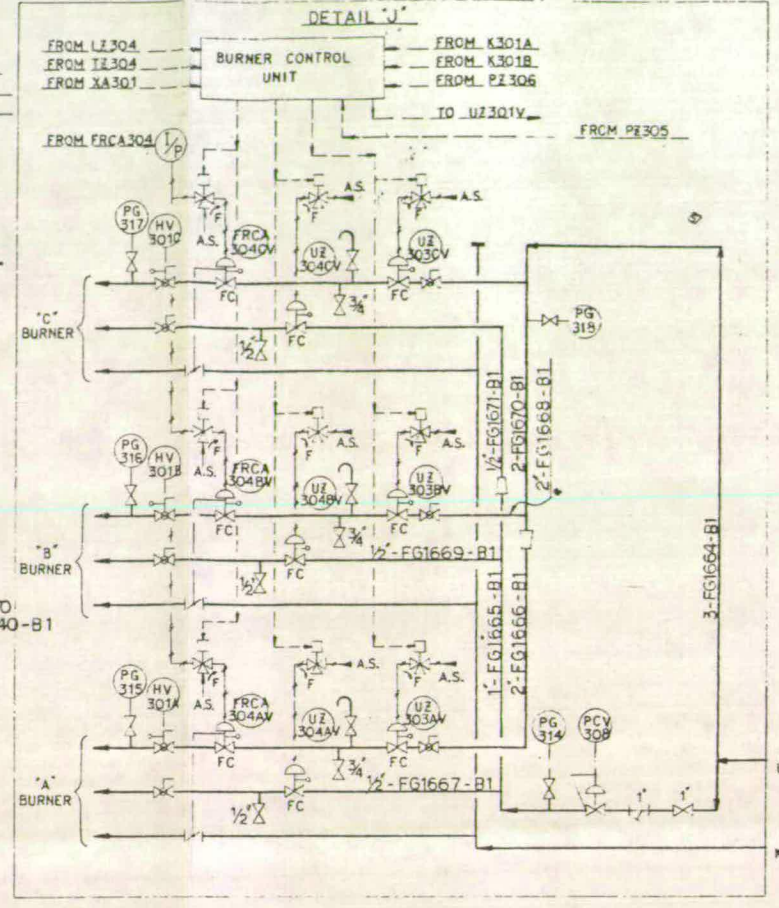| CALANDRE	TUBE
PRESS. DE CAL. 3.5 KG/CM²G	—
TEMP. DE CAL. 191°C	200°C

45/46-S303 (H.INS)
FILTRE AU CHARBON DE GLYCOL
(GLYCOL CHARCOAL FILTER)
PRESS. DE CAL. 5.8 KG/CM²G
TEMP. DE CAL. 135°C

45/46-E302
CONDENSEUR
(CONDENSER)

CALANDRE	TUBE
PRESS. DE CAL. 3.5 KG/CM²G	9.8 KG/CM²G
TEMP. DE CAL. 120°C	100°C

45/46-K301A·B
MACHINE SOUFFLANTE
(BLOWER)

45/46-F302A·B
CHEMINÉE D'USINE
D'ASPIRATION
(SUCTION STACK)

45/46-F301 (H.INS)
CHEMINÉE D'USINE
(STACK)

DETAIL "J"
BURNER CONTROL UNIT

FROM UZ304
FROM TZ304
FROM XA303
FROM K301A
FROM K301B
FROM PZ306
TO UZ301V
FROM PZ305
FROM FRCA304

"C" BURNER
"B" BURNER
"A" BURNER

TRAIN "A"
TRAIN "B"
TRAIN "C"

(FOR CHEMICAL INJECTION)
POUR INJECTION DE
PRODUIT CHEMIQUE

FROZEN

FOR CONSTRUCTION

NOTE * : CHANGEMENT DE CLASSE EST DONNÉ SUR LE PLANS DE
TUYAUTERIE.
(PIPING CLASS BREAK IS SHOWN ON EACH PIPING DRAWING)

GLYCOL REGENERATION "46-S301" UNIT
UNITÉ "46-S301" POUR LA REGENERTION DU GLYCOL

NOTE ⌖ : VERS LE SYSTEM DE PURGE D'EAU HUILEUSE
(TO OILY WATER SYSTEM)
*1 : DÉTECTEUR DE FLAMME (FLAME DETECTOR)

JGC CORPORATION

PIPING AND INSTRUMENT DIAGRAM
OF
MODULE PROCESSING PLANT
GLYCOL REGENERATION SECTION

SONATRACH

DIAGRAMME DE TUYAUTERIES ET D'INSTRUMENTS
POUR MPP
SECTION REGENERATION GLYCOL

DESSIN NO. 0313.40 A1-015

A1

MPP IV

APPENDIX C.1

REVIEW OF THE MOND FIRE AND EXPLOSION INDEX.

1.INTRODUCTION.

The Mond Fire and Explosion Index has been developed by Dr D.J. LEWIS formerly ICI Mond Division. The idea for a point scheme to be used in the petrochemical industry originated in Factory Mutual Inc. The first index to be published was that developed by the Dow corporation (1), and it is from this method that the Mond Index was developed.

1.1 Philosophy Of The Mond Index.

The Mond Index is a rapid hazard assessment method for use on chemical plant or in plant design. The philosophy of the Mond Index is to assign points to the aspect of the process which contribute to the hazard and safety of the plant. It produces a numerical ranking for each section of the plant based upon the properties of materials present, quantity, operating conditions and type of process. Scales are provided to convert the rankings into qualitative descriptions of the hazard potential of each unit. The Index is primarily concerned with fire and explosion problems. Toxicity is considered only as a possible

complicating factor. The method gives credits for plant safety features associated with both hardware and the software.

The index has been designed to suit the needs of ICI Mond Division, who manufacture a wide range of chemicals, and their process plant is not enclosed. LEWIS has extended the method to cover storage areas as well as chemical plants, and the method has been used successfully to calculate the plant spacing requirements (3).

2. GENERAL DESCRIPTION OF THE MOND INDEX.

Initially the plant is divided into a number of units which are then assessed individually. Each unit is assessed by a three-stage procedure. Page 1 of the standard form (a set of blank calculation sheets has been included at the end of this chapter) provides space to record the location of the plant and the particular unit being assessed, the material contained in the unit and any other relevant information in addition to the process operating conditions of temperature and pressure.

The first stage considers the unit in a basic form with the minimum of controls required for normal operation. This gives a worst case assessment. To begin this stage the dominant hazardous material is identified and its material factor calculated. The material factor is a measure of the energy content per unit weight of material

present and provides a numerical base for the indices. However, this base will be modified by many other considerations, such as:

Any special material properties which may enhance the potential hazard

The effects of the type of process

The effects of the process conditions

The quantities involved

Relevant plant layout features, and

Material toxicity.

Each of these sections is sub-divided to cover the individual aspects for which penalty factors may be assigned.

After all the factors have been allocated the indices are calculated and their categories recorded. It should be noted that these represent the worst case assessment.

The second stage in the assessment of the unit is a review of the factors contributing to the initial indices. This gives an opportunity to reconsider any of the penalties assigned earlier or to seek more precise data about materials in use or about plant conditions. The review is unnecessary if, for example, the conditions and materials were well known from the start or if the rating obtained is satisfactory even though pessimistic data where used.

The third stage is the offsetting. This considers those

features which, if correctly maintained, will help to reduce either the magnitude of an incident or will diminish the likelihood of an incident starting. Such features are assigned values of less than one. Formulae are provided to allow reduced values of the indices to be calculated. This final, lower assessment represents:

"The hazard potential of the unit in the condition as studied with all the safety systems and other preventive measures operational in the designed mode." (4).

3. INDEX CALCULATION PROCEDURE.

This description of the procedure will follow the aproach specified in the technical manual (2). In order to simplify the calculation procedure I have developed a computer program which is shown at the end of this Appendix.

3.1 Division Of A Plant Into Units.

The boundaries of the unit to be studied must be defined, and are best identified by the valves which isolate the unit from upstream and downstream processes. All the pipework between the isolation valves is considered in the review of the unit.

Apart from being physically separated from the neighbouring units (or potentially separable) a unit is

also likely to differ in the nature of the operation carried out, the materials it contains or the operating conditions in the unit.

3.2 Selection Of The Dominant Material.

The dominant (key) material is that compound or mixture in the unit which, due to its inherent properties and the quantity present, provides the greatest potential for an energy release by combustion, explosion or exothermic reaction.

3.3 Calculation Of The Material Factor: B

The first step in a Mond index assessment is the calculation of the material factor for the key material present in the unit. The material factor is a quantitative measure of the energy release potential of the key material by fire or explosion. It is based on the properties and possible reactions of the key material in its normal state at ambient temperature. In most instances it is combustion in air that gives the greatest energy release and hence the highest value of B.

3.4 Special Material Hazards: M

This section takes into account any special properties of the key material which may affect either the nature of an incident or the likelihood of its occurence. The

material is considered under the conditions normally existing within the unit; thus the factors assigned in this section may vary from unit to unit within one plant, even though the same material is involved.

3.5 General Process Hazards: P

The hazard potential of the process is dependent on the nature of the material that is being used, and on the way in which it is processed. This section takes account of the hazards that arise out of the type of operation being undertaken. Where the material is only changing physically,there is less hazard than where the material reacts with another substance.

3.6 Special Process Hazards: S

This section looks at specific characteristics of the process which enhance the degree of hazard. For example, the unit operating pressure and temperature are important factors to be considered, as are other more unusual hazards like the build up of an electrostatic charge in the material, the discharge of which may release sufficient energy to ignite a flammable mixture of material.

3.7 Quantity Hazards: Q

The degree of hazard resulting from processing a

material is dependent on the amount of material used in the process. A factor is allocated for the additional hazards associated with the use of large quantities of combustible, flammable, explosive or decomposable materials. This is related to the total amount of heat that can be released in an accident, given the heat of combustion of the material.

3.8 Layout Hazards: L

Various features of the design and layout of the unit being assessed can introduce additional hazards. Special attention is given to "Domino" or "Knock-on" effects which are related to the height of the unit, and the plant separation distances. For example, the potential effects of the collapse of a distillation column are greater, as are the effects of a running liquid fire which occurs at a high level and spread downwards through the plant.

3.9 Acute Health Hazards: T

This section considers the influence of acute toxic hazards on the overall assessment of the unit. The approach used is to consider the delaying effect caused by the material's toxicity when tackling a developing or potential incident. If operators have to wear protective equipment in order to approach the release point there will be a delay in tackling the incident and a greater chance of major fire or explosion.

3.10 Computation Of Indices.

Using the values worked previously four indices are calculated, namely an equivalent of the Dow Index, and separate indices for fire , internal explosion and overall risk. The Dow Index is not used for interpretative purposes but is retained as a link to the Dow method and to simplify later calculations. The next three indices rank particularly hazards within the units and can be used individually. The Overall Risk Rating Index is a weighted combination of the other indices and, as with other indices, its value can be equated to a descriptive category. This index facilitates comparison between units with different types of hazard. For example, Table 3.10 below, taken from the manual, shows the Overall Risk Rating categories which range from Mild, if the index is less than 20, to Very Extreme, if the index exceeds 65,000.

Overall Risk Factor R	Overall Risk Category
0-20	Mild
20-100	Low
100-500	Moderate
500-1,100	High (group 1)
1,100-2,500	High (group 2)
2,500-12,500	Very High
12,500-65,000	Extreme

Overall Risk Rating Categories

Table 3.10

3.11 Equations For Indices Calculations.

3.11.1 Equivalent Dow index, D

$$D = B*(1 + M/100)*(1 + P/100)*(1 + (S + Q + L + T)/100)$$

3.11.2 Fire index, F

$$F = B * K/N$$

3.11.3 Internal explosion index, E

$$E = 1 + (M + P + S)/100$$

3.11.4 Aerial explosion index, A

$$A = B*(1 + m/100)*(Q*H*E/100)(t + 273/300)*(1 + p)$$

3.11.5 Overall risk rating, R

$$R = D(1 + (0.2 * E * SQR(A*F)))$$

3.12 Process Developement By Hazard Factor Review.

When proceeding beyond the initial assessment where the

indices and categories have been determined, the process may be reviewed in order to identify modifications which will reduce the hazard potential of the unit.

Permissible changes such as variation of the materials of construction, reduction in inventory, alteration in sizes of equipment and operating conditions, substitution of different types of process equipment may reduce the hazard potential. The scope for such change is greatest in assessments conducted at an early design stage. For an existing plant the review stage allows reconsideration of the factors allowed initially and can sometimes include changes of the type listed above.

It must be emphasised that the designer should aim at reducing the hazard potential in the most rational, cost effective way. The Mond index is not a substitute for competent design, and a numerical effect of a modification on the Mond Index should not be the only reason for implementing the change in design.

New values assigned to any of the individual hazard factors should be entered in the "Reduced Values" column on the form and a note made of the reason for the change. When all the factors have been reviewed the indices are recalculated. These new, reduced index values form the basis for the final stage of the index, ie offsetting.

3.13 Offsetting Index Values For Safety And Preventive

Measures.

Up to this point in the calculation of the indices, measures which mitigate the hazard potential of the unit have been left apart (disregarded). The following safety preventive measures are taken into account:

a)Containment Hazards

b)Process Control

c)Safety Attitude

d)Fire Protection

e)Material Isolation, and

f)Fire Fighting.

The degree of hazard or hazard potential of a unit is a function of the frequency with which hazards occur, multiplied by their consequencies. Therefore, the offsetting factors can be divided into two groups:

-Preventive Measures; those which reduce the frequency of hazardous occurences, and

-Protective Measures; those which mitigate the concequencies once an undesired incident has occured.

a-Preventive Measures.

These measures are considered under three headings: Containment Hazards; Process Control and Safety Attitude. Each results in a reduction in the frequency

with which accidents occurs.

The more rigorous the design of the process containment system, the less likely a loss of containment results in the release of flammable material, which if ignited may lead to a severe fire or an explosion. The provision of an adequate process control system is an important feature because deviations from normal operating conditions can be rectified before resulting in extreme conditions.

The safety record of a company is a reflection of the safety policies and the management's attitude to safety. A positive management approach to safety is seen in the standard of training for all employees, the authority invested in the safety officer, and by the standard of housekeeping of their plant.

b-Protective Measures.

Protective measures help to reduce the size of any incidents which may occur and are intended to minimise the consequential damage from a fire or an explosion, either by passive resistance or by active intervention. Two aspects of passive resistance are considered: Fire Protection; and Material Isolation. These factors are interrelated.

For example, the material isolation or shutdown system

restricts the amount of fuel available, thus shortening the duration of a fire which results from a loss of containment. This also reduces the degree of fire resistance required to protect the plant.

However, the type of fire protection required is also determined by the nature of the fire.

Finally, account is taken of the fire fighting measures on the plant, which include the provision of hand held fire extinguishers, and fixed fire installations.

3.14 FINAL OFFEST INDICES CALCULATIONS.

The overall Index is offset by each of the hazard reduction factors calculated in the previous section. Because of the grouping of these factors, the reduction in the other indices may be calculated by applying the appropriate offsetting factors. The overall risk rating is then calculated. Subscript "r" will be added to all the indices to distinguish them from the indices determined previously.

It is stated that the offset Overall Risk Category, which is given by Table 3.10, represents:

"The hazard potential of the unit in the conditions as studied with all the safety systems and other

preventive measures operational in the design mode."

(4)

4. ACCURACY OF THE INDEX.

The indices have no dimension although they reflect the hazard potential of the process that is studied, they do not quantify the individual hazard frequency or consequences.

5. MOND INDEX PROGRAM.

The following program is in BASIC.

```
10    REM "MOND INDEX"
20    PRINT CHR$(141);"NAME OF THE UNIT"
30    INPUT NAME$
40    PRINT "GIVE B,M,P,S,Q,L,T,K,H,m,p,AND t"
50    INPUT B,M,P,S,Q,L,T,K,H,m,p,t
60    PRINT "D=";B*(1+(M/100))*(1+(P/100)*(1+((S+Q+L+T)/100))
70    PRINT "GIVE ME THE VALUE OF D"
80    INPUT D
90    PRINT "F=";B*K/N
100   PRINT "GIVE ME THE VALUE OF F"
110   INPUT F
120   IF F>0 AND F<2 THEN PRINT "LIGHT" ELSE GOTO 130
130   IF F>2 AND F<5 THEN PRINT "LOW" ELSE GOTO 140
140   IF F>5 AND F<10 THEN PRINT "MODERATE" ELSE GOTO 150
150   IF F>10 AND F<20 THEN PRINT "HIGH" ELSE GOTO 160
160   IF F>20 AND F<50 THEN PRINT "VERY HIGH" ELSE GOTO 170
170   IF F>50 AND F<100 THEN PRINT "INTENSIVE" ELSE GOTO 180
180   IF F>100 AND F<250 THEN PRINT "EXTREME" ELSE GOTO 190
190   IF F>250 THEN PRINT "VERY EXTREME"
200   PRINT "E=";1+((M+P+S)/100)
210   PRINT "GIVE ME THE VALUE OF E"
220   INPUT E
230   IF E>0 AND E<1.5 THEN PRINT "LIGHT" ELSE GOTO 240
240   IF E>1.5 AND E<2.5 THEN PRINT "LOW" ELSE GOTO 250
250   IF E>2.5 AND E<4 THEN PRINT "MODERATE" ELSE GOTO 260
260   IF E>4 AND E<6 THEN PRINT "HIGH" ELSE GOTO 270
270   IF E>6 THEN PRINT "VERY HIGH"
280   PRINT "A=";B*(1+(m/100))*(1+p)*((Q*H*E)/1000)*(t+273)/300
290   PRINT "GIVE ME THE VALUE OF A"
300   INPUT A
310   IF A>0 AND A<10 THEN PRINT "LIGHT" ELSE GOTO 320
```

```
 A>10 AND A<30 THEN PRINT "LOW" ELSE GOTO 330
 A>30 AND A<100 THEN PRINT "MODERATE" ELSE GOTO 340
 A>100 AND A<400 THEN PRINT "HIGH" ELSE GOTO 350
 A>400 AND A<1700 THEN PRINT "VERY HIGH" ELSE GOTO 360
 A>1700 THEN PRINT "VERY EXTREME"
INT "R=";D*(1+(0.2*E*SQR(A*F)))
INT "GIVE ME THE VALUE OF R"
PUT R
 R>0 AND R<20 THEN PRINT "MILD" ELSE GOTO 410
 R>20 AND R<100 THEN PRINT "LOW" ELSE GOTO 420
 R>100 AND R<500 THEN PRINT "MODERATE" ELSE GOTO 430
 R>500 AND R<1100 THEN PRINT "HIGH (GROUP 1)" ELSE GOTO 440
 R>1100 AND R<2500 THEN PRINT "HIGH (GROUP 2)" ELSE GOTO 450
 R>2500 AND R<12500 THEN PRINT "VERY HIGH" ELSE GOTO 460
 R>12500 AND R<65000 THEN PRINT "EXTREME" ELSE GOTO 470
 R>65000 THEN PRINT "VERY EXTREME"
INT "GIVE M1,P1,S1,L1,T1,AND m1"
PUT M1,P1,S1,L1,T1,m1
INT "D1=";B*(1+(M1/100))*(1+(P1/100)*(1+((S1+Q+L1+T1)/100))
INT "GIVE ME THE VALUE OF D1"
PUT D1
INT "F1=";B*K/N
INT "GIVE ME THE VALUE OF F1"
PUT F1
 F1>0 AND F1<2 THEN PRINT "LIGHT" ELSE GOTO 570
 F1>2 AND F1<5 THEN PRINT "LOW" ELSE GOTO 580
 F1>5 AND F1<10 THEN PRINT "MODERATE" ELSE GOTO 590
 F1>10 AND F1<20 THEN PRINT "HIGH" ELSE GOTO 600
 F1>20 AND F1<50 THEN PRINT "VERY HIGH" ELSE GOTO 610
 F1>50 AND F1<100 THEN PRINT "INTENSIVE" ELSE GOTO 620
 F1>100 AND F1<250 THEN PRINT "EXTREME" ELSE GOTO 630
 F1>250 THEN PRINT "VERY EXTREME"
INT "E1=";1+((M1+P1+S1)/100)
INT "GIVE ME THE VALUE OF E1"
PUT E1
 E1>0 AND E1<1.5 THEN PRINT "LIGHT" ELSE GOTO 680
 E1>1.5 AND E1<2.5 THEN PRINT "LOW" ELSE GOTO 890
 E1>2.5 AND E1<4 THEN PRINT "MODERATE" ELSE GOTO 700
 E1>4 AND E1<6 THEN PRINT "HIGH" ELSE GOTO 710
 E1>6 THEN PRINT "VERY HIGH"
INT "A1=";B*(1+(m1/100))*(1+p)*((Q*H*E1)/1000)*(t+273)/300
INT "GIVE ME THE VALUE OF A1"
PUT A1
 A1>0 AND A1<10 THEN PRINT "LIGHT" ELSE GOTO 760
 A1>10 AND A1<30 THEN PRINT "LOW" ELSE GOTO 770
 A1>30 AND A1<100 THEN PRINT "MODERATE" ELSE GOTO 780
 A1>100 AND A1<400 THEN PRINT "HIGH" ELSE GOTO 790
 A1>400 AND A1<1700 THEN PRINT "VERY HIGH" ELSE GOTO 800
 A1>1700 THEN PRINT "VERY EXTREME"
INT "R1=";D1*(1+(0.2*E1*SQR(A1*F1)))
INT "GIVE ME THE VALUE OF R1"
PUT R1
 R1>0 AND R1<20 THEN PRINT "MILD" ELSE GOTO 850
 R1>20 AND R1<100 THEN PRINT "LOW" ELSE GOTO 860
 R1>100 AND R1<500 THEN PRINT "MODERATE" ELSE GOTO 870
 R1>500 AND R1<1100 THEN PRINT "HIGH (GROUP 1)" ELSE GOTO 880
 R1>1100 AND R1<2500 THEN PRINT "HIGH (GROUP 2)" ELSE GOTO 890
 R1>2500 AND R1<12500 THEN PRINT "VERY HIGH" ELSE GOTO 900
```

```
900  IF R1>12500 AND R1<65000 THEN PRINT "EXTREME" ELSE GOTO 910
910  IF R1>65000 THEN PRINT "VERY EXTREME"
920  PRINT "GIVE K1,K2,K3,K4,K5,K6"
930  INPUT K1,K2,K3,K4,K5,K6
940  "Dr=D1=";D1
950  PRINT "Fr=";F1*K1*K3*K5*K6
960  PRINT "GIVE ME THE VALUE OF Fr"
970  INPUT Fr
980  IF Fr>0 AND Fr<2 THEN PRINT "LIGHT" ELSE GOTO 990
990  IF Fr>2 AND Fr<5 THEN PRINT "LOW" ELSE GOTO 1000
1000 IF Fr>5 AND Fr<10 THEN PRINT "MODERATE" ELSE GOTO 1010
1010 IF Fr>10 AND Fr<20 THEN PRINT "HIGH" ELSE GOTO 1020
1020 IF Fr>20 AND Fr<50 THEN PRINT "VERY HIGH" ELSE GOTO 1030
1030 IF Fr>50 AND Fr<100 THEN PRINT "INTENSIVE" ELSE GOTO 1040
1040 IF Fr>100 AND Fr<250 THEN PRINT "EXTREME" ELSE GOTO 1050
1050 IF Fr>250 THEN PRINT "VERY EXTREME"
1060 PRINT "Er=";E1*K1*K2*K3
1070 PRINT "GIVE ME THE VALUE OF Er"
1080 INPUT Er
1090 IF Er>0 AND Er<1.5 THEN PRINT "LIGHT" ELSE GOTO 1100
1100 IF Er>1.5 AND Er<2.5 THEN PRINT "LOW" ELSE GOTO 1110
1110 IF Er>2.5 AND Er<4 THEN PRINT "MODERATE" ELSE GOTO 1120
1120 IF Er>4 AND Er<6 THEN PRINT "HIGH" ELSE GOTO 1130
1130 IF Er>6 THEN PRINT "VERY HIGH"
1140 PRINT "Ar=";A1*K1*K2*K3*K5
1150 PRINT "GIVE ME THE VALUE OF Ar"
1160 INPUT Ar
1170 IF Ar>0 AND Ar<10 THEN PRINT "LIGHT" ELSE GOTO 1180
1180 IF Ar>10 AND Ar<30 THEN PRINT "LOW" ELSE GOTO 1190
1190 IF Ar>30 AND Ar<100 THEN PRINT "MODERATE" ELSE GOTO 1200
1200 IF Ar>100 AND Ar<400 THEN PRINT "HIGH" ELSE GOTO 1210
1210 IF Ar>400 AND Ar<1700 THEN PRINT "VERY HIGH" ELSE GOTO 1220
1220 IF Ar>1700 THEN PRINT "VERY EXTREME"
1230 PRINT "Rr=";R1*K1*K2*K3*K4*K5*K6
1240 PRINT "GIVE ME THE VALUE OF Rr"
1250 INPUT Rr
1260 IF Rr>0 AND Rr<20 THEN PRINT "MILD" ELSE GOTO 1270
1270 IF Rr>20 AND Rr<100 THEN PRINT "LOW" ELSE GOTO 1280
1280 IF Rr>100 AND Rr<500 THEN PRINT "MODERATE" ELSE GOTO 1290
1290 IF Rr>500 AND Rr<1100 THEN PRINT "HIGH (GROUP 1)" ELSE GOTO 1300
1300 IF Rr>1100 AND Rr<2500 THEN PRINT "HIGH (GROUP 2)" ELSE GOTO 1310
1310 IF Rr>2500 AND Rr<12500 THEN PRINT "VERY HIGH" ELSE GOTO 1320
1320 IF Rr>12500 AND Rr<65000 THEN PRINT "EXTREME" ELSE GOTO 1330
1330 IF Rr>65000 THEN PRINT "VERY EXTREME"
1340 GOTO 10
```

6. REFERENCES.

1)   "Fire and Explosion Index, Hazard classification
Guide", DOW Corporate Safety and Loss Prevention, May
1976.

2) "Technical Manual for the Mond Fire and Explosion Index" ICI Mond Division, 1985.

3) LEWIS, D.J.,"The Application of the Mond Index to Plant Layout and Spacing Distances" Loss Prevention, Vol.13, p.20-26, 1980.

4) LEWIS, D.J.,"The Mond Index - A Development of the Dow Index" The Appaisal and Measurement of Fire Safety, University of Edinburgh, June 1980.

<u>LOCATION</u>

<u>PLANT</u>

<u>UNIT</u>

<u>MATERIALS</u>

<u>ADDITIONAL INFORMATION</u>

COMMENT
NUMBER

PRESSURE = psig   TEMPERATURE t= DEG.C
<u>MATERIAL FACTOR (Section 5)</u>

KEY MATERIAL OR MIXTURE :
FACTOR DETERMINED BY   :
MATERIAL FACTOR   : B=

RANGE   FACTOR
                          INITIAL   REVIEW

<u>SPECIAL MATERIAL HAZARDS (Section 6)</u>

1.OXIDISING MATERIALS	0 TO 20	
2.GIVES COMBUSTIBLE GAS WITH WATER	0 TO 30	
3.MIXING & DISPERSION CHARACTERISTICS	-60 TO 100	m
4.SUBJECT TO SPONTANEOUS HEATING	30 TO 250	
5.MAY RAPIDLY SPONTANEOUSLY POLYMERISE	25 TO 75	
6.IGNITION SENSITIVITY	-75 TO 150	
7.SUBJECT TO EXPLOSIVE DECOMPOSITION	75 TO 125	
8.SUBJECT TO GASEOUS DETONATION	0 TO 150	
9.CONDENSED PHASE PROPERTIES	200 TO 1500	
10.OTHER	0 TO 150	

SPECIAL MATERIAL HAZARDS TOTAL   M

<u>GENERAL PROCESS HAZARDS (Section 7)</u>

1.HANDLING & PHYSICAL CHANGES ONLY	10 TO 50	
2.REACTION CHARACTERISTICS	25 TO 50	
3.BATCH REACTIONS	10 TO 60	
4.MULTIPLICITY OF REACTIONS	25 TO 75	
5.MATERIAL TRANSFER	0 TO 150	
6.TRANSPORTABLE CONTAINERS	10 TO 100	

GENERAL PROCESS HAZARDS TOTAL   P

SPECIAL PROCESS HAZARDS (Section 8)

1.LOW PRESSURE(BELOW 15 PSIA)	50 TO 150	
2.HIGH PRESSURE	0 TO 160	p
3.LOW TEMP.:1.CARBON STEEL +10C TO -25C	0 TO 30	
2.CARBON STEEL BELOW -25C	30 TO 100	
3.OTHER MATERIALS	0 TO 100	
4.HIGH TEMP.1.FLAMMABLE MATERIALS	0 TO 35	
2.MATERIAL STRENGTH	0 TO 25	
5.CORROSION & EROSION	0 TO 400	
6.JOINT & PACKING LEAKAGES	0 TO 60	
7.VIBRATION,LOAD CYCLING,ETC.	0 TO 100	
8.PROCESSES/REACTIONS DIFFICULT TO CONTROL	20 TO 300	
9.OPERATION IN OR NEAR FLAMMABLE RANGE	25 TO 450	
10.GREATER THAN AVERAGE EXPLOSION HAZARD	40 TO 100	
11.DUST OR MIST EXPLOSION HAZARD	30 TO 70	
12.HIGH STRENGTH OXIDANTS	0 TO 400	
13.PROCESS IGNITION SENSITIVITY	0 TO 100	
14.ELECTROSTATIC HAZARDS	10 TO 200	

SPECIAL PROCESS HAZARDS TOTAL   S

QUANTITY HAZARDS (Section 9)

MATERIAL TOTAL TONNES   K
QUANTITY FACTOR   Q

LAYOUT HAZARDS (Section 10)

HEIGHT IN METRES   H
WORKING AREA IN SQUARE METRES   N

1.STRUCTURE DESIGN	0 TO 200	
2.DOMINO EFFECT	0 TO 250	
3.BELOW GROUND	50 TO 150	
4.SURFACE DRAINAGE	0 TO 100	
5.OTHER	50 TO 250	

LAYOUT HAZARDS TOTAL   L

ACUTE HEALTH HAZARDS (Section 11)

1.SKIN EFFECTS	0 TO 50	
2.INHALATION EFFECTS	0 TO 50	

ACUTE HEALTH HAZARDS TOTAL   T

OFFSETTING INDEX VALUES FOR SAFETY & PREVENTATIVE MEASURES
✶✶

A.CONTAINMENT HAZARDS (Section 16.1)
1-PRESSURE VESSELS
2-NON-PRESSURE VERTICAL STORAGE TANKS
3-TRANSFER PIPELINES A)DESIGN STRESSES
                      B)JOINTS & PACKINGS
4-ADDITIONAL CONTAINMENT & BUNDS
5-LEAKAGE DETECTION & RESPONSE
6-EMERGENCY VENTING OR DUMPING

PRODUCT TOTAL OF CONTAINMENT FACTORS   K1=

B.PROCESS CONTROL (Section 16.2)
1-ALARM SYSTEMS
2-EMERGENCY POWER SUPPLIES
3-PROCESS COOLING SYSTEMS
4-INERT GAS SYSTEMS
5-HAZARD STUDIES ACTIVITIES
6-SAFETY SHUTDOWN SYSTEMS
7-COMPUTER CONTROL
8-EXPLOSION/INCORRECT REACTOR PROTECTION
9-OPERATING INSTRUCTIONS
10-PLANT SUPERVISION

PRODUCT TOTAL OF PROCESS CONTROL FACTORS   K2=

C.SAFETY ATTITUDE (Section 16.3)
1-MANAGMENT INVOLVEMENT
2-SAFETY TRAINING
3-MAINTENANCE & SAFETY PROCEDURES

PRODUCT TOTAL OF SAFETY ATTITUDE FACTORS   K3=

D.FIRE PROTECTION (Section 17.1)
1-STRUCTURAL FIRE PROTECTION
2-FIRE WALLS,BARRIERS
3-EQUIPMENT FIRE PROTECTION

PRODUCT TOTAL OF FIRE PROTECTION FACTORS   K4=

E.MATERIAL ISOLATION (Section 17.2)
1-VALVE SYSTEMS
2-VENTILATION

PRODUCT TOTAL OF MATERIAL ISOLATION FACTORS   K5=

F.FIRE FIGHTING (Section 17.3)
1-FIRE ALARMS
2-HAND FIRE EXTINGUISHERS
3-WATER SUPPLY
4-WATER SPRAY OR MONITOR SYSTEMS
5-FOAM & INERTING INSTALLATIONS
6-FIRE BRIGADE ATTENDANCE
7-SITE CO-OPERATION IN FIRE FIGHTING
8-SMOKE VENTILATORS

PRODUCT TOTAL OF FIRE FIGHTING FACTORS   K6=

EQUATIONS
=========

EQUIVALENT DOW INDEX (for initial assessment and review)

$$D = B(1+M/100)(1+P/100)(1+(S+Q+L+T)/100))$$

FIRE INDEX

INITIAL ASSESSMENT AND REVIEW $F = BK/N$

OFFSET $F*K1*K3*K5*K6$

INTERNAL EXPLOSION INDEX

INITIAL ASSESSMENT AND REVIEW $E = 1+(M+P+S)/100$

OFFSET $E*K2*K3$

AERIAL EXPLOSION INDEX

INITIAL ASSESSMENT AND REVIEW $A = B(1+m/100)(1+p)(QHE/1000)(t+273)/300$

OFFSET $A*K1*K2*K3*K5$

OVERALL RISK RATING

INITIAL ASSESSMENT AND REVIEW $R = D(1+(.2E*SQUARE ROOT(AF)))$

OFFSET $R*K1*K2*K3*K4*K5*K6$

INDICES COMPUTATION
====================

INDEX	INITIAL		REVIEW		OFFSET	
	VALUE	CATEGORY	VALUE	CATEGORY	VALUE	CATEGORY
D						
F						
E						
A						
R						

APPENDIX C.2.

REVIEW OF FAILURE MODE AND EFFECTS ANALYSIS.

1. INTRODUCTION.

The Failure-Mode and Effect Analysis (FMEA) is concerned almost entirely with equipment. It is used to identify the ways in which they could fail and the effects, having a serious impact on the safety and successful life of the system, that could be generated. Furthermore, this analysis permits system changes in order to reduce the failure effects.

FMEA is a component oriented technique of analysis and has been widely used in the Nuclear and Aerospace Industries (1,2). The French Nuclear safety Authorities favour FMEA over FTA as in FMEA all component failures are investigated.

2. FAILURE TYPES.

A failure could be defined as any occurence in which a system element does not carry out its function in a desired manner. There are mainly three types of non-human system element failure which are:

2.1 Primary Failure.

A failure of a system element which occurs while the element is functioning under conditions that it was designed for. Primary failures are due only to element aging.

2.2 Secondary Failure.

The failure of a system element which occurs while the element is functioning under conditions that it was NOT designed for. This places the element under excessive stress which exceeds its funtional limitations. This stress can be caused by environmental conditions, by human actions or by failure of other system elements.

2.3 Command Fault.

A failure of a non-human system element to perform its designed function due to an improper control signal or some other factor which interferes with the control signal. This failure does not degrade the condition of the particular element nor is it a result of any malfunction within the boundaries of that element.

3. APPROACH.

The analysis consists of a critical review of the system, coupled with a systematic examination of all conceivable failures at the limits of resolution and an

evaluation of the effects of these failures on the safety and capability of the system. A level of resolution must be specified and must remain consistent throughout the analysis. Time permitting, the analysis should be performed at the lowest system element level (subsystem, component, part, etc.) where a failure mode can be identified (3).

The system review begins by describing the system in terms of functional block diagrams showing each critical function performed by system elements (at the limits of resolution). Functions are identified with each system element (subsystem, component, part, etc.) at the level of resolution. Critical functions are those which must be performed if the system is to operate. They differ slightly from the general functions considered when constructing the systems' hierarchy. Critical functions are stated more concisely and include only those functions necessary for the system to achieve its objective.

A failure occurs when the system element does not perform its function in a suitable manner or a manner which would meet specifications. A system element may have several functions (4).

By considering failures in each critical function, systematic coverage of all functional failures is achieved. Failures are considered by answering the following questions:

a) HOW can the assumed functional failure actually occur, i.e., what is the failure mode? In what manner does the failure happen?

b) What is the root cause; i.e., WHY does the failure occur?

c) What are the effects of the failure; on interfacing elements (local effect) and on the overall system (system effect)?

d) Based on the worst credible effects, what is the failure or hazard classification?

e) How can the failure mode or its causes be removed or the effects made less severe?

These are general objectives which apply in any instance. It is advisable for the analyst to formulate specific objectives so as to define the boundaries of the study.

In carrying out the FMEA in this study the following specific objective was formulated:

"The objective of the FMEA in this study is to help discriminate between minor problems and those which require thorough investigation using fault tree analysis and cause-consequence analysis."

4. PROCEDURE.

The FMEA procedure contains five steps:

1. Determine level of resolution (indenture level)

2. Develop a consistent format

3. Define the problem and boundary conditions

4. Complete the FMEA table

5. Report the results.

Each of these is discussed below.

4.1 Determine Level Of Resolution.

The level of resolution determines the detail to be included in the FMEA tables. If a plant-level hazard is being addressed, the FMEA should focus on the individual systems or subsystems in the plant and on their failure modes and effects with respect to plant-level hazard; for example, the FMEA might focus on the glycol regeneration unit, the storage and transfer unit, the recompression unit,etc..When a system-level hazard is being addressed, the FMEA should focus on individual equipment that makes up the system and on its failure modes and effects with respect to the system-level hazard. For a system level hazard, such as loss of control of liquid level in the separation system, the FMEA might focus on the level transmitter, the level control valve, the level controller etc.. Of course, effects identified at the system or equipment level may subsequently be related to potential

plant hazards in the FMEA tables (5).

4.2 Develop A Consistent Format.

A standard FMEA format promotes consistency in the
information contained in the FMEA tables and assists in
maintaining the level of resolution defined in subsection
4.1. Figure 5.1 at the end of this Appendix shows an
example format for an FMEA table.

4.3 Define The Problem And Boundary Conditions.

This step identifies the specific items to be included
in the FMEA within the previously defined level of
resolution. The problem and boundary condition definition
specifically states what systems and equipment are to be
included in the FMEA. Minimum requirements for the problem
definition include:

   * Identifying the plant and/or systems that are
   subject of the analysis.

   * Establishing the physical system boundaries that
   include the equipment contained in the FMEA. This
   statement specifies the places at which the equipment
   communicate with other processes and utility/support
   systems and what portions of these "interfaces" are to
   be included in the FMEA. These boundary conditions
   should also state the operating conditions at the

interface that are assumed for the FMEA.

* Collecting up-to-date reference information that
identifies the equipment and its functional
relationship to the plant/system. This information is
needed for all equipment included within the system
boundary.

* Providing a consistent ranking definition that
addresses the potential effects of the equipment
failures.

4.4 Complete The FMEA Table.

The FMEA table should be completed in a deliberate,
systematic manner to reduce the possibility of omissions
and to enhance the completeness of the FMEA. A table can
be produced by beginning at a system boundary on a
reference drawing and systematically evaluating the items
in order as they appear in the process flowpath. Each
equipment item can then be checked off or "red-lined" on
the reference drawing when its failure modes have been
evaluated completely. All entries for each item or system
being addressed in the FMEA should be completed before
proceeding to the next item. The following items should be
standard entries in the FMEA table:

4.4.1 Equipment identification.
A unique equipment identifier that relates the equipment

to a system drawing, process, or location. This identifier distinguishes between similar equipment (e.g., motor operated valves) that perform different functions within the same system. Equipment numbers or identifiers from system drawings, such as piping and instrumentation diagrams, are usually available and provide a reference to existing system information.

4.4.2 Failure modes.

The analyst should list all failure modes for each item consistent with the equipment description. Considering the equipment's normal operating condition, the analyst should consider all conceivable malfunctions that alter the equipment's normal operation. The failure modes can be identified by considering the effects of:

a)Premature operation

b)Failure to operate at prescribed time

c)Intermittent operation

d)Failure to cease at prescribed time

e)Failure during operation

f)Degraded output, and

g)Other unique failure conditions.

For example, the failure modes of a normally open valve may include:

* Fails open (or fails to close when required)

*Tranfers to a close position

*Leaks to external environment

*Valve body rupture.

The analyst should concentrate on identifying the various failure modes rather than the potential causes of failure. Considering various causes will assist in identifying different failure modes. However, the analyst should limit the table entries to failure modes even though there may be several causes of the failure mode. The analyst should include all postulated failure modes so that their effects can be addressed.

4.4.3 Operating mode and system configuration.

The operating mode in which the system is being analysed is stated. It is important to examine the effect of the failure in every system configuration and operating mode as the effect of the failures is dependent on these conditions.

4.4.4 Failure effects.

The effects of each failure mode are investigated by considering their effect on the succeeding higher indenture levels of the system. These entered in the columns: Local Effect, Next Higher Level and End Effects. For example, the immediate effect of a pump seal leak is a spill in the area of the pump. If the fluid is flammable, a fire could be expected (because the pump is a potential ignition source) that might involve additional nearby equipment.

The end effect is the result of the failure on the whole system. For example, the safe failure of a device in the

shutdown system will initiate shutdown. The failure to danger mode may than be defined by identifying those failures which delay or prevent shutdown. The extent of the effect of a component failure depends on component's function.

4.4.5 Failure detection method.

The ways in which the failure can be identified are noted in the column with this heading. Often, the failure will be identified by its effect on another component. The presence of a device that is dedicated to warning the operator of the failure is noted here. For example, a gas detector fitted in an enclosed area will warn the operator that there is a leak of hydrocarbons from the process.

Often at low indenture levels, there are no dedicated warning devices and the operator must rely on other indications to detect the failure which is being studied by the analyst, and these should also be noted. These indications fall into three general categories:

a)They occur when the system is operating normally

b)They occur when the system has malfunctioned, and

c)Indications that are incorrect.

4.4.6 Compensating provisions.

The means of mitigating the failure are recorded under the heading Compensation Provision. Design provisions at any indenture level which allow the system to continue operating, or which shutdown the system in safe manner or

which provide a duplicate system to operate in standby, are taken into account.

It is also important to investigate the action that the operator can take to restrict the effect of the failure, given the information at his disposal. The effect of action taken in response to abnormal indications, and also the effect of incorrect action on the system, should be determined.

4.4.7 Ranking.

The analyst should classify each failure mode and effect according to the ranking definition developed in the problem definition. Each effect is examined in terms of its hazard and the potential result of that hazard and then compared to the ranking definition for classification (from MIL-STD-1629 A (6)).

Class I -CATASTROPHIC- Will cause death or severe injury to personnel, or system loss.

Class II -CRITICAL- Will cause personal injury or major system damage or will require immediate corrective action for personnel or system survival. If a safety feature MUST work in order to avert death or serious injury, then effects should be listed as Class II.

Class III -MARGINAL- Can be counteracted or controled without injury to personnel or major system damage.

Class IV -NEGLIGIBLE- Condition that will not result in personal injury, system damage, or process interuption.

4.4.8 Remarks.

Any pertinent remarks are recorded in the final column to aid the review of the FMEA by another analyst or engineer.

5. Report The Results.

The result of the FMEA is a systematic and consistent tabulation of the effects of equipment failure within a process or system. The equipment identification in the FMEA provides a direct reference between the equipment and system piping and instrumentation diagrams or process flow diagrams. The ranking provides a relative measure of the equipment failure mode's contribution to the system hazards.

Equipment failures with an unacceptable ranking should be re-examined to verify the failure modes and their effects. These failures are the most likely candidates for protective measures, especially if the failure leads directly to a serious accident.

6. FMEA Procedure.

A procedure which has been developed by Lygate (8) from

MIL-STD-1629 A (6) is given below. In essence it is a
summary of this chapter, setting out in logical form the
basic rules of FMEA.

STEP No

1   Define the system to be analysed by describing:
1.1   For each operational mode:
1.1.1   Statement of primary and secondary objectives.
1.1.2   A description of the function of each part of the
           system.
1.1.3   Draw functional or reliability block diagrams to
           illustrate the function of each part of the
           system.
1.1.4   Define what constitute the failure.

2   Examine each hardware item in turn:
2.1   For each indenture level starting at the most
           detailed level:
2.1.1   Draw a reliability block diagram to illustrate
           the function of the component being considered.
2.2   Complete the FMEA Worksheet:
2.2.1   Record the component's unique identification
           number.
2.2.2   Identify all possible failure modes by
           considering the effects of:
           a)Premature operation
           b)Failure to operate at the prescribed time
           c)Intermittent operation
           d)Failure to cease at the prescribed time
           e)Loss of output or failure during operation
           f)Degraded output
           g)Other unique failure conditions.
2.2.3   State the operation in which the component is
           being considered.
2.2.4   Identify the effects of each failure on the
           system by considering:
           a)Effect at local level (in the same indenture
             level)
           b)Effect at the next higher indenture level
           C)Effect on the whole system (End Effects).
2.2.5   Identify the means of detecting the failure by
           considering:
           a)Dedicated warning devices
           b)Other indications:
           i)when the system is operating normally.
           ii)When the system has malfunctioned.
           iii)that are incorrect because of failure of an
               indicating device.
           c)Record the means of isolating the failure.
2.2.6   Identify and evaluate the compensating provisions
           which mitigate the effect of the failure:
           a)Consider the design provisions at any indenture
             level which may be:
             i)redundant components which permit continued

operation
        · ii)safety shutdown or relief devices
          iii)alternative   modes   of   operation   (e.g.,
              stand-by systems)
        b)Consider the action the operator may take:
        i)identify the best course of action given the
           information he has available.
        ii)investigate the effects of incorrect action in
           response to abnormal indications.
2.2.7   Classify the severity of the effects of each
        failure:
        a)Category I   -CATASTROPHIC- Will cause death
          or severe injury to personnel, or system
          loss.
        b)Category II   -CRITICAL- Will cause personal
          injury or major system damage or will require
          immediate corrective action for personnel or
          system survival. If a safety feature MUST work
          in order to avert death or serious injury, then
          effects should be listed as Class II.
        c)Category III -MARGINAL- Can be conteracted or
          controled without injury to personnel or major
          system damage.
        d)Category IV -NEGLIGIBLE- Condition that will
          not result in personnel injury, system
          damage, or process interuption.
2.2.8   Note any pertinent remarks, particularly design
        improvement to/be recommended in the FMEA report.
        Information should be given about Category I or
        II failure modes and appropriate action to be
        taken to reduce the probability of their
        occurence.

7. COMMENTS.

    FMEA can be initiated at any stage of design or

development and at any level of detail (2). the technique

leads to minimisation of the risk failures, ensures that

items of optimum reliability are selected in system

design, optimises probability of mission accomplishment,

and is especially beneficial in spotting single-point

failures. On the other hand, the effectiveness of the

technique is limited to analysis of single units or single

failures. Other failures may be overlooked. As usually

applied, it may give inadequate attention to human error,

hazardous characteristics of the equipment, adverse environments, or the effects of failure combinations .

The results of the FMEA are useful in other hazard evaluation methods. For example, in conjunction with a HAZOP study, the FMEA provides a concise summary of the hazards associated with components failure. (In fact, the FMEA is a subset of a complete HAZOP study). The FMEA is also useful in fault tree analysis, event tree analysis, and cause-consequence analysis. where the analyst must determine the contributing equipment failure for a stated hazard. For example, an important hazard identified in a HAZOP can be compared to the effects listed in the FMEA to identify specific equipment failure modes that are directly involved with the hazard (7).

8. REFERENCES.

1 Cross, A. "An introduction to FMEA and FTA" National Center of System Reliability, 1982.

2 National Aeronautics and Space Administration, "Instructions for Preparation of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL).", NSTS 22206, October, 1986.

3 Dussault, H.B., "The Evaluation and Practical Applications of Failure Modes and Effects Analysis", RADC-TR-83-72, Rome Air Development Centre, Griffin Air

Force Base, New York, March 1983.

4 King, C.F. & Rodd, D.F. "Design and maintenance of
failure tolerant process" A.I. Chem. E. Journal Vol.18,
p.257, 1983.

5 Cavicchia, V., Pennazzi, M., Toccafondi, G. and Vezey,
E.E., "Timely Risk Assessment Improves Plant Safety",
Hazard Prevention Journal, Nov./Dec. 1985.

6 US Departement of Defence, "Military Standard Procedure
for Performing a Failure Mode, Effects and Critically
Analysis", MiL-STD-1629A, Washington, D.C., Nov 1980.

7 Fitzgerald, J.N., "FMEA or FTA - Which One When?" Hazard
Prevention Journal, Nov./Dec. 1984.

8 Lygate, J.F., "An Evaluation Of Different Methods Of
Hazard Analysis Based On A Study Of An Offshore Gas
Compression System", PhD Thesis, Edinburgh University,
1983.

identification number	item/functional identification (nomenclature)	function	failure mode and causes	operational mode	FAILURE EFFECTS			failure detection method	compensating provisions	severity class	remarks
					local effects	next higher level	end effects				

215

APPENDIX C.3

REVIEW OF FAULT TREE ANALYSIS.

1.INTRODUCTION.

The original concept of fault tree analysis (FTA) was developed at the Bell Telehone Laboratories in work on the safety evaluation of the Minuteman Launch Control System in 1961. From then on, it has been widely used in the nuclear power industry and constitutes the core of the methodology applied in risk studies (1), where in addition to calculating the expected frequency of undesired events, their consequences are assessed (2). Relatively few applications of the method to process plant system have become known. They mostly refer to trip systems of hazardous installations (3), auxilary systems, or parts of chemical processes (4-9). The fault tree analyses for process plant systems, which have become known, deal with events during normal steady-state operation. Start-up and shut-down, which frequently give rise to accidents, are not addressed.

During the last twenty years several authors published papers which discussed the application of FTA to complex chemical process plants (10-15). However, the main emphasis of the work has been to develop computer programs to aid the analyst construct and evaluate fault

trees. Useful review of computer methods in FTA has been published by Cross (16) and Arendt and Fussell (17) and Camarinopoulos (24).

1.1 Definition.

Fault tree analysis is a deductive method which is normally used in a quantitative way, although it requires as an initial step a qualitative study of the system under consideration, just as any method of system analysis. After defining the undesired event, its logical connections with the basic events of the system are searched for and the result of this search is represented graphycally by means of a fault tree, as, for example, in Figure 1 at the end of this Appendix (fault tree derived from API RP 14c). The tree reflects the outcome of the qualitative part of the analysis, in which questions of the "how can it happen?" type are answered. These serve to identify, firstly, process functions and subsystems such as cooling or electric supply whose failure causes the undesired event and then connects these failures successively with the basic events.

1.2 Logic Gates And Event Symbols.

The logical connections in the fault tree are generally represented by two types of gates, the "OR" and the "AND". In the case of the "OR" gate, any one of the entries alone is capable of producing the output event, while the output

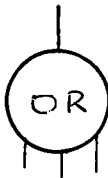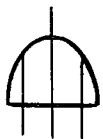event of an "AND" gate only occurs if all its entry events
are fulfilled.

Table 1.2 shows the different type of logic gates and
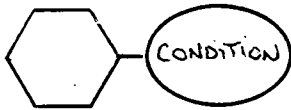the symbols used to represent the events described in a
fault tree.

Logic Symbols
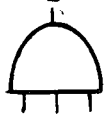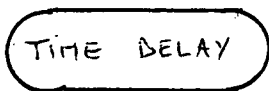
AND gate

Output exists only if all inputs exist

OR gate

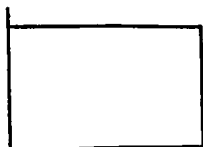Output exists if any input exists

INHIBIT gate

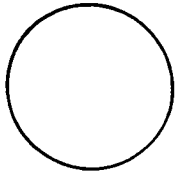Output equals input if condition input
satisfied

DELAY gate

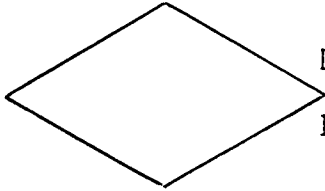Output exists after delay time has elapsed

Event Symbols

RECTANGLE
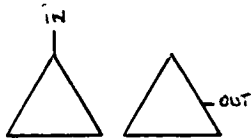
Fault event usually resulting from more
basic fault events

CIRCLE

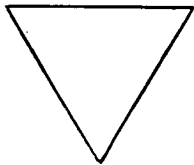A basic component fault, assumed to be an

independent event

DIAMOND

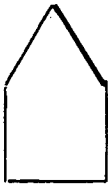Fault event not developed to its cause

in

TRIANGLE

out

A connecting or transfer symbol

UPSIDE DOWN TRIANGLE

A similarity transfer. The input is similar

but not identical to the like identified

input

HOUSE

Event normally expected to occur

TABLE 1.2 Fault Tree Logic and Event Symbols.

Throughout the analysis of the unit I have used the set

symbols listed in Table 1.2.

Two states of the basic events are normally admitted. They are either failed or functioning which implies two possible states for the undesired event, its occurrence, and its nonoccurrence. The two states are adopted with certain probabilities which are generally obtained for each type of component by evaluating the operating behaviour of a great number of similar components. Applying these probabilities to the basic events of the tree, the probability of the undesired event may be calculated.

2. PROCEDURE.

In order to carry out a fault tree analysis the following steps are required:

a. Familiarisation with the system using process description, piping and instrumentation diagrams, etc., and information obtained from the plant personnel.

b. Definition of the top and initiating events using material information, checklists, historical evidence, etc..

c. Development of the fault tree(s).

d. Obtaining probabilities for the failure of technical components and human error (see chapter 2).

e. Verify The Tree

f. Qualitative evaluation

g. Quantitative evaluation

h. FTA Report

2.1 Identification Of The Top And Initiating Events.

Petrochemical processes involve both physical and chemical hazards. Physical hazards derive from operating conditions which may be extreme, such as very low or very high temperatures and pressures. Chemical hazards are those associated with the materials present in the process, which may be toxic, flammable or explosive, or exhibit several of these properties at the same time. The matter is complicated further by the fact that some of these properties may vary with changes of process parameters such as temperatures, pressures, or concentrations, or that these changes may give rise to side or spontaneous reaction, for example, heating, decomposition, or polymerisation. As it happens, incidents in chemical plants are characterised by these changes only. In addition, dangerous properties, if not present under normal process conditions, may develop upon contact of process media with auxiliary media such as coolants, lubricants, or impurities, which may be introduced into the process with process streams or originate from

component materials. After release they may occur as a consequence of reactions with substances present in the environment. The above enumeration, which is by no means complete, shows what difficulties the process safety analyst has to face.

2.1.1 Undesired events.

The undesired event in a safety analysis for a petrochemical process plant usually is a toxic release, a fire or explosion, or a situation ·in which these may be produced as, for example, release of hydrocarbons containing hydrogen sulphide. It is usually assumed that in addition to air, water and ignition source are present in the environment. In our case the undesired event will be a near-miss event. The latter is usually defined as an event which could have developed into a catastrophe (a toxic release, a fire or explosion). Once the undesired event or events have been fixed, the initiating events (events potentially capable of bringing about the undesired event) must be found.

2.1.2 Initiating events.

If a system is designed properly, incidents can only occur if there are deviations from normal operating conditions. These may be provoked by component failures, which imply either the loss of function (stuck valve, for example) of the loss of integrity (e.g., damaged gasket)

and spontaneous/external events or human error.

Systems usually have components which are required to be working in order for the system to function (operational components), stand-by components which take over from them should they fail, and components which belong to protection and safety systems, and hence only have to work under special circumstances. Since only failures of the operational components may affect system behaviour directly, they are usually taken to be initiating events. In addition, the loss of component integrity (of the system boundary) in such a way that a release from the system or the introduction of air or auxiliary media to the system has to be considered, if dangerous situations can result. Human error must be considered as well.

2.1.3 Outline of a computer-aided search for undesired and initiating events.

The search for undesired events requires the analyst to have a thorough knowledge of the system under investigation and a good background in physics, chemistry, and engineering. His ability in detecting dangerous situations should be enhanced by experience with previous analyses and an overview of past incidents in the same type or similar plants. This knowledge, together with specific information on the properties of the materials involved, process conditions, and component failure modes (e.g., a valve may fail open or closed, leak, or be

stuck), is combined to identify the undesired and initiating events.

This situation lends itself to building an expert system. Therefore, a preliminary computer program was written which combines material properties (18), information on possible failure modes of components obtained in the field study, and case histories (19) with input information on the process to yield specific warnings and undesired and initiating events. The program processes information using rules in the form IF...THEN, and it is assumed in line with the spirit of a safety analysis that anything that might go wrong will go wrong: IF the initial condition is satisfied THEN the outcome will occur with probability 1. For the case histories, a screening process according to material and event type is carried out. The user must then select those events which proceed in his specific case. Operational component failures are simply input after consulting a list with possible failure modes. The results of an analysis performed with the program are recorded and provide feedback in form of a checklist for later use.

2.2 Fault Tree Development.

In a process/system there are usually a number of stand-by components (which may step in if operational components fail) and protective and safety systems. These are normally capable of coping with the major part of

initiating events and may be considered as barriers between those and the undesired event. The latter only occurs if these barriers fail.

If components from several barriers have to fail for the undesired event to occur, these are combined with the initiating event by an "AND" gate. If several of these combinations exist, they are input into an "OR" gate, just as the contributions from the different initiating events to the undesired event. The components which have to be in failed state at the same time if the initiating event is to cause the undesired event are called redundancies and their number indicates the degree of redundancy.

2.2.1 Obtaining probabilities for the failure of components and human error.

Quantification of fault trees is achieved by assessing failure data or probability to each event on the tree. These data are then summed using Boolean algebra to reach a probability that the top event can occur. It is for this reason that FTA is used to study the reliability of systems. Failure rates and probabilities can be obtained as discussed in chapter 2.

When quantifying a fault tree for the first time, many people do not pay sufficient attention to the dimensions of the data used to calculate the probability or frequency of the top event. This results in an incorrect calculation

of the probability of the top event.

2.3 Verify The Tree.

A fault tree should be verified by a senior engineer who has an intimate knowlege of the system that has been modelled. It is easy for the analyst to misunderstand or overlook an important aspect of the process.

The time taken to verify the tree will be shortened if the analyst documents the assumptions he has made as he was constructing the tree. Most inadequacies in the tree will be related to these assumptions particularly when they have to do with temporal aspects. An engineer checking the tree and its assumptions may clarify the situation enabling the analyst to construct a more accurate model.

2.4 Common Mode Failures.

Apart from the independent failures treated previously, the possibility of common mode failures in technical system has to be considered with attention. This type of failure leads to the simultaneous unavailability of several components. The following types of common mode failures may be distinguished:

a) Failures of two or more redundant components or partial systems of similar or identical design, due to

an outside cause, for example, a corrosive environment which leads to rapid component degradation

b) Failures of two or more redundant components or partial systems which occur as a consequence of a single failure; this type of common mode failure is called "casual" failure

c) Failures of two or more redundant components or partial systems which occur as a consequence of functional dependencies as, for example, the dependence on a common auxilary system.

The remaining types of common mode failures due to common external cause (e.g., planning, construction, or maintenance errors) should be treated by evaluating relevant operating experience. In this category, which comprises the common mode failures in the strictest sense of the word, a distinction should be drawn between those:

a) which occur or are discovered on occasion of an incident

b) those which are discovered on functional demand of the system either because of testing or an operational requirement, or

c) those which are self-annunciating (e.g., because the components affected are of the type which gives an alarm upon failure).

Operating experience primarily supplies data for the last two types of common mode failures, while those occuring only on occasion of an incident can in general only be discovered using analytical methods.

The evaluation of operating experience may be carried out with several models; among them are the B-factor method and the specialized Marshall-Olkin model. These models are discussed in detail in reference 25 and 26.

2.5 Qualitative Evaluation.

The completed fault tree provides much useful information by displaying the interactions of equipment failures that could result in an accident. However, except for the simplest fault trees, even an experienced analyst cannot identify directly from the fault tree all the combinations of equipment failures that can lead to an accident. A failure mode is Known as a cut set which is a set of primary failures or undeveloped faults which can give rise to the top event. Minimal cut sets are all the combinations of equipment failures that can result in the fault tree Top event, and they are logically equivalent to the information displayed in the fault tree. The minimal cut sets are useful for ranking the ways in which the accident may occur, and they allow quantification of the fault tree if appropriate data are available. Large fault trees require computer programs to determine their minimal cut sets. Details of different computer codes which

shorten the time taken to carry out FTA can be found in reference 16 and 17.

The main source of problems is when a number of different events specified in a tree have common cause. For example, the blockage of the impulse lines of the level transmitter and of the extra low level switch could result from the build up of residue in the lines. This common cause is extremly unlikely to occur during the interval between maintenance work. The analyst should therefore examine the tree, and reconstruct it to reflect the effect of the common cause failures.

A problem which arises during the qualitative evaluation is that sometimes events are mutually exclusive. In large trees there will be events that will be in opposition to each other. For example, the level control valve cannot be too far closed and too far open at the same time. The analyst must discover these mutually exclusive events and discount the minimal cut sets where both events appear.

After the cut sets have been determined, the effect of design modifications can then be investigated by studying their effect on the tree. As a general rule, the greater the number of events in a minimal cut set, the lower the probability of the top event. Design changes which generate AND gates at the highest levels in the tree should be recommended. This reduces the probability of the top event.

2.6 Quantitative Evaluation.

The probability of occurrence of each basic event is
required to start the quantitative evaluation of the fault
tree. The probability of the top event may then be
calculated and the most probable minimal cut sets or
failure modes determined. The mathematical techniques
required to resolve fault trees are well developed and
computer programs are available to help resolve the
probabilities of the minimal cut sets and the top event.
(20-24).

A variety of sources which include data banks and
company maintenance records can provide the analystwith
the required data. Careless application of data
particularly of data taken from different contexts, from
the Nuclear Industry for example, has caused most design
engineers to regard quantified FTA with scepticism. This
hostility mainly arises when the analyst fails to
communicate the assumptions he has made and fails to carry
out a sensitivity analysis to determine the level of
uncertainty of the top event probability.

During the design stages most of the problems can be
identified and resolved by quantitative analysis. As the
quality and accuracy of failure rate data improves, more
reliance can be justifiably placed on quantified fault
trees.

2.7 FTA Report.

The analyst presents his findings and recommendations in the form of a report which should include the FTA, a short written description of the tree, the assumptions that have been made and a list of the most likely failure modes.

The report should discuss the need for any design changes and illustrate their effects on the tree. The comments of the engineer who has verified the analysis should be included as this strengthens the integrity of the analysis.

3. REFERENCES.

1) PRA Procedure Guide, "A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, Vol.1 and 2, U.S. Nuclear Regulatory Commission, Washington D.C, 1983.

2) U.S. Nuclear Regulatory Commission, Reactor Safety Study, "An Assessment of Accident Risk in U.S. Commercial Power Plants", WASH-1400, NRC, Washington, D.C., 1975.

3) Kumaomoto, H. and Henley, E.J., "Protective system hazard analysis", Ind. Eng. Chem. Fundam., 17(4), 274, 1978.

4) Nielsen, D.S., Platz, O. and Kongso, H.E, "Reliability Analysis of a Proposed Instrument Air System" RISO-M-1903, Riso Research Centre, Roskilde, Denmark, 1977.

5) Shaeiwitz, J.A., Lapp, S.A, and Powers, G.J., "Fault tree analysis of sequential systems", Ind. Eng. Chem. Process Des. Dev., 16(4), 529, 1977.

6) Hauptmanns, U., "Fault tree analysis of a propsed ethylene vaporisation unit", I & EC Fundam., 19(3), 300, 1980.

7) Hauptmanns, U., Yellera, J., and Sastre, H., "Safety analysis for the ammonia-air Mixing system of a plant for the production of nitric acid", J. Chem. Eng. Jpn., 15(4), 286, 1982.

8) Hauptmanns, and Sastre, H., "Safety analysis of a plant for the production of vinyl acetate", J. Chem. Eng. Jpn., 17(2), 165, 1984.

9) Andow, P.K., "Expert systems in process plant fault diagnosis", Inst. Chem. Eng. Symp. Ser., 90, 1984.

10) Powers, G.J & Tompkins, F.C, "A synthesis strategy for fault trees in chemical processing systems" Loss Prevention, vol.8 p.91-99, 1974.

11)Powers, G.J & Tompkins, F.C, "Fault tree synthesis for

chemical processes" AIChE Journal vol.20, No.2, p.376-387, Mar. 1974.

12)Powers, G.J & Tompkins, F.C, "Computer aided synthesis of fault trees for complex processing sytems" Generic Techniques in System Reliability Assessment, Noordoff, p.307 314, 1976.

13)Lapp, S. & Powers, G.J "Computer assisted generation and analysis of fault trees", 2nd Int.Symp. on Loss Prevention and Safety Promotion in the Process Industries, p.VII-377-384, 1977.

14)Lawley, H.G, "Operability studies and hazard anallysis" Loss Prevention, vol.8 p.105, 1974.

15)King, C.F & Rudd, D.F, "Design and maintenance of economically failure tolerant processes" AIChE Journal vol.18, No.2, p.257-269, Mar. 1972.

16)Cross, A. "Computers programs for fault tree analysis" SRS Quaterly Digest, Jan. 1980.

17)Arendt, J.S & Fussell, J.B "System reliability engineering methodology for industrial application" Loss Prevention, vol.18 p.18-25, 1980.

18) Sax, N.I., "Dangerous Properties of Industrial Materials", van Norstrand Reinhold, New York, 1984.

19) Kletz, T.A., "Plant instruments: which ones don't work and why", Chem. Eng. Progr., 76(7), 68, 1980.

20) Barlow, R.E. and Proschan, F., "Statistical Theory of Reliability and Life Testing - Probability Models", Holt, Rinehart, & Winston, New York, 1975.

21) Hammersley, J.M. and Handscomb, D.C., "Monte Carlo Methods", Methuen, London, 1975.

22) Hauptmanns, U., Yellera, J., "Fault tree evaluation by Monte Carlo simulation", Chem. Eng., p.91, January 1983.

23) Guldner, W., Polke, H., and Zipf, G., "Computer Code Package RALLY for the Probalistic Safety Assessment of Large Technical Systems", GRS-57, Gesellschaft fur Reaktorsicherheit, Cologne, 1984.

24) Camarinopoulos, L. and Yllera, J., "An inproved top-down algorithm combined with modularisation as a highly efficient method for fault tree analysis", Reliability Eng., 11, 93, 1985.

25) Fleming, K.N. and Raabe, P.H., "Comparison of three methods for quantitative analysis of common cause failure", Proc. ANC Topical Meet. Probabilistic Analysis of Nuclear Reactor Safety, GA-A-14568, General Atomic Co., San Diego, California 1978.

26) Vesely, W.E., "Estimating common cause failure probabilities in reliability and risk analysis: Marshall-Olkin specialisations", in Nuclear Systems Reliability and Risk Assessment, Fussel, J.B. and Burdick, G.R., Eds., Society for Industrial and Applied Mathematics, Philadelpia, 1977.
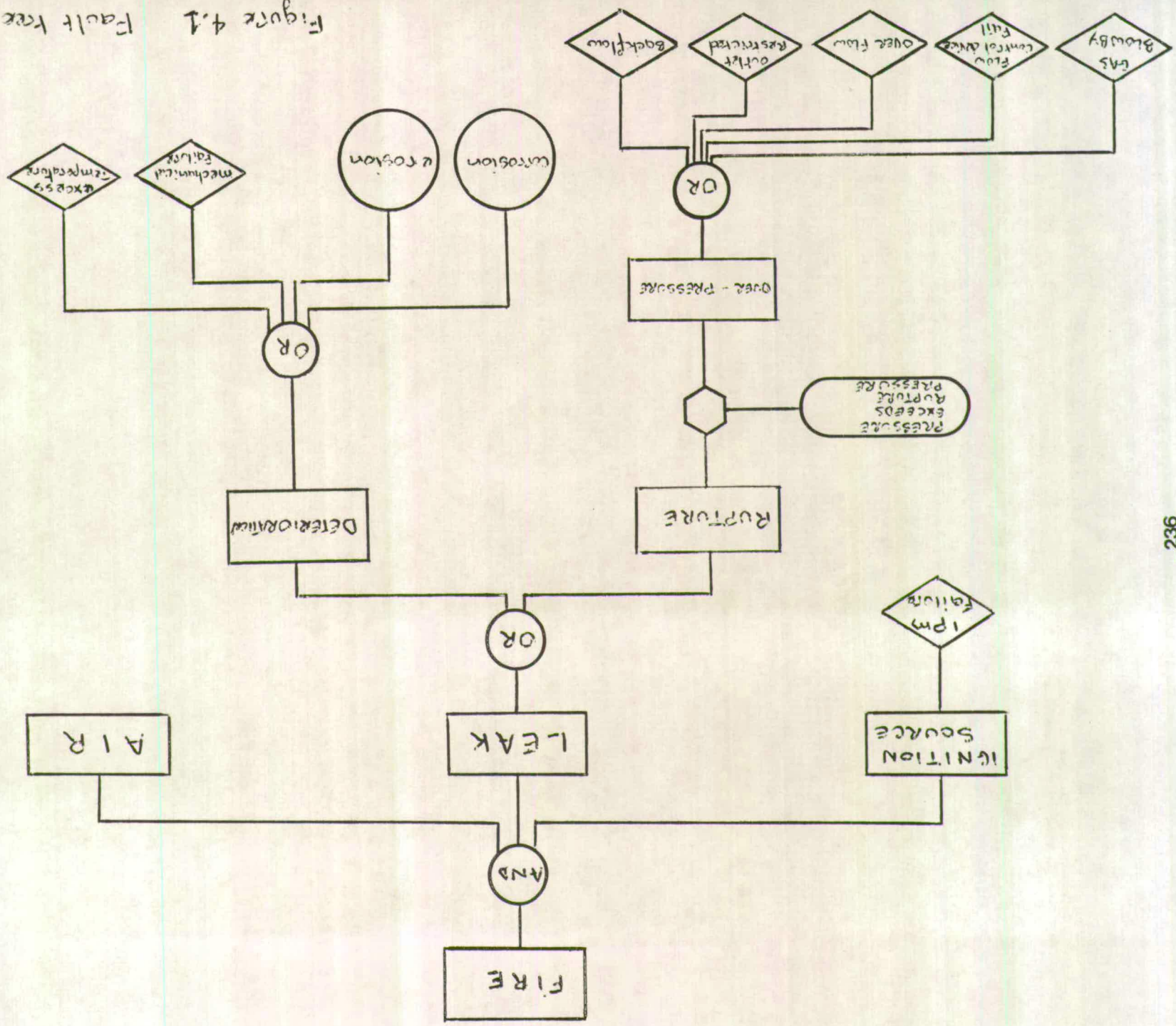
APPENDIX C.4

REVIEW OF THE CAUSE-CONSEQUENCE ANALYSIS.

1.INTRODUCTION.

Reliability performance of a completed plant are largely judged on the costs resulting from faults in term of loss of production, damage to plant, or injuries to staff. It is therefore important to develop systematic methods for cause-consequence analysis, relating the potential modes of failure to the ultimate consequences for the system.

For such failure/consequence analysis, the cause-consequence diagrams or cause-consequence charts (CCC) provide the engineer with both an analysis strategy, and a notation for presentation and documentation. Besides, the cause-consequence diagrams offer a systematic support for probabilistic modelling (Nielsen and Runge (1)).

1.1 Definition.

A cause-consequence diagram is constructed by defining a critical event, and then both defining the consequence events and paths which flow from the critical event and defining cause events for the critical event and logical

relations between the cause events. In other words, the forward development is similar to an event tree and the backward development is similar to a fault tree. The main elements of the diagram are therefore event and condition definitions and logic gates and vertices.

1.2 Logic Symbols.

Table 1.2 shows the different type of logic symbols used to represent the events described in a cause-consequence diagram. The logic symbols include both gates which describe the relations between cause events and vertices which describe the relations between consequences. The event and condition symbols describe the type of event or condition. The symbols given are those which have been used by Nielsen(2).

The main logic gates are the AND gate and the OR gate. There are corresponding logic vertices in form of the AND vertex and the OR vertex.

The EITHER/OR vertex, or decision box, is also very useful. It is utilized in particular to determine the effect of an event or condition on the paths which the system takes. If, as is often the case, the 'NO' output from the decision box is the result of an abnormal condition, then a fault tree occurs on the diagram for that abnormal conditions.
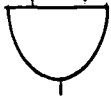
Logic Symbols   Meaning of Symbols

                                      AND gate
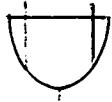
                                      OR gate

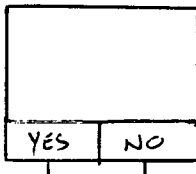   AND vertex

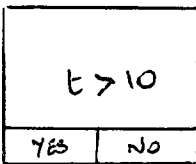   Mutually exclusive, exhaustive
                                      OR vertex

                                      Mutually exclusive OR vertex
                                      (after time delay)

| YES | NO |
                                      EITHER/OR vertex, decision

t > 10
| YES | NO |
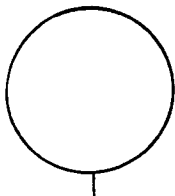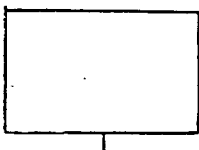   Condition vertex

Event and condition Symbols

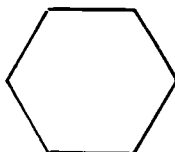   Basic condition

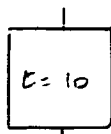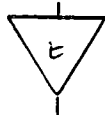   Initiating   event   (may   be
                                      critical event)
                                      Event

                                      Significant Consequence

                                      Condition

$t = t_0$

Fixed Time Delay

t

Variable Time Delay

TABLE 1.2. Cause-Consequence Diagram Logic and Event Symbols.

Throughout the analysis of the unit I have used the set symbols listed in Table 1.2.

1.3 Quantification Of Cause-Consequences.

Quantification of cause-consequence diagrams is achieved, in the same way as for the quantification of FTA, by assessing failure data or probability to each event on the diagram. These data are then summed using Boolean algerbra.

2.APPROACH.

2.1 System definition.

On the highest level (plant level) the purpose of systematic cause-consequence analysis is to relate potential modes of failure of individual components to the ultimate consequences for the system ('loss of production', 'plant damage', etc.). In starting the analysis, however, the following question arises: What is the expedient starting point? In our case it will be

near-miss events.

Near-miss events are faults that arise during normal plant operation and could lead to large potential consequences (loss of life or property). They could be qualified as critical events that have been subdued either by the process control system or the operators . The direct effects would be that energy or mass balances of main process are disturbed. Attention should be focussed on faults or events that directly affect these balances and cause parameter changes/transients.

Near-miss events can constitute the starting point for a search of a top event of which the potential consequences are sought. The cause-consequence analysis then proceedes from these near-miss events.

The ability of the plant to meet and deal with excessive transients is largely determined by systems which are designed to perform accident preventing actions ('designed protective actions). In this way undesired event sequences are prevented. However, a desired intervention may fail ('designed protective action x does not occur as intended') or it may not have been possible to design an intervention action at all. In such cases one must rely on accident-limiting systems (barriers, sprinkler systems, evacuation, etc.).

2.2 The Cause-Consequence Diagram.

The display format used in connection with cause-consequence analysis is the cause-consequence diagram. Throughout this section the text will be illustrated by an example of a cause-consequence diagram for a near-miss event due to foam formation in a gas/liquid separation vessel.

Foaming occured in a low pressure separation vessel leading to an increase in the liquid level. The response of the control system was to open the level control valve. Since this rise in the liquid level is only apparent the first consequence is that the liquid residence time is shortened reducing the separation efficiency.

In the consequence diagram different possible event sequences are described. Often a near-miss event can lead to different event sequences that may depend on conditions within the process system; on fig. 1 it is indicated that different event sequences can occur if, for instance, one or more of the accident-preventing actions ('designed safety actions') does not occur as intended. As consequence diagrams provide the possibility for diplaying the logical connection between events and conditions, different sequences can be systematically identified.

An advantage of presenting sequence events in a cause-consequence diagram is that the analyst is invited to study sequence. The sequence of events can be followed

along the different paths in the block diagram.

Provided that the 'basic inputs' of the cause diagrams are independent, then the cause-consequence diagram displays the logical connection between a set of independent faults and their consequences.

As a cause-consequence diagram for a near-miss event describes one or more sequences of events, the time dimension is introduced in the diagram. This provides, of course, the possibility of taking into account random faults that may occur in the time following the occurrence of the near-miss event; often a system with accident-limiting function is required to operate for a certain period (e.g. a pressure safety valve).

2.3 System Configuration.

The basic material for cause-consequence analysis is the plant hardware description in the form of functional system diagrams and piping and instrumentation diagrams. These must be supplemented by physical layout drawings, observation of the actual hardware layout if this is possible, and with experience of component behaviour, especially in the later stages of the analysis. The information required can be listed as follows:

   1. Interconnection of plant components,
   2. Location of systems with respect to each other,

i.e. process components, systems with accident-preventing or limiting functions, and auxiliary systems such as power, lubrication, cooling supplies, etc.,

3. Operating modes of systems,

4. Normal operating conditions for each component (in each mode) together with component limits for static and transient pressure, temperature, stress, and radiation loading,

5. Main process variables,

6. Energy sources and their location,

7. Physical and chemical properties of species under normal as well as abnormal conditions.

A review of the necessary detailed information of this kind for chemical plant is given by Powers et al. (3).

3. CCA PROCEDURE.

A procedure for cause-consequence analysis has been developed by NEILSEN and al. Some of the main steps are:

1. Consider a NEAR-MISS EVENT.
When studying a near-miss event within the boundaries of certain process system it is assumed that no other critical event has occured within the system.

2. Modify the dynamic model of the process taking the near-miss event into account.

3. Specify the changes/transients (delay and magnitude) of the main process parameters at locations where there are protective devices or parts of protective devices (safety valves, sensors, etc.).

3a. Which trip limits/set points are exceeded?

4. Are loading limits for relevant process components exceeded by effects from process parameter changes/transients?

5. Identify which 'designed protective actions' (i.e. accident-preventing or -limiting actions) are potential according to the answers to items 3a.

In this connection it should be realized that:

a) a designed protective action can, if released, be 'desirable' as well as 'undesirable' in the context of the actual accident situation.

b) a desirable designed protective action may fail (i.e. designed protective action x does not occur as intended).

6. Construct a consequence diagram which shows the potential combinations of 'release' and 'not release' designed protective actions.

7. For each of the identified potential accidents specify the changes/transients of main process parameters (pressure, temperature) in relevant process components.

8. The following applies to each of the identified, potential accidents: Are loading limits for relevant process components exceeded by effects

from process parameter changes/transients?

If so, what are the potential, significant consequences? (´damage to ..´, ´escape of..´, ´injury to..´).

4.QUANTITATIVE EVALUATION.

An assessment of the probability of significant plant hazards may be highly desirable. A necessary basis for probabilistic analyses is that:

1) thorough cause-consequence analyses have been performed, and that

2) the ability of safety systems to cope with the various critical events have been substantiated during the analysis.

The probabilistic modelling techniques deal with component faults that can be considered as spontaneous and can be covered by significant statistical data. The effectof repair and test policy can be taken into account, if relevant. In connection with probabilistic failure modelling the cause-consequence diagram provides a systematic method of documentation (4).

5. REFERENCES.

1)Neilsen, D.S. and Runge, B., "Unreliability of a Standby System with Repair and Imperfect Switching", IEEE Transactions on Reliability, Vol. R-23, No.1, April 1974.

2)Neilsen, D.S.,"Use of cause-consequence charts in practical system analysis.", Atom. Energy Commn, Res. Est., Riso, Denmark, Rep.Riso-M-1743, 1974.

3)Powers, G.J. and Tompkins, F.C., "Fault Tree Synthesis for Chemical Processes", AIChE Journal, Vol.20, No.2, 1974.

4)Neilsen, D.S., Platz, O., and Runge, B., "A Cause-Consequence Chart for a Redundant Protection System", IEEE Transactions on Reliability, 1984.

BIBLIOGRAPHY

Andow, P.K., "Event trees and Fault Tree" Loughborough University of Technology, Course on Loss Prevention in Process Industries, 1979.

Andow, P.K., "Expert systems in process plant fault diagnosis", Inst. Chem. Eng. Symp. Ser., 90, 1984.

Anyakora, S.N., Engel, G.F.H., and Lees, F.P., "Some data on reliability of instruments in the chemical plant environment", Chem. Eng., p.396, November 1971.

Arendt, J.S & Fussell, J.B "System reliability engineering methodology for industrial application" Loss Prevention, vol.18 p.18-25, 1980.

Atomic Energy Commission, "reactor Saffety Study", WASH-1400, 1975.

Balemans, A.W.M., et al., "Checklist: Guidelines for Safe Design of Process Plants", 1st International Loss Prevention Symposium, 1974.

Barlow, R.E. and Proschan, F., "Statistical Theory of Reliability and Life Testing - Probability Models", Holt, Rinehart, & Winston, New York, 1975.

Bell, B.J. and Swain, A.D., "A Procedure for Conducting Human Reliability Analysis" NUREG/CR-2254, U.S. Nuclear Regulatory Commission, Washington, D.C., May 1983.

Berenblut, B.J & Menashe, J., "Ranking of Risk in Commerce and Industry.", Safety and Loss Prevention I.Chem. E. Symp., No 77 April 1982.

Browning, R.L., "Use of a Fault Tree to Check Safeguards.", Loss Prevention, Vol. 12, p. 20-26, 1978.

Camarinopoulos, L. and Yllera, J., "An inproved top-down algorithm combined with modularisation as a highly efficient method for fault tree analysis", Reliability Eng., 11, 93, 1985.

Cassidy, K., "The National and International Framework of Legislation for Major Industrial Accident Hazards" I. Chem. E. Symp. Series No. 110, pp. 401-413, May 1988.

Cavicchia, V., Pennazzi, M., Toccafondi, G. and Vezey, E.E., "Timely Risk Assessment Improves Plant Safety", Hazard Prevention Journal, Nov./Dec. 1985.

Cizek, J.G., "Diamond Shamrock Loss Prevention Review Program", Canadian Society for Chemical Engineering Conference, 1982.

Cox, D.R., "Renewal Theory", Methuen, London, 1962.

Cross, A., "An Introduction to Failure Mode and Effects Analysis and Fault Tree Analisis.", National Center of System Reliability, 1981.

Cross, A. "Computers programs for fault tree analysis" SRS Quaterly Digest, Jan. 1980.

Cross, A. "An introduction to FMEA and FTA" National Center of System Reliability, 1982.

Davis, K.R., "Techniques for the Identification and Assessment of Major Accident Hazards", The Institution of Chemical Engineers, EFCE Publication Series No. 42, pp.289-308, (UMIST) Manchester, 22-24 April 1985.

Dow Chemical Company, Fire and Explosion Index, Hazard Classification Guide, 5th Edition, 1981.

Drysdale, D.D. & David, G.J., "Hazard Analysis for a Storage Sphere of Pressurized Liquified Flammable Gas.", Fire Safety Journal, No. 2, P. 91-103.

Dussault, H.B., "The Evaluation and Practical Applications of Failure Modes and Effects Analysis", RADC-TR-83-72, Rome Air Development Centre, Griffin Air Force Base, New York, March 1983.

Embrey, D.E., "Approaches to the Evaluation and Reduction of Human Error in the Process Industries", Institution of Chemical Engineers Symposium, 66, 1981.

"Fire and Explosion Index, Hazard classification Guide", DOW Corporate Safety and Loss Prevention, May 1976.

Fitzgerald, J.N., "FMEA or FTA - Which One When?" Hazard Prevention Journal, Nov./Dec. 1984.

Fleming, K.N. and Raabe, P.H., "Comparison of three methods for quantitative analysis of common cause failure", Proc. ANC Topical Meet. Probabilistic Analysis of Nuclear Reactor Safety, GA-A-14568, General Atomic Co., San Diego, California 1978.

Fussel, J.B., "Fault Tree Analysis- Concepts and Techniques.", Generic Techniques in System Reliability Assessment, P. 133-162, Noordhoff-Leyden, 1976.

Gibson, s.b., chemical engineering progress, 76(11), 1980.

Guldner, W., Polke, H., and Zipf, G., "Computer Code Package RALLY for the Probalistic Safety Assessment of Large Technical Systems", GRS-57, Gesellschaft fur Reaktorsicherheit, Cologne, 1984.

Hammersley, J.M. and Handscomb, D.C., "Monte Carlo

Methods", Methuen, London, 1975.

Hauptmanns, U., "Fault tree analysis of a propsed ethylene vaporisation unit", I & EC Fundam., 19(3), 300, 1980.

Hauptmanns, and Sastre, H., "Safety analysis of a plant for the production of vinyl acetate", J. Chem. Eng. Jpn., 17(2), 165, 1984.

Hauptmanns, U., Yellera, J., and Sastre, H., "Safety analysis for the ammonia-air Mixing system of a plant for the production of nitric acid", J. Chem. Eng. Jpn., 15(4), 286, 1982.

Hauptmanns, U., Yellera, J., "Fault tree evaluation by Monte Carlo simulation", Chem. Eng., p.91, January 1983.

Hawksley, J.L. and Grollier-Baron, R., "Some Aspects of Risk Management in the Petrochemical and Process Industry", Safety and Reliability Objectives in High Technology and Industry, Hotel Okura, Amsterdam, 2/3 March 1989.

Helmers, E.N. and Schaller, L.C., Plant/Operation Progress, Vol.1, No.3, 1982.

Holden, P.L., "Development in Risk Assessment and its Applications in Process Plant Safety Studies", The Institution of Chemical Engineers, EFCE Publication Series

No. 42. pp.263-272. (UMIST) Manchester, 22-24 April 1985.

Homke, P., Krause, H.W., Ropers, W., Verstegen, C., Schlenker, H.V., Huren, H., Dorre, D., and Tsekouras, A., "Zerverlassigkeitskenngroßenermittlung im Kernkraftwerk Biblis - Abschlußbericht", Rep. no. GRS-A-1030, Gesellschaft fur Reaktorisicherheit, Cologne, 1984.

Huchingson, R.D., "New Horizon for Human Factors in Design", McGraw-Hill Book Company, New York, N.Y., 1981.

"Instantaneous Fractional Annual Loss-Process Factor Algorithm for Petrochemicals.", Insurance Technical Bureau, 1979.

King, R. and Majid, J., "industrial Hazard and Safety Handbook", Butterworths, London, 1979.

King, C.F. & Rodd, D.F. "Design and maintenance of failure tolerant process" A.I. Chem. E. Journal Vol.18, p.257, 1983.

King, C.F & Rudd, D.F, "Design and maintenance of economically failure tolerant processes" AIChE Journal vol.18, No.2, p.257-269, Mar. 1972.

Kletz, T.A., "Plant instruments: which ones don't work and why", Chem. Eng. Progr., 76(7), 68, 1980.

Kletz, T. A., "HAZOP & HAZAN: Notes on the Identification and Assessment of Hazards", Loss Prevention, The Inst. of Chem. Eng., ISBN 0-85295-165-5, Rugby, U.K., 1983.

Knowlton, R.E., "An Introduction to Guide Word Hazard and Operability Studies", CSChE Conference, 1982.

Knowlton, R.E., "An Introduction to Creative Checklist Hazard and Operability Studies", CSChE Conference, 1982.

Knowlton, R.E. & Shipley, R.K., "A Guide to Hazard and Operability Studies.", Published by Chemical Industry Association, 1977.

Kumaomoto, H. and Henley, E.J., "Protective system hazard analysis", Ind. Eng. Chem. Fundam., 17(4), 274, 1978.

Lapp, S. & Powers, G.J "Computer assisted generation and analysis of fault trees", 2nd Int.Symp. on Loss Prevention and Safety Promotion in the Process Industries, p.VII-377-384, 1977.

Lawley, H.G., "Operability Studies and Hazard Analysis.", Chemical Engineering, Progress 70(4), P.45-56, April 1974.

Lawley, H.G., "Size Up Hazard This Way.", Hydrocarbon Processing, Vol 55, No. 4, April 1976.

Lawley, H.G, "Operability studies and hazard anallysis" Loss Prevention, vol.8 p.105, 1974.

Lawley, Chem. Eng. Process _Vol 18, No 5, P. 105-116, 1973.

Lees, F.P., "Loss Prevention in Process Industries.", P. 194, Butterworth & Co., 2nd Edition, 1983.

Lees, F.P., "The Hazard Warning Structure of Major Hazards.", Trans. I. Chem. E., Vol. 60, P. 211-221, 1982.

Lewis D.J., The Mond Fire Explosion And Toxicity Index _ A Development of The Dow Index Presented at the AICHeE Loss Prevention Symposium Houston, April 1979.

Lewis, D.J.,"The Application of the Mond Index to Plant Layout and Spacing Distances" Loss Prevention, Vol.13, p.20-26, 1980.

Lewis, D.J.,"The Mond Index - A Development of the Dow Index" The Appaisal and Measurement of Fire Safety, University of Edinburgh, June, 1980.

Lewis, D.J.,"Hazard Control and Major Hazards (Fire, Explosion, Toxic Release)", The Institution of Chemical Engineers, Loughborough University of Technology, 23-27 Jannuary 1989.

Lihou, D., "Fault Trees From Operability Studies.", University Of Aston, Sep. 1980.

Lygate, J.F., "An Evaluation Of Different Methods Of Hazard Analysis Based On A Study Of An Offshore Gas Compression System", PhD Thesis, Edinburgh University, 1983.

Martin-Solis, G.A., et al, "An Approach to Fault Tree Synthesis for Process Plants.", 2nd. Int. Symp. on Loss Prevention and Safety Promotion, Pv11, 367-375, 1977.

Martin-Solis, G.A., et al, "Fault Tree Synthesis for Design and Real Time Applications", Trans. IChem. E., Vol. 60, P. 14-25, 1982.

Munday, G. et al, "A Measure pf the Hazard of an Industrial Operation." 3rd International Symposium on Loss Prevention and Safety Promotion, Sep. 1980.

National aeronautics and space administration, "Instructions for Preparation of Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL).", NSTS 22206, October, 1986.

Neilsen, D.S.,"Use of cause-consequence charts in practical system analysis.", Atom. Energy Commn, Res. Est., Riso, Denmark, Rep.Riso-M-1743, 1974.

Nielsen, D.S., Platz, O. and Kongso, H.E, "Reliability Analysis of a Proposed Instrument Air System" RISO-M-1903, Riso Research Centre, Roskilde, Denmark, 1977.

Neilsen, D.S., Platz, O., and Runge, B., "A Cause-Consequence Chart for a Redundant Protection System", IEEE Transactions on Reliability, 1984.

Neilsen, D.S. and Runge, B., "Unreliability of a Standby System with Repair and Imperfect Switching", IEEE Transactions on Reliability, Vol. R-23, No.1, April 1974.

Pikaar, M.J. et al., "Process Safety Assessment of New and Existing Plants", 5th International Symposium on Loss Prevention and Safety Promotion, Cannes, September, 1986.

Pilz, V., "FTA: How Useful?" Hydrocarbon Processing, P. 275-283, May 1980.

Powers, G.J & Tompkins, F.C, "A synthesis strategy for fault trees in chemical processing systems" Loss Prevention, vol.8 p.91-99, 1974.

Powers, G.J & Tompkins, F.C, "Fault tree synthesis for chemical processes" AIChE Journal vol.20, No.2, p.376-387, Mar. 1974.

Powers, G.J & Tompkins, F.C, "Computer aided synthesis

of fault trees for complex processing sytems" Generic Techniques in System Reliability Assessment, Noordoff, p.307 314, 1976.

PRA Procedure Guide. "A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants", NUREG/CR-2300, Vol.1 and 2, U.S. Nuclear Regulatory Commission, Washington D.C, 1983.

"Procedure for Performing a Failure Mode, Effects and Criticality Analysis.", Dept. of Defence USA, MiL-STD-1629A, Nov. 1980.

"Procedures For Performing a Failure Mode and Effect Analysis", MIL-SDT-1629 A, Department of Navy, Washington DC 20362, 1977.

Prugh, R.W., "Apllication of Fault Tree Analysis.", Loss Prevention, Vol. 14, P. 1-9, 1980.

Sax, N.I., "Dangerous Properties of Industrial Materials", van Norstrand Reinhold, New York, 1984.

Shaeiwitz, J.A., Lapp, S.A, and Powers, G.J., "Fault tree analysis of sequential systems", Ind. Eng. Chem. Process Des. Dev., 16(4), 529, 1977.

Shipley, R.K., "The Efficient Use of Operability Studies.", Sep. 1980.

Skala, V., "Improving instruments service factors", Instrum. Technol., p.27, November 1974.

Solomon C.H., The Exxon Chemicals Methods for Identifying Potential Process Hazards. I.Chem.E. Loss Prevention Bulletin No. 52, Aug. 1983.

Swain, A.D. and Guttman, H.E., "Handbook on Human Reliability Analysis with Emphasis on Nuclear Plant Applications", NUREG/CR-1278, U.S. Nuclear Regulatory Commission, Washington, D.C., 1983.

Taylor, J.R. et al., "A Design Review Approach to Safety Analysis", 5th International Symposium on Loss Prevention and Safety Promotion, Cannes, September, 1986.

Taylor, J.R., "A Background to Risk Analysis", Vol. 1-4, Riso Research Centre, Roskilde, Denmark, 1979.

"Technical Manual for the Mond Fire and Explosion Index" ICI Mond Division, 1985.

Thomson, J.R. "Engineering Safety Assessment - An introduction", Longman Scientific and Technical, UK, 1987.

Tveit, O.S. et al, "risk Analysis of a Typical North Sea Production Platform.", Offshore Technology Conference 1980, Paper No. 3905.

US Departement of Defence, "Military Standard Procedure for Performing a Failure Mode, Effects and Critically Analysis", MiL-STD-1629A, Washington, D.C., Nov 1980.

U.S. Nuclear Regulatory Commission, Reactor Safety Study, "An Assessment of Accident Risk in U.S. Commercial Power Plants", WASH-1400, NRC, Washington, D.C., 1975.

Vesely, W.E., "Estimating common cause failure probabilities in reliability and risk analysis: Marshall-Olkin specialisations", in Nuclear Systems Reliability and Risk Assessment, Fussel, J.B. and Burdick, G.R., Eds., Society for Industrial and Applied Mathematics, Philadelpia, 1977.

Vinnem, J.E., "Definition, Quantification and Acceptance of Risk.", National Center of Reliability, NCSR R23, Vol. 2, P. 67-103, July 1980.

Watson, I.A., "Review of Human Factors in Reliability and Risk Assessment", The Institution of Chemical Engineers, EFCE Publication Series No. 42, pp.309-322, (UMIST) Manchester, 22-24 April 1985.

Whitehouse, H.B., "IFAL - A New Risk Analysis Tool" The Institution of Chemical Engineers, EFCE Publication Series No. 42, pp.309-322, (UMIST) Manchester, 22-24 April 1985.