THE PROPAGATION OF FAULTS IN PROCESS PLANTS: A STATE OF THE ART REVIEW

P.K.Andow,* F.P.Lees* and C.P.Murphy*

The state of the art in the description of fault propagation in process plants is reviewed with respect both to design and to process control. Existing methods considered include failure modes and effects analysis, hazard and operability studies, fault trees, event trees and cause-consequence diagrams, and process computer alarm analysis. An outline is given of an approach to the creation of a general method of describing fault propagation in process plants, applicable both to design and to control.

INTRODUCTION

During the last decade the increasing concern with loss prevention has resulted in a much greater interest in methods of representation and investigation of faults and fault propagation in process plants (1). There is now quite a wide range of techniques available to the engineer. They include, for design, failure modes and effects analysis (FMEA), hazard and operability (hazop) studies; fault trees, event trees and cause-consequence diagrams; and, for process control, alarm analysis using a process computer.

The various techniques have been developed as solutions to the problems which arise at the different stages of plant design and operation.

It is the purpose of the present paper to draw attention to the fact that the existing techniques have common features and that the problem of fault propagation in process plants is a generic one. It is possible, therefore, to envisage a more general comprehensive and powerful method of representation and investigation of fault propagation in process plants. Effectively, the present generation of techniques would be subsets of this method.

The investigation of faults and fault propagation now involves a considerable amount of engineering effort. It is attractive, therefore, to develop a method which is economical of this effort.

* Department of Chemical Engineering, Loughborough University of Technology, Loughborough, Leicestershire. LE11 3TU.

EXISTING METHODS

Some of the principle existing methods of representing and investigating faults and fault propagation in a process plant are as follows:

Design

- Failure modes and effects analysis
- Hazard and operability studies
- Fault trees
- Event trees
- Cause-consequence diagrams

Process Control

- Process computer alarm analysis

Failure Modes and Effects Analysis

In a failure modes and effects analysis (FMEA) the failure modes of a component are listed and the effects of failure in these modes are developed in a tabular format. A typical entry might be

Component	Failure mode	Effect
Fuel oil flowmeter	reading low	High oil flow to furnace

Examples of failure modes and effects analysis have been given by Recht (2) and by King and Rudd (3).

Hazard and Operability (Hazop) Studies

There are various types of hazard and operability (hazop) study. Different types of study are suitable for different types of plant (continuous processes, batch processes, etc.).

In a hazard and operability study for a continuous plant the deviations of the various process variables (flow, level, pressure, temperature, concentration) are considered systematically and the causes and effects of these deviations are developed, again in a tabular format. Use is made of guide words applied to the process variable FLOW require respectively consideration of no flow, high flow and low flow. A typical entry in the table might be:

Guide Word	Deviation	Possible Causes	Possible consequences
NONE	No flow	1. Pump failure	1. Overheating and polymerisation in heat exchanger
		2. Pump suction filter blocked	2. Loss of feed to reactor
		3. Pump isolation valve closed.	

Examples of hazard and operability studies have been given by Lawley (4) and by Rushford (5).

A guide to the method has been published by the Chemical Industry Safety and Health Council (6).

Hazard and operability studies are finding increasing use, particularly in the U.K., in hazard identification in process plants.

Fault Trees

In a fault tree the fault event which is to be investigated is taken as the top event of the tree and the tree is developed in terms of the cause events and of the logical relations (gates) between these events. A typical fault tree is shown in Figure 1.

Alternative representations of the information given in the fault tree are

Truth tables
Boolean algebra

The truth table and Boolean algebra expressions for the fault tree shown in Figure 1 are also given in that figure.

There is a large number of fault trees illustrated in the literature, including examples given by Fussell (7), by Lawley (4) and by the Atomic Energy Commission (8).

Developments in fault tree methodology are described by Fussell, Barlow and Singpurwalla (9).

Fault trees are extensively used in hazard identification and assessment in process plants.

Event Trees

In an event tree the fault event which is to be investigated is taken as the bottom event of the tree and the tree is developed in terms of the consequence events and of the logical relations (vertices) between these events. A typical event tree is shown in Figure 2.

Examples of event trees have been given by von Alven (10), by the Atomic Energy Commission (8) and by the Health and Safety Executive (11).

Cause-Consequence Diagrams

In a cause-consequence diagram the fault event which is to be investigated is taken as the critical event and the diagram is developed in terms of the cause events and consequence events and of the logical relations (gates and vertices) between these events.

The cause-consequence diagram has a further feature which distinguishes it from conventional fault trees and event trees. This is that it takes into account the time of order of events, where this is significant.

A typical cause-consequence diagram is shown in Figure 3. The equivalent fault tree diagram is also shown in Figure 3, but it is emphasised that in a conventional fault tree the time order is not taken into account.

Examples of cause-consequence diagrams have been given by Nielsen (12) and by Taylor (13-14).

Cause-consequence diagrams are not yet widely used, but are likely to find increasing application for hazard identification and assessment in process plants.

Process Computer Alarm Analysis

The techniques for the analysis of fault propagation which have just been described have been developed for use in the design of process plants.

There is need also for techniques for the analysis of fault propagation in real time for use in control of process plants. Increasingly, process plants are controlled by a process computor. Normally one of the main functions of such a computer is to scan each process measurement to check whether it has gone outside its alarm limit into an alarm condition. On large complex plants it is possible for a considerable number of alarms to come up. It is then a difficult problem for the operator to sort the alarms into groups of associated alarms and to diagnose the basic fault in each group.

This problem is most acute in the nuclear industry. It is this industry, therefore, which has taken the lead in developing alarm analysis by process computer. Alarm analysis systems at the nuclear power stations at Oldbury and at Wylfa have been described by Paterson (15) and by Welbourne (16), respectively.

The alarm trees used in these alarm analysis programs differ somewhat from fault trees. Essentially, the structure is much looser and there is no predefined top event. The analysis is activated only when a series of alarms occurs in real time. The alarm tree is an essentially linear display of the series of alarms raised as the fault propagates through the plant.

In effect, such an alarm tree may be represented by an alarm network as illustrated in Figure 4. This network shows the interactions between the various alarms in the plant. Such a network may be used in real time to generate alarm trees of the type just described.

Examples of alarm trees have been given by Welbourne (16) and examples of alarm networks by Andow (17) and by Andow and Lees (18).

Process computer alarm analysis is used to some degree in the nuclear industry, particularly in the UK, but apart from one or two experiments does not appear to be used in process plants.

GENERIC FEATURES OF EXISTING METHODS

The behaviour of process plants is complex. Two aspects of this complexity are of particular importance in the present context: unsteady-state behaviour and fault conditions.

The engineering model which gives the most complete description of a plant is a full unsteady-state model covering both normal and fault conditions. Although some use is made of such models, particularly in the investigation of critical control systems, they are used less than some other techniques described. The reasons for this relate not only to the creation of the model but also to its use. The construction of a full unsteady -state model of a plant includes the formulation of a large number of algebraic and differential equations, the determination of large amounts of process data and the translation of data correlations into a form suitable for computer use and the writing of a computer program for the solution of these equations. This is a

major task, involving much time and effort. The magnitude of this task is much increased if the model has to take account of fault conditions as well as normal unsteady-state behaviour. But the problem does not end there. There is an infinite number of process and fault conditions for which the model may be interrogated. It is not easy to select the sets of conditions for which the model should be run.

It is not surprising, therefore, that alternative techniques have been developed. Most of these techniques involve a fairly drastic simplification of the inherently complex behaviour of process plants.

The fundamental simplification is the use of defined events and states. Process variables and fault conditions are intrinsically continuous, but for the purpose of the techniques they are treated as being a finite, and usually very limited, number of events/states such as:

Process variable	Flow	High /Normal/Low
Fault condition	Valve stickiness	Jammed open /Normal movement/ Jammed shut

The starting point for a particular technique is thus generally the occurrence of some undesirable event. The essence of the technique is that it describes the causes and/or consequences of this critical event, in other words the fault propagation. For the techniques described the critical event is as follows:

FMEA	Failure mode
Hazop studies	Deviation
Fault trees	Top event
Event trees	Bottom event
Cause-consequence diagrams	Critical event

The definition of events leads naturally to the linking of these events by simple logical relations such as the AND or OR gates which are the basic relations for fault trees.

These logical relations may be represented graphically. The familiar symbols for AND and OR gates are examples of such representation. But in addition there is a formal logic, namely Boolean algebra, which is available for the manipulation of these logical relations.

The development of a representation of fault propagation such as a fault tree is found to be not entirely straight-forward. A purely intuitive development may lead to contradictions such as the occurrence of event A in one part of the tree and the event $\overline{A}$ (not A) in another part. It is necessary, therefore, to have rules governing the development of the tree which eliminate the possibility of such contradictions.

PROBLEMS OF EXISTING METHODS

As already emphasised, the methods of representing fault propagation which have been developed are simplifications, sometimes over-simplifications, of very complex plant systems.

It is not surprising, therefore, that a number of problems has been encountered in the use of some of these techniques. This is most clearly apparent in relation to fault trees.

Some areas where problems arise are

Process variables

Time aspects

Dependence

Incoherence

Process variables are intrinsically continuous, but are treated in fault trees as discrete events/states which are either inside or outside defined limits, which are frequently rather arbitrary.

A fault tree gives the relationships between events at a particular moment in time. This assumption of time-independence also underlies the corresponding Boolean algebra. The fault tree method does not readily accommodate situations in which time order of events or time delays are significant.

On the other hand, the cause-consequence diagram does handle this aspect. This is one of the most valuable features of the method.

Another aspect of fault trees, which is of particular importance in the study of rare but catastrophic events, is the possibility of dependence between events in the tree. The basic assumption in the use of a fault tree is normally that the faults are independent. If there is a common cause of failure, the safety of the system may be reduced by orders of magnitude.

Another problem in fault tree work is that of incoherence. There are various types of incoherence, including incoherence in faults and incoherence in repair. Incoherence in faults may be illustrated by a system in which an event occurs if either of the flows A or B is zero. This would normally be represented by a simple OR gate. If the event does not occur, however, if both flows A and B are zero, this representation is incoherent.

DEVELOPMENTS IN MODELLING

There is a variety of different types of model which are, or might be, used as the starting point for the representation of fault propagation in process plants. Some of these types of models are

Word models

Mini-fault tree models

Input-output models

Digraph models

Equation models

A word model is a plain language description of relationships in the unit. A statement that an increase in flow will cause an increase in level is an example of a very simple word model. A rather more complex word model is the

statement that an increase in flow will cause an increase in level if the level control loop has failed. Word models are used in hazard and operability studies.

A mini-fault tree model consists of a fault tree for a particular top event on the unit. A separate mini-fault tree is required for each top event which is to be considered. This type of model is generally a particularly convenient input for automatic tree synthesis. Mini-fault trees have been used by Fussell (19) in the automatic synthesis of fault trees for electrical systems. He also refers to them as transfer functions. They have also been used by Martin-Solis, Andow and Lees (20) and Martin-Solis (21) in the automatic synthesis of fault trees for process plants. A typical mini-fault tree and the equation model from which it is derived are shown in Figure 5.

An input-output model consists of an input-output matrix for the unit. An example of such a model is shown in Figure 6. This type of model is again a convenient input for automatic tree synthesis. Input-output models have been used by Salem, Apostolakis and Okrent (22) in the automatic synthesis of fault trees for process plants.

A digraph model is a diagram which shows graphically the interactions between the variables in the unit. A typical digraph is shown in Figure 7. Digraph models have been used by Powers and Lapp (23 - 24) in the automatic synthesis of fault trees for process plants.

There are various types of model based on the equations of the unit, ranging from a full mathematical description to a relatively simple set of equations. Only one type of equation model is considered here. This is the enhanced functional model as used by Andow and Lees (18). If the full equation for the level in the tank in Figure 4 is

$$A \frac{dL_B}{dt} = F_A - F_C$$

where A is the tank cross-sectional area, L is the level, F_A and F_C are the flow in and out respectively and t is time, then the corresponding enhanced functional model is

$$\frac{dL_B}{dt} = (+F_A, -F_C)$$

This indicates that the level rises if F_A increases, but falls if F_C increases. Enhanced functional models have been used by Andow and Lees in the automatic synthesis of alarm networks of process plants for process computer alarm analysis. This type of model has also been used by Berenblut and Whitehouse (25).

Ideally, the fault propagation method should offer the user a choice of models as data inputs and should be capable of mapping from one model to another. This would allow him to use the most convenient type of model for a particular unit.

It is too early to say what degree of interchangeability is feasible. Some types of model tend to contain more information than others. While it is possible to pass from a high-information model to a low-information model by discarding information, the reverse process is clearly not possible. Nevertheless, it is probable that a method can be developed which gives some degree of interchangeability and does offer the user some degree of choice.

Of the techniques described, that which has been the subject of most development is the fault tree method.

The original fault tree method involves the selection of a top event to be investigated, the manual construction of the fault tree and the manual determination of the minimum cut sets. This is still the most widely used approach.

The effort involved in fault tree analysis soon led, however, to developments in the automatic analysis of the tree and in particular to the development of methods for the automatic computation of the minimum cut sets.

These developments still require, however, that the fault tree itself be constructed manually. Naturally attempts are being made to synthesise the fault tree automatically, but this is a much more difficult problem.

As far as synthesis is concerned it is necessary to distinguish between synthesis for electrical systems which consist of components with binary states only and process systems which contain variables with continuous ranges. Much of the reported work has been concerned with electrical systems.

The basic approach to fault tree synthesis is to break the overall system down into components, modules or units which can be described be some kind of model and then to devise models for these units and rules for linking models together again to form the fault tree.

Thus, for example, Fussell (19) has described a technique for synthesising fault trees for electrical systems in which the models are mini-fault trees and in which these mini-fault tres are strung together to form the overall fault tree.

A technique for synthesising fault trees for process systems has been developed by Salem, Apostolakis and Okrent (22). The models used are input-output matrices of units.

Another technique for fault tree synthesis for process systems has been developed by Powers and co-workers. Early work by Powers and Tompkins (26) described the use of input-output matrix models, but more recent work by Powers and Lapp (23 -24) emphasises the use of digraph models.

Fault trees for process systems have been synthesised by Martin-Solis (21) using mini-fault tree models. The latter are closely related to the equation models used by Andow (17). The method of Martin-Solis was developed initially for alarm analysis, but is equally applicable to design studies.

Synthesis of cause-consequence diagrams has been described by Taylor and coworkers (13, 27). The models used apparently include both mini-fault tree and equation models.

An account of cause-consequence diagrams has been given by Himmelblau (28).

A technique of synthesising the alarm network required for alarm analysis has been developed by Andow (17) and is described by Andow and Lees (18). This method makes use of equation models. These equation models are enhanced functional models as already described. Essentially, the technique is to use

the equations to determine which process variables interact with each other and so to produce a network showing the interactions of these variables. The network is similar to that shown in Figure 4 but is larger. This network is then 'combed' to remove all process variables which are not measured so that the smaller network giving the interactions between the process measurements, or alarms, only is retained as shown in Figure 4. The alarm network so obtained has a much looser structure than a fault tree.

An alternative approach to synthesis of the fault propagation structure for alarm analysis is the use of fault trees. As already mentioned, a method of fault tree synthesis for alarm analysis has been developted by Martin-Solis (21). The fault trees developed by this method differ somewhat from those used in design in that in the real time situation some branches of the tree need not be developed because the corresponding alarms are known to be absent. The work of Martin-Solis was done on a normal process control computer.

OUTLINE OF A GENERAL METHOD

The foregoing account of the state of the art in the modelling of fault propagation in process plants indicates the lines on which a systematic approach may be develped.

An outline specification for a generalised method for the representation and investigation of fault propagation in process plant might be as follows:

1) The method is developed for the study of fault propagation specifically in process plants.

2) The method is systematic, flexible and economical of effort.

3) The method is computer-based with automatic and semi-automatic / interactive features.

4) The basis of the method is the decomposition of the plant into a set of modules, or units. with an associated topography; the use of models of these units; and the creation of a fault propagation structure from these models by application of synthesis features.

5) The method accepts as inputs a variety of types of model and effects interchange between models by application of interchange features.

6) The synthesis features include
   Event/state definition
   Operators (gates and vertices) and associated logic
   Propagation rules
   Methods to handle time aspects

7) The regular, or canonical, form of the fault propagation structure is that held in the computer and other forms are derivations from or subsets of this form.

8) The models and topography are particular to the plant investigated, but the synthesis features are general.

9) The fault propagation structure can be interrogated to obtain various types of information, including those given by existing methods, e.g. fault trees or minimum cut sets. These types information are subsets of the information implicit in the fault propagation structure.

10) The interrogation facilities include numerical output, e.g. minimum cut sets; graphical output, e.g.fault tree diagrams; and interactive facilities.

11) The interrogation facilities include facilities for the validation of the models and of the fault propagation structure.

Any method for the study of fault propagation in process plant should take into account the particular characteristics of such plants, especially the continuous nature of the process variables and the time effects.

The study of fault propagation in process plant based on defined events/states has numerous pitfalls. Any method used should be formal and systematic. It should be as flexible as possible. It should be economical of effort.

The approach outlined is only practical as a computer-based method. Some of the features of both synthesis and analysis may be fully automatic. Others may be semi-automatic with a degree of interaction by the engineer.

The method involves decomposing the plant into a set of modules, or units, with specified connections between them; providing models of these units, either as standard models or as special models written for the specific plant or, more generally, a mixture of the two; applying to these models rules for defining events, for linking events by operators such as gates and vertices, for developing propagation of the faults and so building trees such as fault trees, event trees and cause-consequence diagrams; and for handling the time aspects.

The method accepts as inputs a variety of types of model. Some of these were discussed earlier. There is some degree of interchangeability between the models used. Interchange is effected by the application of interchange rules.

The essence of the method is sets of rules for the creation of the fault propagation structure from the models. These include rules for the definition of events/states; rules governing the use of gates and vertices and of associated logic; rules for the propagation of faults or construction of trees; and rules for handling time aspects.

The other features described in the above list are self-explanatory.

DEVELOPMENTS IN COMPUTER-AIDED DESIGN

The effectiveness of any of the methods for the study of fault propagation which have been described depends on the way in which they were used.

The methods are essentially aids to the engineer. They cannot relieve him, however, of the need to study and understand thoroughly the plant with which he is concerned. Thus, for example, a hazard and operability study is normally conducted by a small multidisciplinary team of people who have both widespread experience and knowledge of the particular process. Similarly, a major part of the work of an engineer who is carrying out a fault tree analysis of a plant is gaining an understanding of it.

A fault propagation method of the type described can be invaluable aid to the engineer, but he cannot use it blindly. In particular, there are dangers in attempting to make the whole process of the synthesis and analysis of the fault propagation structure automatic. A more appropriate alternative is to make the process semi-automatic and interactive, with intervention by the engineer at appropriate stages.

There are related problems in the area of the design bases of the plant which the engineer is trying to model. The acquisition of data on the plant struct-

ure is time-consuming. In addition, it is not easy to ensure that the data are kept up to date as modifications are made to the design.

Developments in computer-aided design are relevant to both these problems. It seems likely that increasingly the data base for the design of a process plant will be held in a computer and updated as the design progresses. This data base would then be available to engineers concerned with particular features such as process control or fault propagation.

Interactive computing is an integral part of computer-aided design. It is envisaged that many of the stages not only in the creation of the fault structure but also in its interrogation and validation would be interactive.

INTERROGATION AND VALIDATION

The problems discussed so far are primarily those of the creation of fault structure of the plant. It is envisaged that for a general method the regular form would be a fault structure held in a computer program.

This method of representing the fault structure appears to be intrinsically the most powerful and flexible form, but is opaque to the user. This opacity hs obvious disadvantages, but it also has some advantages. It requires the user to define carefully precisely what information he requires to know.

In principle, a fault structure of the kind envisaged is capable of being interrogated to produce various types of output, including the common existing types. Thus, for example, it would produce as graphical output a fault tree diagram and as alphanumeric output the minimum cut sets.

The general method would therefore give the same type of information as some of the existing methods such as fault tree methods. There are other existing methods such as hazard and operability studies, however, which yield a somewhat different type of information. In order to extract the latter type of information it would be necessary to develop methods of interrogation.

The problem of interrogation of the fault structure is not peculiar to the general method outlined. It exists equally, for example, with very large fault trees. These also tend to be somewhat opaque.

Closely related to the problem of interrogation is that of validation. Validation of the fault structure is essential whatever method is used to model fault propagation. There is a need for development of methods of validation. Clearly, interrogation methods constitute an important aspect of validation methods.

STATE OF THE ART

Currently there appear to be several groups of workers who are developing methods of representing and investigating faults and fault propagation in process plants.

The work of Powers and Lapp is based on the digraph models, that of Taylor on the cause-consequence diagrams and that of the authors on the development of the functional models and alarm networks of Andow and Lees and the mini-fault trees of Martin-Solis, Andow and Lees.

All these developments are based on computers. In the case of the authors' own work, the regular form of the fault propagation structure is the data

structure held in the computer, other forms such as fault trees are regarded as subsets of this data structure, and particular emphasis is placed on achieving a fault description of the process which allows the generation of the data structure to proceed as nearly automatically as possible.

The work described by Powers and Lapp is apparently done on a large computer, while that described by Taylor and that of the authors is done on a small computer of the general type used in process control (eg PDP 11). The methods used by the two latter groups involve interactive computing.

ACKNOWLEDGEMENT

The authors wish to acknowledge the support of the Science Research Council in this work.

REFERENCES

1. Lees,F.P. 1979 "Loss Prevention in the Process Industries", Butterworths, London.

2. Recht,J.L., 1965, "Systems Safety Analysis",Nat. Safety News, 92(6), 37.

3. King, C.F. and Rudd, D.R., 1971 "Design and Maintenance of Economically Failure-Tolerant Processes", AIChE J., 18, 257.

4. Lawley, H.G., 1974 "Operability Studies and Hazard Analysis", Chem. Engng.Prog., 70 (4), 45.

5. Rushford, R., 1977 "Hazard and Operability Studies in the Chemical Industries", Trans.N.E. Coast Inst.Engrs. and Shipbuilders. 93(5), 117.

6. ChemicalIndustry Safety and Health Council, 1977, "A Guide to Hazard and Operability Studies", London.

7. Fussell, J.B.,1976, "Fault Tree Analysis: Concepts and Techniques", in E.J.Henley and J.W.Lynn, "Generic Techniques in Systems Reliability Assessment", Noordhoff, Leyden.

8. Atomic Energy Commission, 1975, "Reactor Safety Study. An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants", Rep. WASH 1400, Washington, D.C.

9. Barlow, R.E., Fussell, J.B. and Singpurwalla, N.D. (eds.), 1974, "Reliability and Fault Tree Analysis", SIAM, Philadelphia.

10. von Alven, W.H. (ed.), 1963, "Reliability Engineering", Wiley, New York.

11. Health and Safety Executive, 1978, "Canvey: An Investigation of Potential Hazards from Operations in the Canvey Island / Thurrock Area", H.M.Stationery Office, London.

12. Nielsen, D.S., 1971, "The Cause-Consequence Method as a Basis for Quantitative Accident Analysis", Danish Atomic Energy Commission, Riso, Rep. Riso-M-1374.

13. Taylor, J.R., 1974, "A Semi-Automatic Method for Qualitative Failure Mode Analysis", paper presented at CSNI Mtg. on Development and Appl. Reliab. Techs. to Nuclear Plants, Liverpool, April 8 - 10.

14. Taylor, J.R., 1974, "Sequence Effects in Failure Mode Analysis", Danish Atomic Energy Commission, Riso, Rep. Riso-M-1740.

15. Paterson, D., 1968, Application of a Computerised Alarm Analysis System to a Nuclear Power Station", Proc. IEE, 115, 1858.

16. Welbourne, D., 1968, "Alarm Analysis and Display at Wylfa Nuclear Power Station, "Proc. IEE, 115, 1726.

17. Andow, P.K., 1973, "A Method for Process Computer Alarm Analysis", Ph.D. Thesis, Loughborough University of Technology.

18. Andow, P.K. and Lees, F.P., 1975, Process Computer Alarm Analysis: Outline of a Method Based on List Processing", Trans.Instn.Chem.Engrs., 53, 195.

19. Fussell, J.B., 1973, "A Formal Methodology for Fault Tree Construction", Nucl.Sci.Engng., 52, 421.

20. Martin-Solis, G.A., Andow, P.K. and Lees, F.P., 1977., "An Approach to Fault Tree Synthesis for Process Plants", Second Int. Symp. on Loss Prevention and Safety Promotion in the Process Industries, DECHEMA, Frankfurt.

21. Martin-Solis, G.A., 1978, "Fault Tree Synthesis for Real Time and Design Applications on Process Plant", Ph.D. Thesis, Loughborough University of Technology.

22. Salem, S.L., Apostolakis, G.E. and Okrent, D.L., 1976, "Computer-Oriented Approach to Fault-Tree Construction", University of California, Los Angeles, Rep. UCLA-ENG-7635.

23. Powers, G.J. and Lapp, S.A., 1976, "Computer Aided Fault Tree Synthesis", Chem.Engng.Prog., 72(4), 89.

24. Powers, G.J. and Lapp S.A., 1977, "Computer-Aided Synthesis of Fault Trees", IEEE Trans.Reliab., R-26, 2.

25. Berenblut, B.J. and Whitehouse, H.B., 1977, "A Method for Monitoring Process Plant Based on a Decision Table Analysis",Chem.Engr., Lond., 318, 175.

26. Powers, G.J. and Tompkins, F.C., 1974, "Fault Tree Synthesis for Chemical Processes", AIChE J., 20,376.

27. Hollo, E. and Taylor, J.R., 1976, "Algorithm and Program for Consequence Diagram and Fault Tree Construction", Danish Atomic Energy Commission, Riso, Rep.Riso-M-1907.

28. Himmelblau, D.M., 1978, "Fault Detection and Diagnosis in Chemical and Petrochemical Processes", Elsevier, Amsterdam.

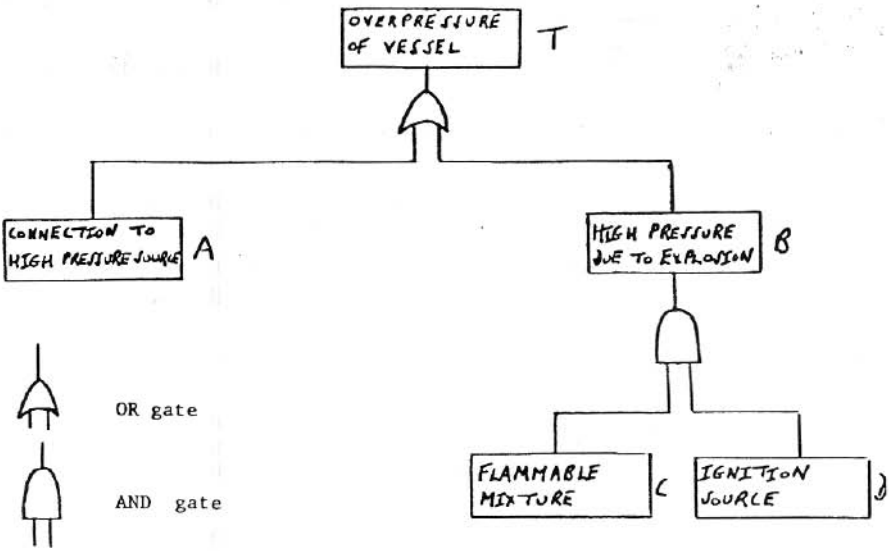

OVERPRESSURE OF VESSEL
T
CONNECTION TO HIGH PRESSURE SOURCE
A
HIGH PRESSURE DUE TO EXPLOSION
B
OR gate
AND gate
FLAMMABLE MIXTURE
C
IGNITION SOURCE
D

Figure 1

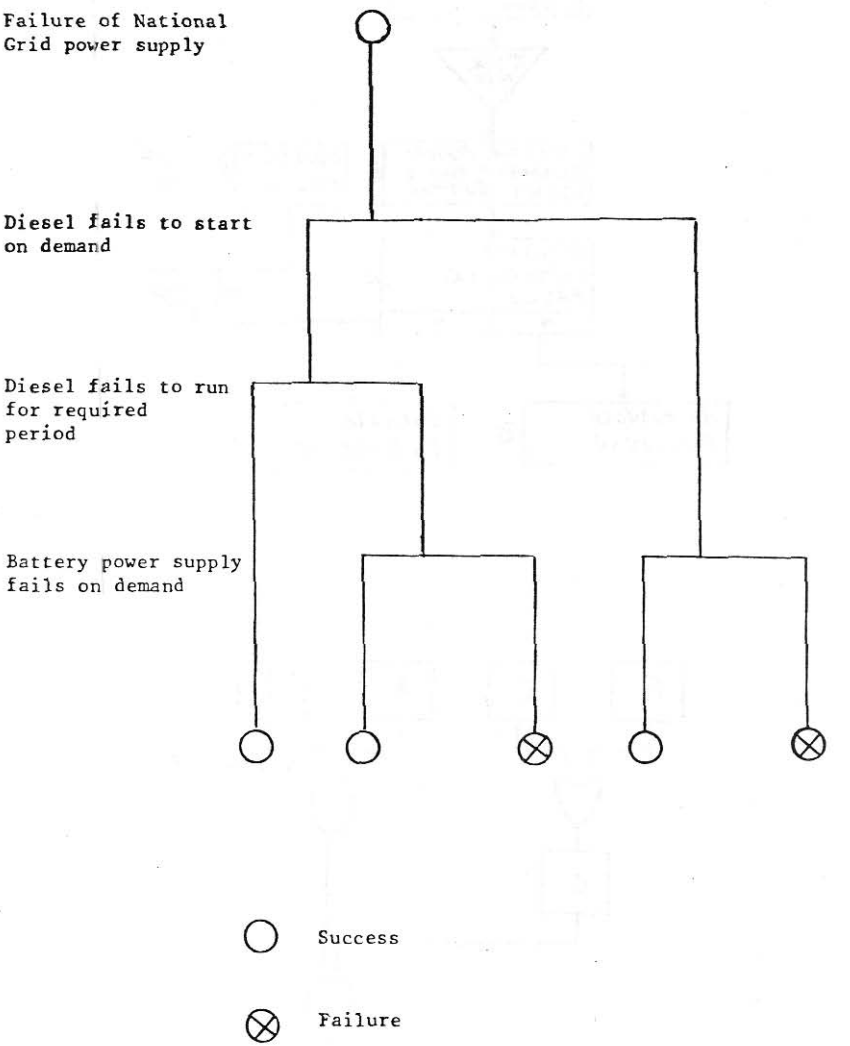
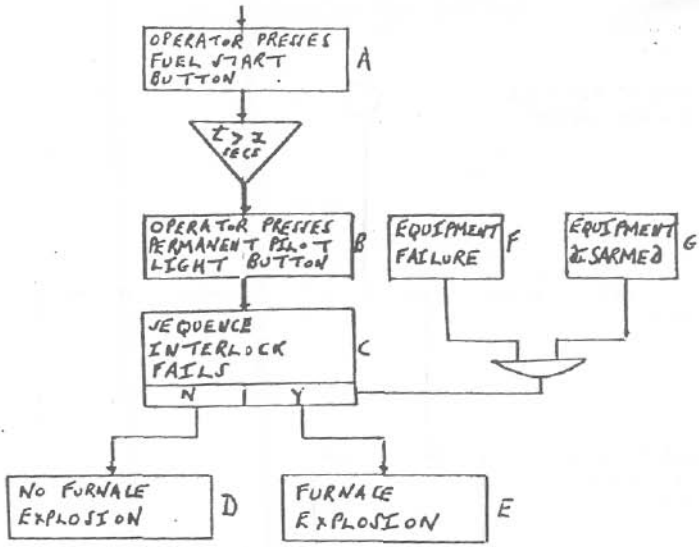

Failure of National Grid power supply
Diesel fails to start on demand
Diesel fails to run for required period
Battery power supply fails on demand
Success
Failure

Figure 2


OPERATOR PRESSES FUEL START BUTTON
A
t > 2 secs
OPERATOR PRESSES PERMANENT PILOT LIGHT BUTTON
B
EQUIPMENT FAILURE
F
EQUIPMENT DISARMED
G
SEQUENCE INTERLOCK FAILS
C
N
Y
NO FURNACE EXPLOSION
D
FURNACE EXPLOSION
E

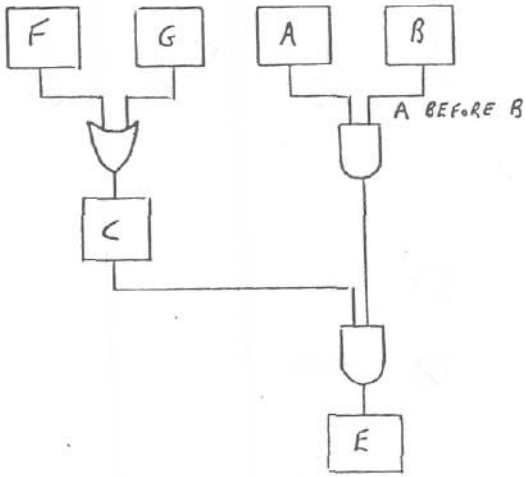

F
G
A
B
A BEFORE B
C
E

Figure 3

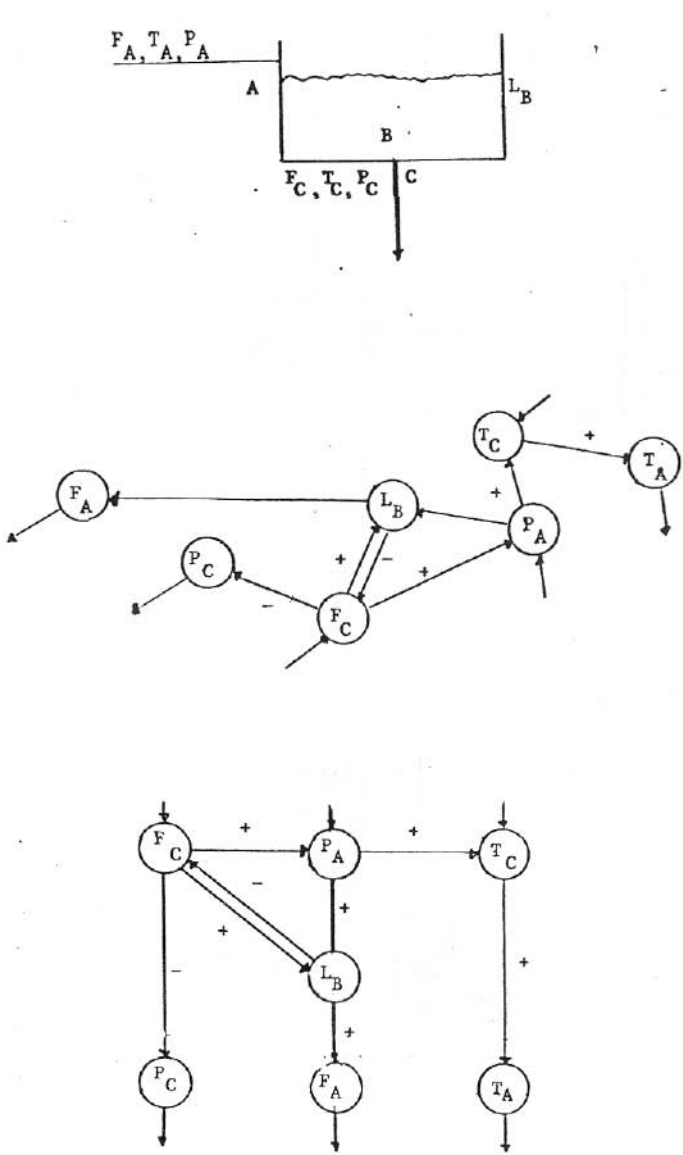
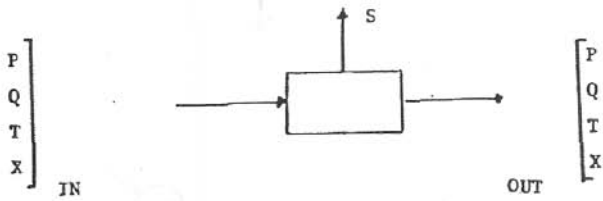


Figure 4



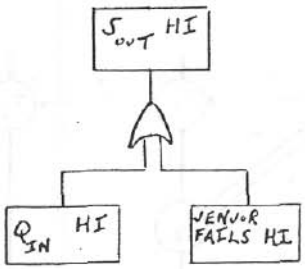


Figure 5

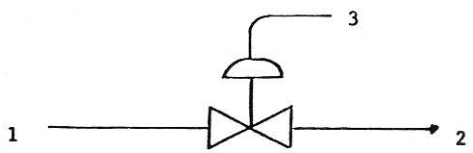


Figure 6

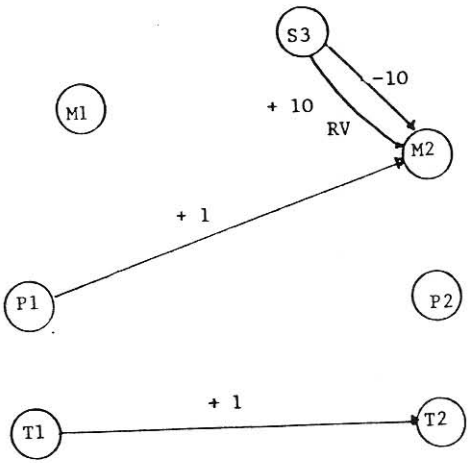


Figure 7