# Assessment of safety systems using fault tree analysis

ISSN 0367-7850



# Assessment of safety systems using fault tree analysis

By J.M. Morgan, B.Sc., M.Sc., Ph.D., C.Eng., M.Inst.E. (Group Leader) and J.D. Andrews, B.Sc., Grad.I.M.A., F.S.S. (Senior Scientist), Controls Division, Midlands Research Station, Research and Development Division, British Gas Corporation

*Communication 1242*

50th Autumn Meeting, Congress Theatre, Compton Street, Eastbourne
Tuesday 13th and Wednesday 14th November 1984
President: W. L. Mercer, B.Sc., Ph.D., C.Eng., F.I.Gas E., F.I.M.

The Institution of Gas Engineers

Founded 1863
Royal Charter 1929
Patron
Her Majesty The Queen

# ASSESSMENT OF SAFETY SYSTEMS USING FAULT TREE ANALYSIS

By J.M. MORGAN, B.Sc, M.Sc, Ph.D, C.Eng, M.Inst.E.
(Group Leader)
J.D. ANDREWS, B.Sc, Grad IMA, FSS.
(Senior Scientist)
Midlands Research Station, British Gas Corporation.

Communication 1242

To be presented at the 50th Autumn Meeting,
Eastbourne, November 1984

CONTENTS



## 1. SUMMARY

The safe and reliable operation of process plant depends upon the correct functioning of control and protection systems. The performance of such systems has, in the past, generally been assessed through a combination of engineering judgement and historical experience. However, there are limitations with these conventional methods when dealing with novel or complex systems and more sophisticated techniques are required. Fault tree analysis is one such technique which can identify the failure modes of a system and predict the likelihood of unsafe or undesirable occurrences.

Fault tree analysis was originally developed and applied within

the aerospace industry. It has subsequently been used extensively in the nuclear industry and more recently for petrochemical and process applications. The capabilities of fault tree analysis and other related techniques have been evaluated to determine their potential application to control and protection systems employed within the gas industry.

This paper describes the manual and computer-aided techniques that have been investigated. The results of applying these techniques to examples of safety systems installed on British Gas facilities are presented. It is shown that computer-aided analysis can make a valuable contribution towards optimising the design and maintenance of safety systems.

## 2. INTRODUCTION

The excellent safety record which British Gas has established for its own facilities and for plant operated by gas consumers has been achieved through applying sound engineering judgement and taking note of historical experience. Codes of Practice and Standards have been written incorporating the wealth of knowledge within the gas industry and some have formed the basis of British Standards.

However, the conventional qualitative approach to engineering control or protection systems has several drawbacks. If a new concept in plant design is proposed, where there is no historical information, a guarantee cannot be given that all the faults resulting in unsafe failure are recognised. Similarly, for complex systems it is often difficult to assess the safety and reliability through the use of engineering judgement alone. Therefore considerable opportunity exists for the application of techniques which can identify failure modes and quantify the reliability and availability of a system. Fault tree analysis is a technique which can provide this information and, as such, it can make a valuable contribution to safety.

Before the 1940's improvements in the reliability of control and instrumentation systems were generally the result of trial and error. When a system or component failed it was rebuilt using any improvement in technology which may have taken place since its initial construction together with information learned from the mode of failure of the original. As with many other technologies, it was World War II which led to advances in the field of reliability and gave rise to the development of the first mathematical models. These models, although very simple, were applied first in Germany to the V.1. missile, after the first batch of ten either blew up on the launching pad or fell into the English Channel. Efforts to improve reliability at this time were focussed extensively at producing better quality components.

Over the next twenty years advances in the aerospace and nuclear industries accelerated the development of reliability techniques and the specialised application areas grew wider. The need for

success was further increased during the development of Intercontinental Ballistic Missiles and the subsequent Mercury and Gemini rocket programmes. Indeed it was the Minuteman missile project which gave rise to the concept of fault tree analysis.

The 1970's saw great strides in the application of these techniques. Professor Rasmussen led a team of people which produced the "Wash 1400 Reactor Safety Study", covering a wide range of potential nuclear accidents. This type of study, although very costly, became widely adopted by chemical and other industries throughout the world.

The work presented relates to the application of fault tree analysis and an associated technique known as cause-consequence analysis to examples of control and protection systems used in the gas industry. The potential benefits of applying these techniques, in particular through the use of computer programs, is considered.

The basis of fault tree analysis is explained in Section 3, with a description of the computer programs which have been used. An application of the technique to part of a fire protection system is presented in Section 4. Cause-consequence analysis is particularly suitable for examining sequentially operating systems and a study of an automatic flue damper assembly is given in Section 5, together with a description of the technique. Finally, work being carried out on a computer program which automatically constructs fault trees is presented in Section 6.

## 3. FAULT TREE ANALYSIS

Fault tree analysis is a method for determining the causes of an undesired event. Graphically, the undesired event represents the top of a tree whose branches will be developed downward. Once the undesired event (often called a top event) is specified, it is necessary to identify the immediate causes which directly contribute to it. Each of these causes must be further broken down into preceding causes. This process is continued until every cause of the undesired event is traced.

The objectives of a fault tree analysis can be summarised as follows:

a) to demonstrate to designers and operators how a system can fail and what effect modifications can have.

b) to identify failure modes in order to highlight the key components in a system.

c) to examine the failure modes in terms of basic causes in order to identify common links which could reduce system reliability.

d) to express the occurrence of the undesired event in terms of its probability or frequency. This can be used to provide a

relative measure of improvement that would result from design changes.

A good introduction to the concepts associated with fault tree analysis is provided by Henley and Kumamoto[1].

## 3.1 FAULT TREE CONCEPTS

In order that a full appreciation can be achieved of the fault tree analysis presented in Section 4, a number of concepts associated with the technique are briefly described.

### The basic fault tree

The best way to illustrate the method of fault tree construction is to consider a simple example. A circuit consisting of a lamp, a battery and three switches in series is shown in Figure 1(a). The desired event is that the light comes on when all three switches are closed. If we consider what could prevent the light from working, we see that this would happen if any one of the three switch contacts were broken. This is represented in a logical manner in the fault tree by an OR gate with three input

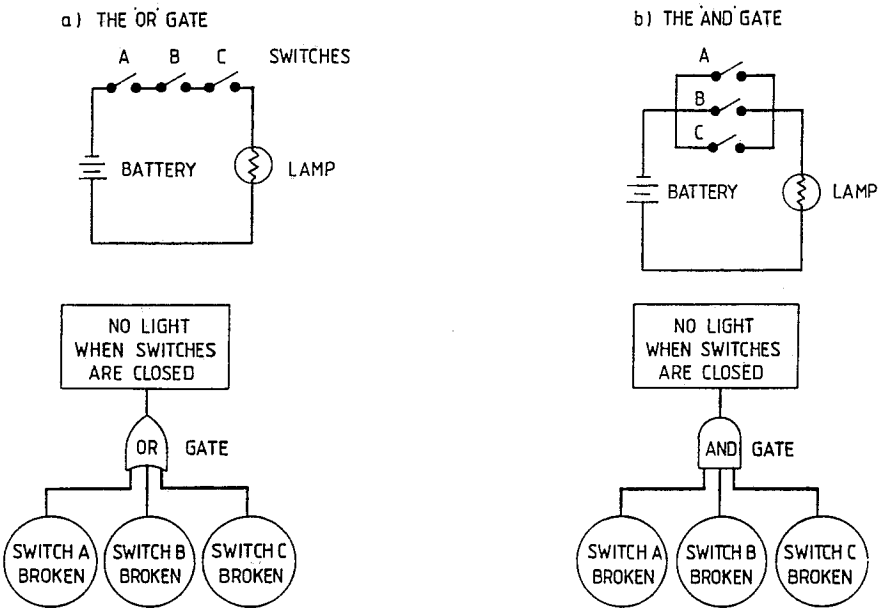



FIG. 1 THE BASIC STRUCTURE OF FAULT TREES

events. If the individual probability of each switch contact being broken is known, then the probability of having no light is approximately the addition of each of the probabilities.

When the three switches are placed in parallel, as shown in Figure 1(b), all of the three switch contacts would have to be broken for there to be no light. This is represented in a fault tree by an AND gate again having three input events. This time the probability of having no light is obtained by multiplying the individual probabilities. Fault trees are built up using a series of OR gates and AND gates, where the OR gates have the effect of increasing the number of individual failures which contribute to the undesired event, whereas the AND gates increases the number of combined failures that are necessary.

Revealed and unrevealed failures

If it is immediately apparent when a failure occurs, such as a light failing when in use, the failure is termed revealed. Conversely, if a failure remains unnoticed, it is termed unrevealed. For example, if a light had not been used for some time, during which a fault had developed, this would be an unrevealed failure. No remedial action can be taken to repair unrevealed failures until they are discovered, either during maintenance, or when there is a need for the system containing the failure to operate.

Unrevealed failures play a significant part in reducing the safety of control and protection systems, particularly those operating in a dormant or standby condition, or where redundancy is employed. Therefore, it is essential that they are identified during the design stage and, where possible, design changes made to eliminate them. Where it is not possible to eliminate unrevealed failures during design, their existance should be identified during maintenance or testing.

Common mode failure

A common mode failure occurs when a condition or an event causes the simultaneous failure of two or more components. For example, consider a system which has two identical components in parallel. It might be assumed that the extra redundancy built into this system in comparison with a single component system would mean that it was more reliable. This would be true if the components failed independently of each other. However, this would not be so if the component failures were not independent and had a common cause, such as failure of a common power supply or identical manufacturing faults. Then the system with two components would be no better with respect to the common failure than the single component system.

In practice, the presence of common mode failures usually set an upper limit on the reliability or availability of a system, by negating levels of redundancy which might apparently be present. Analysis of common mode failure would then give some indication as to where redundancy should stop and where perhaps more reliable components should be used, or more frequent maintenance performed.

Availability and reliability

A control or protection system is designed to perform certain functions and its ability to do so can be expressed in terms of its availability or its reliability. The concepts of availability and reliability are best explained in terms of an example involving an aircraft flight. Whether the plane passes all the checks before takeoff is a matter of availability. Once it is in flight, whether the plane can fly to its destination is a question of reliability.

System availability is defined as the probability that the system works on demand. Conversly system unavailability is the probability that the system is in a failed state when a demand is placed on it. To calculate system unavailability we are interested in failures which contribute to the downtime of the system.

When we consider system reliability it is failures which cause the working system to make a transition from the normal working state in to the failed state which are of interest. In this context system unreliability is the probability of one or more system failures occurring over an interval of time.

## 3.2 FAULT TREE EVALUATION

Once a fault tree has been constructed two types of information can be determined. Firstly, the various combinations of component failure which can lead to system failure can be obtained. Secondly, the likelihood of system failure can be calculated, if component failure rates, repair times and maintenance periods are known.

A fault tree analysis can absorb a great deal of effort, as was shown by the "Wash 1400 Reactor Safety Study"[2], where it was estimated that over the duration of the work, 25 years of man effort was expended. In order to minimize the amount of effort involved it is standard practice to use computer programs to produce the qualitative and quantitative results. As this stage of the analysis involves procedures which are defined by formal mathematical rules, it is ideally suited for computer implementation.

Three programs for fault tree evaluation have been used for the presented work; FTAP[3], IMPORTANCE[4] and FAUNET[5]. The two programs, FTAP and IMPORTANCE, are usually run together, FTAP providing the component failure combinations which cause the undesired event and IMPORTANCE quantifying and ranking these results. The main feature of IMPORTANCE is that it will compute the relative contribution to system failure of individual failures and failure combinations. These importance measures can be used to test the sensitivity of the system to specific failures and highlight areas in which improvement in design can be made. Such information is of great value in identifying the critical failure as it is virtually impossible with most fault tree analyses to visually inspect all the failure combinations to make an assessment of their relative contribution to system failure.

FAUNET is a fault tree evaluation program developed to run efficiently on small mini computers. The program is initially used to determine failure combinations. Subsequently, quantitative results can also be calculated for either system availability or reliability. A recent development by the authors is an interface program which converts fault trees created by the automatic fault tree construction program RIKKE[6], described in Section 6, into the correct format for FAUNET. This opens up the possibility of completely automating the analysis in the future.

To illustrate the techniques described above, a fault tree analysis is presented, in the following section, of an LNG spill detection system.

## 4. FAULT TREE ANALYSIS OF AN LNG SPILL DETECTION SYSTEM

### 4.1 THE FIRE PROTECTION SYSTEM

British Gas has a number of Liquid Natural Gas (LNG) storage facilities to help ensure that when there is an exceptionally high demand for natural gas, such as during a cold winter, the supply can be maintained. The cryogenic LNG is stored in tanks, surrounded by bunds to control the spread of LNG in the unlikely event of a loss of containment. At the facility where the study was carried out, if ignition of a spillage from one tank should occur, water deluge systems are incorporated to cool the remaining tanks for the duration of the resultant fire, as shown in Figure 2. The water deluge systems are initiated by the operator immediately a spill of LNG is detected rather than waiting for a fire to develop. At the same time electrical power to the affected tank is automatically isolated to remove ignition

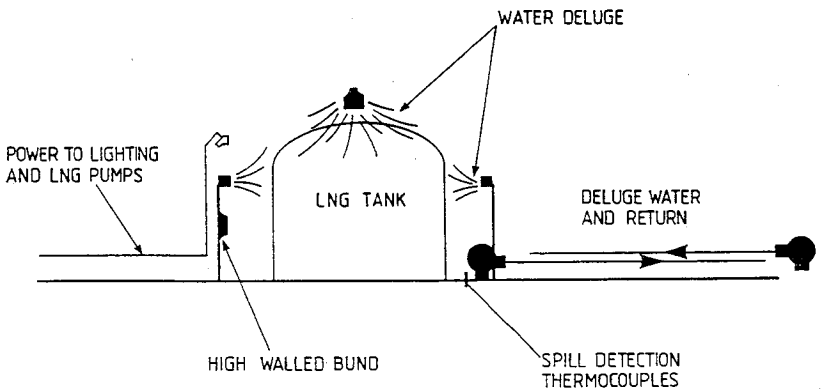



FIG. 2 MAIN FEATURES OF THE FIRE PROTECTION SYSTEM

sources and its own water deluge system is inhibited to avoid deluging the LNG in the bund, which would increase the evaporation rate.

A schematic diagram of the fire protection system is shown in Figure 3. Initially the requirement of the fire protection system is one of availability in the event of a spillage of LNG. It is essential that the operational sequence is performed correctly and rapidly. Following this the requirement is one of reliability, where the deluge has to be maintained until the situation is made safe. In the event of a fire this could be as long as 24 hours.

A fault tree analysis was carried out on the LNG spill detection system, which forms part of the fire protection system, to determine the benefits of applying the technique to a complex system and to establish the practical problems associated with such an exercise. In order to highlight the strengths of the techniques, the results of the analysis were used to redesign the existing detection system and a second analysis was performed. The results of both studies were then compared in order to establish whether any improvement in performance might be expected if the design changes were implemented. Studies of fire protection systems carried out at Lawrence Livermore National Laboratory[7] provided valuable guidelines for the work described.

## 4.2 THE SPILL DETECTION SYSTEM

A schematic diagram of the main elements of the spill detection system is shown in Figure 4, where it can be seen that there are four thermocouples installed at the base of each tank. Each thermocouple is connected to a fire resistant cable which passes over the bund wall and then to underground cables which are routed back to the control room. A signal processor provides an output from each of the four thermocouples, in the event of a spillage of LNG being detected. The output signals from two of the thermocouples illuminate separate lamps on a mimic panel, warning the operator that a spillage has occurred. An output from either of the two remaining thermocouples isolates all electrical supplies to the affected tank, deactives the circuitry which enables the operator to deluge that particular tank and illuminates a single lamp on the mimic panel. A signal from any of the four thermocouples will operate a siren in the control room.

If the detection system is to operate successfully when a spillage occurs, it must therefore perform a total of six functions. Three lamps should be illuminated on the mimic panel, power should be isolated to the affected tank, the deluge to the same tank should be inhibited and finally a siren should be activated in the control room.

## 4.3 THE ANALYSIS

To construct a fault tree, it is first necessary to establish the undesired (top) event. Studies of human error have shown that an operator who is usually very reliable in executing his normal duties has an extremely high probability of making a mistake

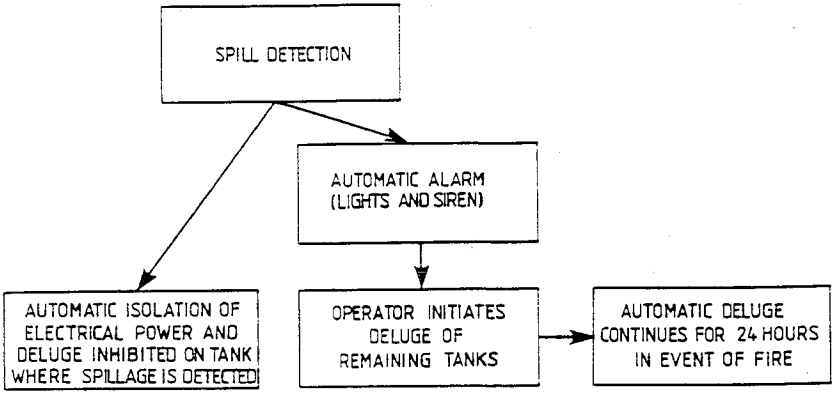



FIG. 3 SCHEMATIC DIAGRAM OF THE FIRE PROTECTION SYSTEM

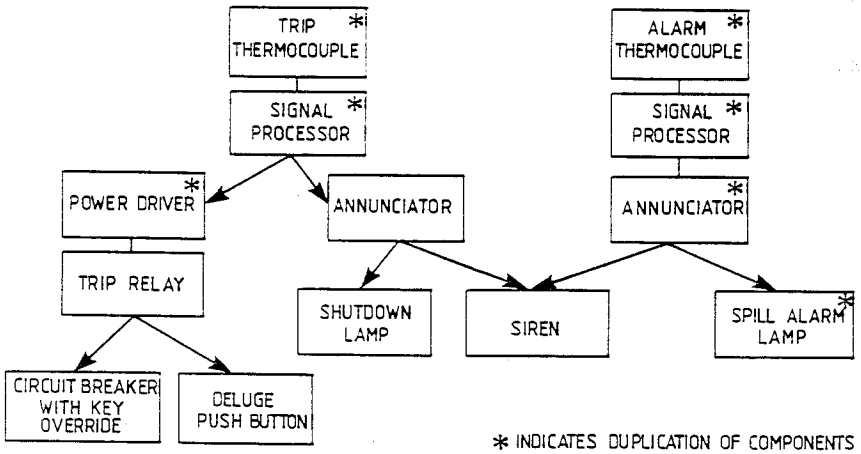



FIG. 4 EXISTING SPILL DETECTION SYSTEM

under pressure. This is when he is given the correct information on which to act. It is therefore highly undesirable to present the operator with conflicting information which requires him to assess which part of the system is malfunctioning. Consequently failure of any of the six system functions was chosen as the undesired event. This resulted in a basic fault tree with six main failure branches, shown in Figure 5. Some failures will, of course, be more important than others, but each degrades the spill detection system in some way.

The spill detection system is in a dormant condition while the integrity of the LNG tank is maintained and must be ready to operate if a spillage of LNG occurs. As such it was the failures which contributed to the downtime or unavailability of the system which were of interest. These failures were split into two groups, failures which were immediately revealed, causing downtime for repairs and failures which remained unrevealed, degrading the system until routine maintenance rectified the faults.

Fault trees were drawn for the six failure branches for both unrevealed and revealed failures. If we consider, for example, the unrevealed failures for one of the warning lights, Figure 6, it can be seen that one cause is the bulb failing on the mimic panel. Following the signal path further into the instrumentation system, the next cause is failure of the annunciators. In this manner all the causes of unrevealed failure were traced until, finally, failure of the thermocouples was considered. In a similar manner revealed failures, which would cause the light to spuriously illuminate when there had not been a spillage of LNG, were traced.

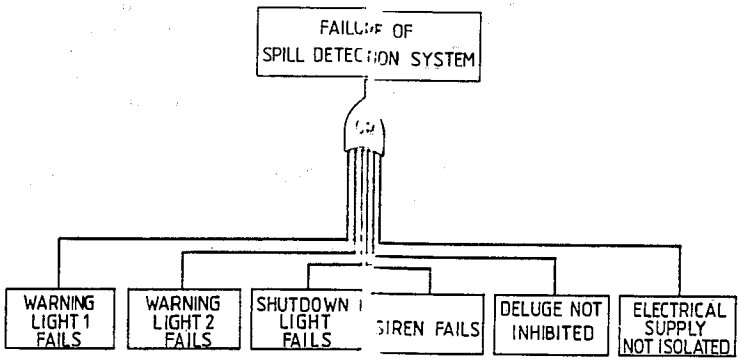



FIG. 5 FAULT TREE STRUCTURE FOR EXISTING SYSTEM

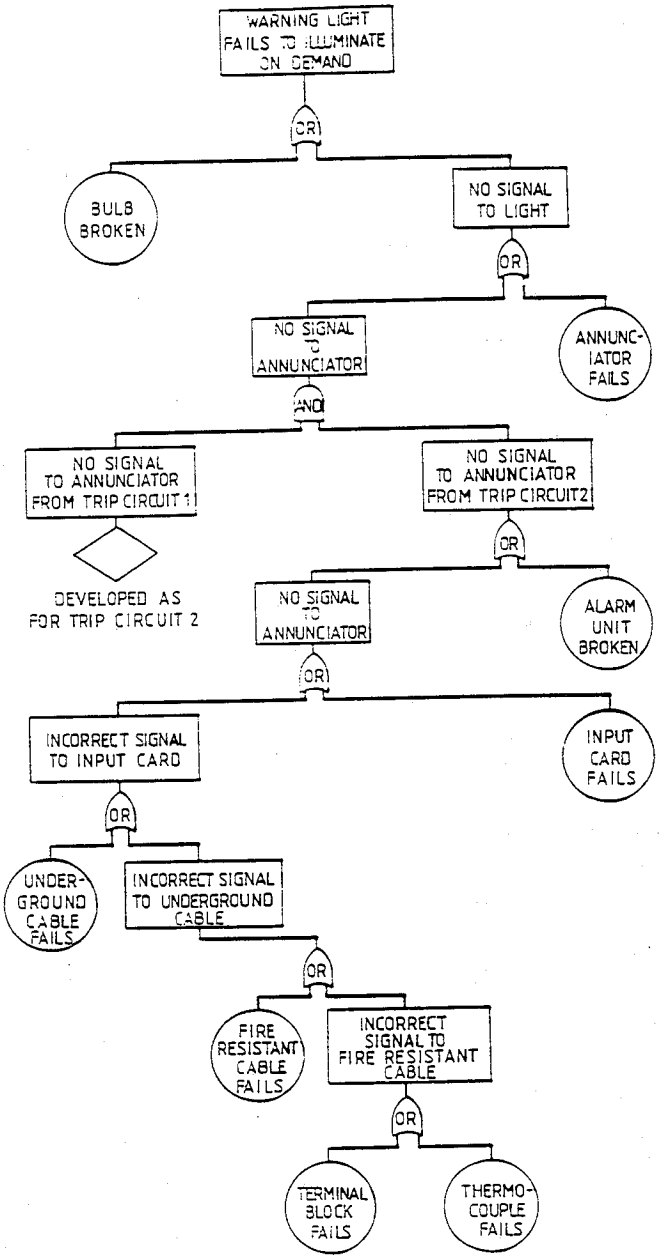



FIG. 6 SECTION OF FAULT TREE FOR THE EXISTING SYSTEM

Having produced the complete fault tree, the next step was to obtain the qualitative information indicating which individual failures and combinations of failures could prevent the correct operation of the spill detection system. All the fault trees produced were evaluated using FTAP and FAUNET, described in section 3.2. For the existing spill detection system, 41 single failures, 102 combinations of two failures and 1 combination of three failures were identified as being capable of causing the system to fail in an unrevealed way. This shows a lack of redundancy in some areas and although only a qualitative guide, the knowledge of failure combinations indicates the degree of security which exists. There were also 59 single component failures which would cause the system to fail in a revealed manner. Revealed failures are not in general as critical as unrevealed failures, but the integrity of the detection system will be downgraded while repair is carried out.

The next step was to consider the quantitative evaluation of the fault trees to determine the availability of the detection system in the event of a spillage of LNG occurring. To accomplish this, data was required on the failure probabilities of the individual components included on the fault trees. Several data sources were used for the study, the main two being the WASH-1400 report[2] and the UKAEA System Reliability Service Data Bank[8]. It is important that exactly the correct failure modes are considered in the context of the system being examined. For example, relays can fail in the energised state or the de-energised state and have different failure probabilities accordingly.

A good knowledge of maintenance schedules and repair procedures is also very important, as failures that are not revealed on occurrence, will degrade the spill detection system for as long as they persist. These unrevealed failures will only be noticed during maintenance or when there is a demand on the system, which is then too late. Also, if it is the intention that maintenance should indicate failure of individual components, each component must be checked. It is not sufficient merely to check the overall function of the system, if there is some redundancy, as such checks will not reveal its loss.

The time taken to repair components which have failed is another important feature which has to be considered in the analysis, as the spill detection system will be unavailable or downgraded during the period in which repair is made. In practice, repair times will depend on the presence of maintenance personnel and on the stocks of spare components. Poor repair procedures and a lack of spare components can severely reduce availability.

## 4.4 THE RESULTS

A summary of the main results for the existing spill detection system is given in Table 1. The predicted likelihood that total failure of the spill detection system would occur in the event of a spillage of LNG was only 0.5%. In this case there would be no warning to the operator, power would remain on the affected tank and the deluge to the same tank would not be inhibited. In comparison, the likelihood that some single function would fail to operate was approximately 47%. This figure appears high, but

TABLE 1: QUANTITATIVE RESULTS FOR FAULT TREE ANALYSIS OF SPILL DETECTION SYSTEM

| OUTCOME | MAINTENANCE INTERNAL | PROBABILITY OF OUTCOME (UPON DEMAND) EXISTING SYSTEM | REDESIGN SYSTEM |
|---|---|---|---|
| Failure of complete system | 6 months | 0.5% | 0.4% |
| Failure of any one function | 6 months | 47% | 5% |
| Annunciators function but deluge not inhibited and electrical supply not isolated | 6 months | 3% | Not possible |
| Spurious operation of system due to revealed faults | Mean time for system repair 18 hours | 1% | 1% |

it must be borne in mind that many of the failures may be regarded as trivial, such as one of the three lamps on the mimic panel not working. In this case it is unlikely that the operator will fail to initiate the deluge to the remaining tanks. Failure of from two to five of the functions had a likelihood of between 0.5% and 47% of occurring. For example, there was a probability of 3% that the annunciators would function in the event of a spillage, but the electrical supply to the tank would not be isolated and the deluge would not be inhibited.

Revealed failures, although readily noticed, do contribute to system unavailability, as when the fault is being repaired the system is not fully operational. If the assumption is made that revealed failures can be repaired in 18 hours, then there was a probability of approximately 1% that some function would be under repair when there was a demand for the spill detection system to work. The overall likelihood of a single failure being present then became 48%, being the addition of unrevealed faults and revealed faults.

## 4.5 DESIGN CHANGES

One of the strengths of fault tree analysis is that once a study has been performed, the results can be used to assist with improving the design. Subsequently, if a second analysis is then carried out, a comparison between designs can determine the extent of any improvements. The following design changes were proposed for the spill detection system and a second fault tree analysis carried out. The redesigned system is shown in Figure 7.

1. The four spill detection circuits have the same function, to isolate power to the tank, inhibit the deluge and annunciate this to the operator.
2. The operational logic to the power driver is reversed so that loss of power becomes a revealed failure.

3. The action of the circuit breaker in isolating power to the tanks must be accomplished before the relevant light can illuminate on the mimic panel. Indication by inference is not acceptable.

4. Only two indicator lamps are present, one lamp to indicate that a spill has been detected and the other lamp to indicate that the electrical supply to the tank has been isolated and the deluge inhibited. This should avoid confusion and combined with recommendation 3 give the operator clear and accurate information.

5. Two bulbs are provided in each lampholder on the mimic panel, providing extra redundancy at minimal cost.

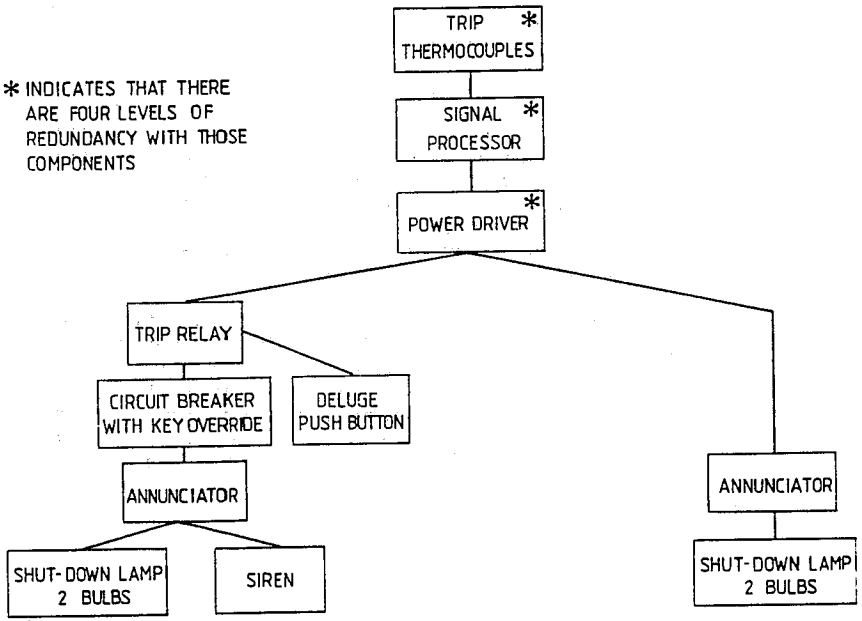



FIG. 7 MAIN FEATURES OF REDESIGNED SPILL DETECTION SYSTEM

## 4.6 A COMPARISON OF DESIGNS

The fault tree analysis for the redesigned spill detection system followed an identical procedure to that carried out for the existing system. The undesired event was again that of the spill detection system failing on demand. As before, the tree breaks down to unrevealed failures and failures giving revealed faults or spurious operation of the system. The only difference is that only two lamps are present on the mimic panel, compared with three on the existing system, giving a total of five functions instead of six.

For the redesigned system, again using the computer programs FTAP and FAUNET, it was found that 20 single failures, 3 combinations of two failures and 6561 combinations of four failures could cause the system to fail in some way. It is worth noting that the large reduction in single and double failures that contribute to the system failure, indicates a marked improvement in design. Too much concern should not be placed on the large number of four failure combinations, as in fact individually they are extremely unlikely to occur. The aim of a study such as this is to reduce the number of low order failure combinations (i.e. single and double) which cause system failure. An increase in the number of higher order failures combinations is acceptable if, as in this case, the overall availability is increased.

A summary of the results of the quantitative analysis for the redesigned system is given in Table 1 along with the corresponding results for the existing system for comparison. A modest reduction from 0.5% to 0.4% in the likelihood that the whole spill detection system would fail on demand was predicted. However, there was a significant decrease from 47% to 5% in the likelihood that any one of the function would fail to work when required. Also, for the redesigned system, it was not possible to indicate to the operator that the deluge had been inhibited and power had been isolated to the affected tank if this had not occurred. Finally, the probability that part of the system would be unavailable due to revealed failures causing spurious operation, remained at approximately 1%.

One of the strengths of quantitative fault tree analysis is that the effects of varying maintenance schedules can be predicted. It was originally assumed that the spill detection system was maintained every six months. In this case, the predicted availability of the existing and redesigned systems was 52% and 94% respectively, as is shown in Table 2. Monthly maintenance on the whole system increased this availability to 90% and 98% respectively, but such regular checking of every component in the spill detection system would probably be impractical. However, by examining the results from the computer program IMPORTANCE, it was seen that the annunciation system represented a significant contribution to system failure. It was considered that a weekly check on the full annunciation system, including the siren and the lights, could improve system performance without the need for major installation changes; the maintenance on the rest of the system remaining at six month intervals. This resulted in the predicted availability increasing to 54% and 98% respectively. The increase in availability was most significant for the

TABLE 2 : EFFECT OF MAINTENANCE CHANGES FOR THE SPILL DETECTION SYSTEM

| FAILURE TYPE | MAINTENANCE INTERVAL | AVAILABILITY EXISTING SYSTEM | AVAILABILITY REDESIGN SYSTEM |
|---|---|---|---|
| Failure of any one system function | 6 months | 52% | 94% |
| Failure of any one system function | 1 months | 90% | 98% |
| Failure of any one system function | weekly checks on annunciation system 6 months on rest of system | 54% | 98% |

redesigned system producing a figure as high as that predicted through monthly maintenance on the whole system. However, unlike checking all the components monthly, a weekly check on only the annunciation system, which could be carried out by installing a push button on the mimic panel, was though to be a practical proposition. It is interesting to note that the probability of failure of any part of the redesigned system, ie 2%, was divided equally between revealed and unrevealed failures.

As a result of this study, a decision has been made to carry out the proposed modifications to the existing spill detection systems and change the maintenance schedules accordingly.

## 5. CAUSE-CONSEQUENCE ANALYSIS

### 5.1 DESCRIPTION OF THE TECHNIQUE

There are a large number of potential applications for quantitative safety analysis which relate to sequentially operating systems. Of particular interest is the safe start up and shut down of gas fired plant. Unfortunately, fault tree analysis alone is not suitable for examining sequential systems, or those incorporating temporal effects, as it can only represent failures in one phase of operation or at one instant in time. For example, it would not be possible to draw a single fault tree covering all the possible failures during the start up of a burner control system. This is because components such as valves may be correctly in the open state at one sequence step, but not in another and so one failure mode cannot be used to cover the whole startup.

To overcome this problem a technique known as cause-consequence analysis was developed at the RISØ National Laboratory, Denmark[9]. Effectively, a cause-consequence analysis involves the construction of a diagram which traces the logical sequence of operation of a system. Each step is represented by a decision box and both the correct and incorrect outcomes are subsequently developed. In this way a diagram is produced with the one correct sequence of operation and all the possible sequences which result from faults occurring in the system.

The approach of cause-consequence analysis is best explained through its application to a simple problem. A circuit consisting of a lamp, battery and switch in series is shown in Figure 8, together with a cause-consequence diagram representing the various possible outcomes which could occur when the switch is closed. The diagram follows the sequence of events from closing the switch to obtaining light. Decision boxes allow causes of correct and incorrect operation to be introduced and all the consequences that result. In this way, a complete step by step picture is produced of the sequence of lighting the lamp and all fault sequences that could occur. If the probabilities of the various outcomes at decision boxes are known then the likelihood of all the outcomes can be calculated. Fault trees can be used to determine failure probabilities at each decision box as only one phase of operation is being considered at a time.

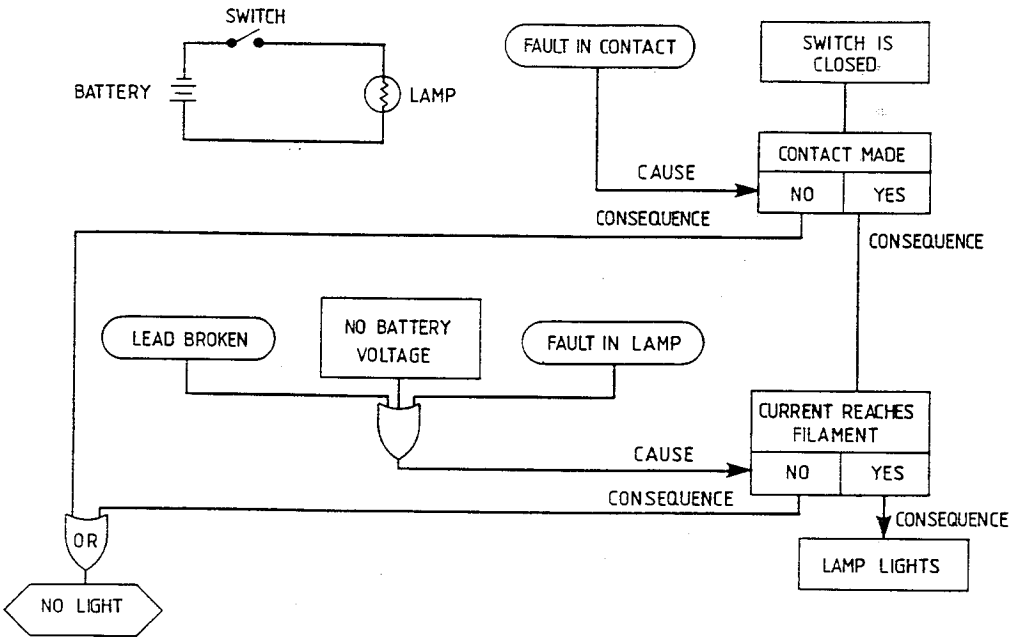


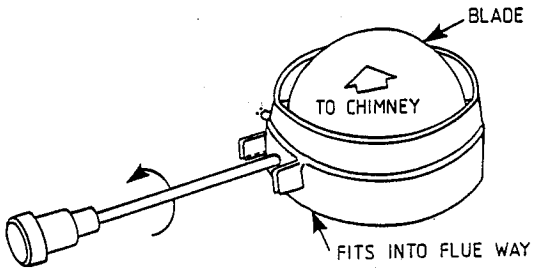

FIG. 8 A SIMPLE EXAMPLE SHOWING THE STRUCTURE OF A CAUSE - CONSEQUENCE DIAGRAM

## 5.2 APPLICATION TO AN AUTOMATIC FLUE DAMPER ASSEMBLY

Some 21 months ago British Gas published a standard, IM/19, on the use of automatic flue dampers on gas-fired space heating and water heating appliances[10]. The standard includes safety requirements for automatic flue dampers intended to prevent or restrict natural ventilation through the flue when the appliance is shutdown.

At the time when IM/19 was being formulated, there was little historical information available on the performance of automatic flue dampers. There was also particular concern about the potential hazard resulting from failure of the damper, to open when the associated burner system began to fire. It was recognised that a quantitative safety analysis could provide valuable information on the performance of damper assemblies.

a) THE FLUE DAMPER ASSEMBLY




b) THE FLUE DAMPER ELECTRICAL CIRCUIT

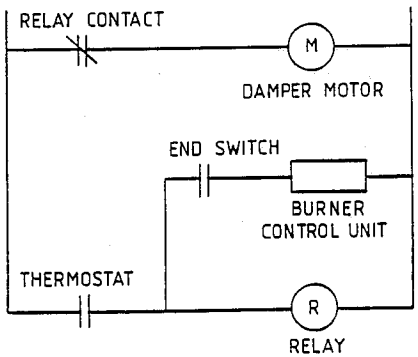



FIG. 9 THE FLUE DAMPER

Due to the sequential mode of operation, it was not possible to apply fault tree analysis alone to ascertain the reasons and likelihood that the damper could remain closed whilst the appliance fired. However, it appeared an ideal application for cause-consequence analysis; consequently a study was made.

The damper chosen for the study was based on a typical device sold in the USA. The aperture of the flue is controlled by a circular blade which rotates on a spindle, see Figure. 9 (a). The blade is spring loaded in such a way that it will normally assume a fully open position. An electric motor and gear train drive the damper blade closed. An end-switch is fitted which is designed to close when the damper blade is fully open. The control circuit for the damper is shown in Figure. 9 (b), with the contacts in the damper-closed, burner-off condition. The component in Figure. 9 (b) labelled 'burner control unit' represents the connection between the damper control circuit and the appliance. When power is applied the ignition sequence of the appliance can start.

The cause-consequence diagram for the start-up sequence of the burner is shown in Figure. 10. The first event is taken as "thermostat closes"as this event initiates the start-up sequence. The path leading to outcome 5 is the normal start-up sequence. All other outcomes represent failure conditions which divide into three categories; firstly, dangerous starts, where the ignition sequence of the appliance is allowed to start with the damper blade closed or in an unsafe position - outcomes 1, 4 and 9; secondly, where the damper control system prevents the ignition sequence of the appliance from starting - outcomes 2, 6, 7, 8 and 10; thirdly, "safe but incorrect" starts, where the damper and appliance operate properly although failures have occurred in the damper system - outcomes 3 and 11.

For the purpose of this study, it was assumed that the burner operated for 10,000 cycles per annum and the flue damper system was serviced at yearly intervals. Failure rate information for the components of the damper system was obtained from recognised data sources[2,8]. As might be expected, the cause-consequence analysis indicated a high probability for normal safe operations of the damper. However, the analysis also indicated a significant probability for "safe but incorrect" starts whereby an unrevealed failure of the end switch in the closed position degraded the safety, as it would always indicate an open damper. This situation would prevail until either the failure was detected during servicing or a further fault occurred; the latter generally leading to a dangerous start. An extra check ensuring that the end switch was open before start up could commence would have eliminated this problem (i.e. a safe start check).

The results also showed a probability of damper failure which would prevent the burner from firing. This would lead to a requirement for service and might encourage the customer to tamper with the control system in an effort to light the burner. It would be important that such faults are repaired properly as, in some cases, merely shorting out the end switch would appear to restore the system to working order. In fact, in this case the system would be considerably less safe than normal.

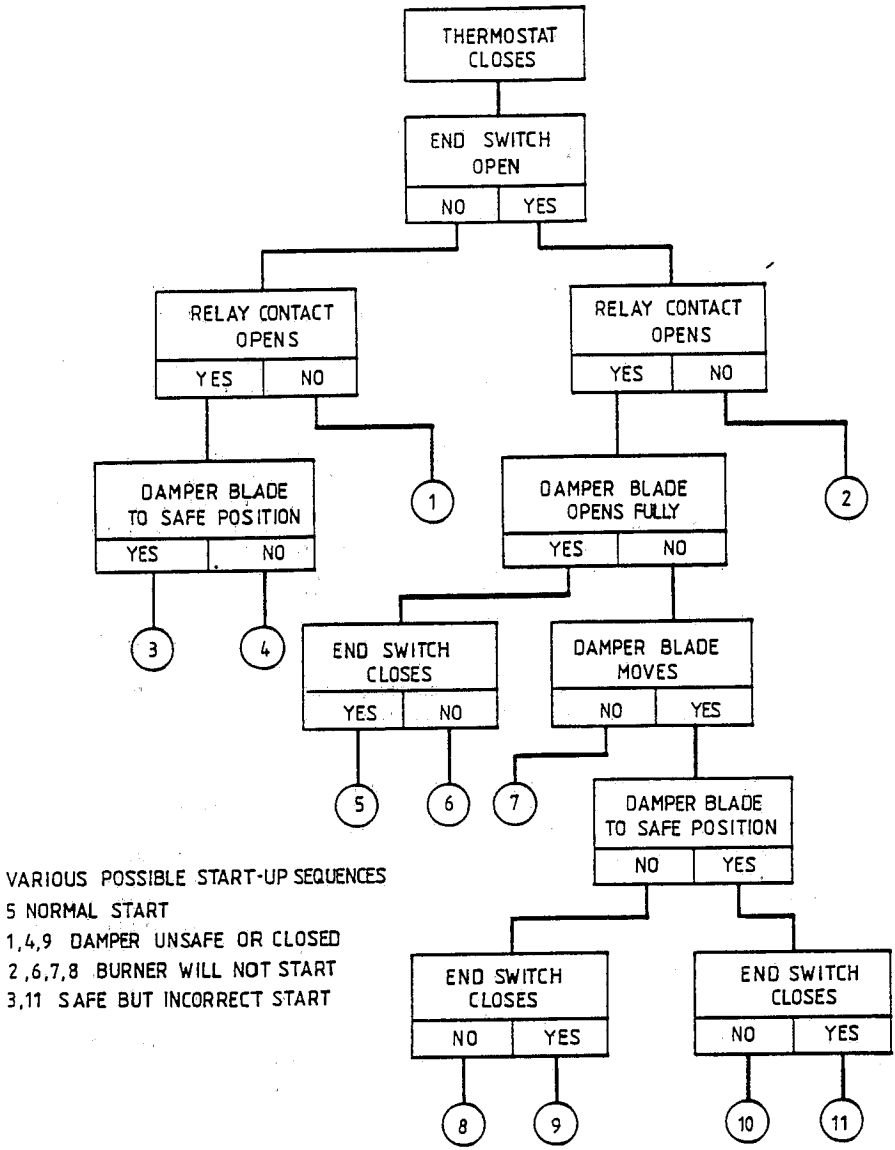



FIG. 10 CAUSE CONSEQUENCE DIAGRAM FOR START UP SEQUENCE OF AUTOMATIC FLUE DAMPER

The results of the study provided assistance to those concerned with formulating the standard for automatic flue dampers. In particular, the study clearly showed the importance of fitting an interlock to prove the damper blade in the fully open position prior to initiation of the burner ignition sequence and during the run period. It also showed that the predicted reduction in burner reliability through the introduction of the damper could produce an increased demand on servicing and could affect safety if tampering took place.

## 6. AUTOMATIC FAULT TREE CONSTRUCTION

Computer algorithms are now being developed which can automate the task of constructing fault trees. Many computer programs have been written to evaluate fault trees once they have been drawn manually, as the method used is based entirely on proven mathematical and statistical principles. Unfortunately this is not the case for programs which attempt to automatically contruct the fault trees as there is no one set of rules which can be applied in every situation to produce the correct tree. Two engineers analysing a complex system will probably produce trees with differences in their structure for the same undesired event, which when evaluated would produce identical results. With the added incentive provided by the amount of man effort required to produce fault trees manually and the desire to standardise the approach to construction, a number of groups have been involved in developing programs to automatically construct fault trees. These groups include Taylor and Olsen[6] (RISØ, Denmark), Andow and Lees[11] (Loughborough University) and Lapp and Powers[12] (Carnegie - Mellon Univeristy, Pittsburgh).

The capabilities of the RIKKE fault tree construction program, developed by Taylor and Olsen at the RISØ National Laboratories, Denmark, are being investigated. In order to use the RIKKE program, libraries containing component failure models must be created together with graphic symbols for each component in the system to be studied. The component failure models contain information which enables the computer program to construct fault trees for any failure associated with the system. Graphics symbols provide a unique diagramatic representation of each component and are used to build a picture of the system on an appropriate visual display unit. The complete system schematic diagram is entered into the computer by connecting the graphics symbols representing each component. When the complete system is entered, a plant failure model is automatically created which links all the component failure models. The engineer must then choose the undesired event and once this has been done, the program constructs the fault tree by abstracting the appropriate information from the plant failure model.

Work with the RIKKE program, initially concentrated on using the generalised component models developed at RISØ. However this often produced trees which were unrealistically large. Work is now in progress to produce component models specific to a number of gas industry applications. It has been found that RIKKE is

well suited to instrumentation systems, such as the spill detection system described in Section 4. The ON/OFF or binary switching logic often associated with the operation of instrumentation systems is readily translated into fault trees format. Work is continuing on building models for process applications, however, process variables, such as pressure and temperature, need to be divided into more classes than the simple on/off states mentioned above. For example, pressure may need to be represented as very low, low, normal, high and very high.

Modelling multivalued logic for process applications is currently in progress, but it could be some time before any significant success is achieved in this area.

## 7. CONCLUSIONS

The potential benefits which both fault tree and cause-consequence analysis offer have been demonstrated through the application of the techniques to control and protection systems.

The fault tree analysis of the spill detection system showed that it is possible to predict the likely performance of a complex instrumentation system. The computer programs FAUNET, FTAP and IMPORTANCE provided both qualitative information on failure combinations and quantitative information on availability. In particular, a knowledge of the relative importance of various component failures helped to identify areas where design changes could be effective. A second analysis allowed the extent of the improvement to be predicted. It was also possible to determine the additional improvements that would result from more frequent selective maintenance on certain components. This last feature is particularly attractive for plant where maintenance costs are high and large stocks of spares are kept for all components. It may be possible to reduce considerably the stocks for non critical components and ensure the availability of critical ones.

The cause-consequence analysis of the flue damper assembly demonstrated that it is possible to apply the technique to a sequentially operating system. It also showed that an indication of the safety and reliability which could be expected from new equipment can be obtained, even though historical information is not available. The fact that the installation of the damper assembly would probably provide more nuisance failures than dangerous failures is significant. Further work is necessary to widen the application of cause-consequence analysis and to this end computer simulation techniques are being investigated.

The application of techniques such as fault tree analysis is time consuming, requiring the effort of skilled engineers and, as such, it is a costly exercise. It is therefore essential to apply the techniques selectively. If a great deal of engineering expertise exists for a particular type of control or protection system and codes and standards are available, then there may be little benefit in applying fault tree analysis. Certainly, the

greatest return would be obtained when dealing with complex control and instrumentation systems, which need a high level of reliability or availability and where it is not readily apparent as to how cost effective improvements in performance can be achieved.

It is essential that the advantages which modern computing techniques offer are fully utilised, if the application of fault tree analysis and cause-consequence analysis is to become a practical proposition for wide spread use. Automatic fault trees construction is a subject which is receiving close attention. However, care must be taken not to overlook the main reason for performing a fault tree analysis. That is to gain an indepth understanding of the system being studied. As such, the manual approach allows an appreciation of both the technique being used and the system it is applied to. There is certainly a place for automatic fault tree construction programs, but it should not be used at the expense of the understanding which the manual approach offers.

The consequences of failure of large scale plants are such that high availability and reliability are necessary from the associated control and protection systems and fault tree analysis and other similar techniques have an important role to play at the design stage of such plant. Legislation may in the future require the use of such techniques, but regardless of this it is undoubtedly the cost effectiveness of their application which will increase their use.

## ACKNOWLEDGEMENTS

This paper is published by permission of British Gas. The authors would like to acknowledge and thank their colleagues in both Production and Supply Division and Marketing Division for the opportunity to apply the techniques described. Without their co-operation the work would not have been possible. In particular, thanks are due to Mr. C.A.J. Gregory, Plant Operations Department, who contributed much to the success of the fault tree application. Valuable assistance was provided by colleagues at London Research Station with running the fault tree evaluation programs FTAP and IMPORTANCE. Thanks are also due to Mr. G.R.Roberts and Mr. D.M.Johnson of Midlands Research Station who made significant contributions to the work.

## REFERENCES

1. HENLEY, E.J. and KUMAMOTO, H., Reliability Engineering and Risk Assessment, Prentice Hall Press, 1981.

2. RASMUSSEN, N.C., Reactor Safety Study : An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plant. U.S. Nuclear Regulator Commission. Report No. WASH-1400 (NUREG 75-014), October 1975.

3. WILLIE, R., Fault Tree Analysis Program (FTAP), Lawrence Livermore National Laboratory. Report No. UCRL - 73981, 1978.

4. LAMBERT, H.E., GILMAN, F., The IMPORTANCE Computer Code. Lawrence Livermoor Laboratory. Report No. UCRL-79269, 1977.

5. PLATZ, O., OLSEN, J.V., FAUNET - A Program Package for Evaluating Fault Trees and Networks. Report RISØ-348, 1976.

6. OLSEN, J.V., LIND, M. and TAYLOR, J.R., RIKKE - A Computer Program for Automatic Fault Tree, Cause-Consequence Diagram, Simulation and Model Construction. Report RISØ-N-28-78, May 1978.

7. HASEGAWA, H.K., Fire Protection Research for Energy Technology : FY80 Year End Report. Lawrence Livermore National Laboratory. Report No. UCRL-53179, May 1981.

8. UKAEA, Systems Reliability Service, Data Bank.

9. NIELSEN, D.S., The cause-consequence diagrams method as a basis for quantitative accident analysis. Atom. Energy Commn., Res. Est., RISØ, Denmark, Report RISØ-M-1374, 1971.

10. British Gas Standard IM/19, Automatic Flue Dampers for use with Gas Fired Space Heating and Water Heating Appliances, 1983.

11. MARTIN-SOLIS, G.A., ANDOW, P.K. and LEES, F.P., Fault Tree Synthesis for Design and Real Time Applications. Trans. I. Chem. E., Vol. 60, 1982.

12. LAPP, S.A., POWERS, G.J., Computer-Aided Synthesis of Fault Trees. IEE Transactions on Reliability, April 1977.

1242 Price £6.00

Discussions to this and other papers at the 50th Autumn Meeting will be published in a single volume



*Printing by Adlard & Son Ltd, Dorking, Surrey*