Reliability Engineering **14** (1986) 85–106

Application of the Digraph Method of Fault Tree Construction to Process Plant

J. D. Andrews and J. M. Morgan†

British Gas R & D, Midlands Research Station, Wharf Lane, Solihull, West Midlands B91 2JW, Great Britain

(Received: 15 August 1985)

ABSTRACT

This paper describes the digraph method of fault tree construction and its application to the process stream of a butane vaporiser. It is shown that an accurate, well-structured fault tree can be produced for a process system which incorporates a number of control loops.

1 INTRODUCTION

Fault tree analysis is now a well-established technique for assessing the safety and reliability of engineering systems. It is often used to determine the causes of unsafe or undesired events which can be identified by techniques such as hazard and operability studies. Fault tree analysis has been extensively applied in the aerospace, nuclear and chemical industries and recently within British Gas.[1] Unfortunately, as yet, the development of a rigorous approach to the construction of a fault tree has not been achieved. Two engineers given the same system and undesired event would usually develop fault trees differing in structure. This type of analysis is also very time-consuming and, as such, there is a considerable

† To whom correspondence should be addressed.

A version of this paper was presented at the 5th National Reliability Engineering Conference – Reliability '85, 10–12 July 1985, Birmingham, UK, and is reproduced by kind permission of the organisers.

incentive to produce a fault tree construction algorithm which could be implemented on a computer. Fault trees would then be produced automatically and there would be a consistent repeatable approach to the way the undesired event is developed.

A number of algorithms have been proposed by different groups for automating the construction process.[2,3] One such algorithm is based on the directed graph or digraph method, developed at Carnegie-Mellon University in the mid 1970s by Lapp and Powers[4,5] and further developed by Lambert[6] and Allen.[7,8] A digraph provides an intermediate step which gives explicit relationships between the process variables, from which the fault tree can be constructed. This method provides a structured approach which is well suited for modelling systems including control loops, where a set of rules, termed an 'operator', can be applied.

However, there are some pitfalls which have been encountered by others whilst using the technique.[9] The main problem occurs when it is necessary to model the two-way flow of information. In this case there are difficulties with the application of operators associated with control loops. In fact, application of such operators breaks down when control loops within control loops are encountered in a system and Lapp and Powers' technique of considering the loop node-by-node must then be used.

In order to assess the capabilities of the digraph technique it has been selectively applied to British Gas process plant. One such application, relating to a butane vaporising system, is presented, together with a description of the technique itself.

2 THE DIGRAPH METHOD

The digraph method is a two-step approach to fault tree construction. Initially, the digraph is constructed from a description of the system to show, by means of a multivalued logic diagram, the interrelationships between the process variables. This diagram not only represents the normal working state of a system but also indicates component failure modes which can nullify or change the relationships usually experienced between process variables. The second stage is then to progress from this intermediate step to develop the fault tree for the chosen undesired event by means of a construction algorithm.

Conventional fault tree construction techniques do not in general

provide an easily applicable tool for failure analysis of complex control systems. For example, it is difficult to envisage the control loop structures from the system description when manually constructing a fault tree. However, the digraph clearly displays the control loops within a system and having identified their structure the fault tree can be produced by application of the relevant operators.

2.1 Unit model digraphs

In order to construct a digraph of a system the function of each component must be represented in digraph terminology. This is accomplished by means of a unit model digraph, derived for each component by considering the way in which the component functions in terms of the basic laws governing energy, mass and momentum. In addition, by identifying the effects that the component failure modes produce, the unit model digraph performs the same function as mini fault trees or decision tables in other fault tree construction methods.

A digraph is a set of nodes and connecting edges. Nodes on the digraph represent the process variables. When one variable affects another then a directed arrow or edge is drawn to connect them. The direction of the arrow is from the independent variable to the dependent variable and may be either a normal edge, which indicates that the relationship is normally true, or a conditional edge which indicates that the relationship holds only when the condition is satisfied. When several edges connect the same pair of nodes then only one relationship is in operation at any one time: that is, the connecting edges are mutually exclusive.

Variables are represented on the digraph by nodes with alphanumeric labels. This label conventionally has two parts; the first being a letter to represent the process variable such as P, M, T, S or C for pressure, mass flow, temperature, signal and concentration, respectively, and the second being a number to show the location of the variable on the system. Therefore M2 represents the mass flow rate at location 2.

As an example, consider the air-to-close regulating valve shown in Fig. 1(a). The valve is operated by the air pressure on the valve actuator (location 3). Variation of air pressure will adjust the position of the valve, changing the flow cross-sectional area and thus affecting the mass flow rate at the value output (location 2). P3 and M2 are therefore related and their nodes are joined by an edge whose direction is from P3, the independent variable to M2 the dependent variable (Fig. 1(b)).

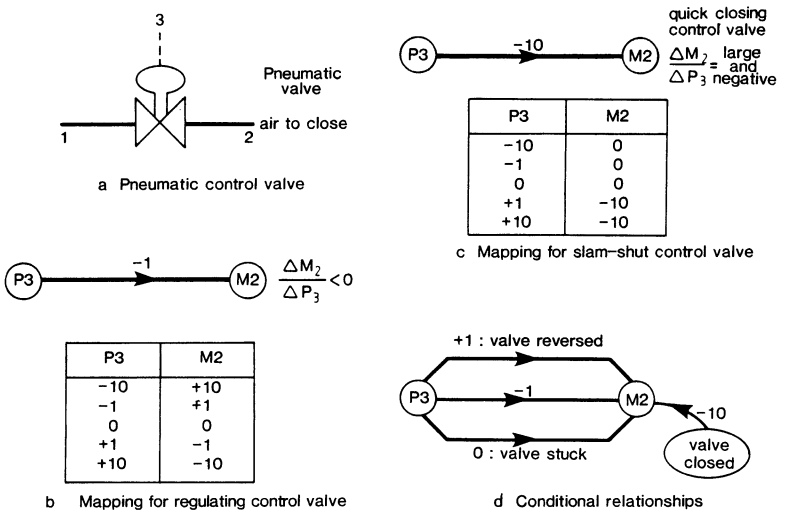

Fig. 1. Digraph nomenclature.

In order to show the strength of the relationship between the two variables, numbers are placed on the directed edge to represent the gains. Gains of ± 1 and ± 10 are termed moderate and strong relationships, respectively, and 0 indicates a nullification of the relationship between the two variables. These values are defined for digraphs by $\Delta Y/\Delta X$ where X and Y are the independent and dependent variables, respectively. Therefore the sign of the gain indicates the direction Y changes when X increases. For the air-to-close regulating control valve, when P3 increases, the flow rate decreases and this results in a gain of -1 being placed on the edge between the two variables. A gain of -1 implies the relationship between P3 and M2 shown in Fig. 1(b).

The same five numbers, -10, -1, 0, $+1$, $+10$, are used in digraphs to represent both the disturbances and the gains. A disturbance is the deviation that the process variable has made from its normal expected value, which is represented by zero. For example, a disturbance of magnitude 1 indicates a range of values that is considered moderate. The sign of the disturbance indicates whether the deviation is above (+) or below (−) that of the normal value. Large disturbances are indicated by a magnitude of 10. The multivalued logic scheme with the five values has been derived in order to model control systems and the classification of 'large' versus 'moderate' is usually based on the ability of the system to control the disturbance. Changes in the variable value which are beyond

the capacity of the system action to compensate are therefore given a ± 10 value. Moderate disturbances (± 1) are expected to occur. The relationship for the disturbances in the process variables is illustrated in Fig. 1(b) for the control valve.

If the control valve in Fig. 1(a) was of the slam shut protection type with only two states, open or closed, an increase in air pressure P3 would shut the valve and cause mass flow to instantaneously decrease to zero. This represents a strong relationship and is illustrated in the mapping diagram of Fig. 1(c). Loss of air pressure cannot open the valve further than fully open and is represented by the first two rows in the table having zero values for M2. It can be seen here that a $+10$ disturbance combined with a -10 gain causes a -10 disturbance in the dependent variable as the maximum magnitude in the numbering scheme is 10. The general rule for determining the value of the disturbance of the dependent variable is to multiply the value of the disturbance of the independent variable and the gain of the dependent variable, noting that the absolute value of the disturbance of the dependent variable cannot exceed 10.

Edge dependent or conditional relationships are also added to include non-working states: for example, the valve stuck in its normal position. In this instance, changing the air pressure has no effect on M2 and is represented by a zero gain. In this case the relationship between the independent and dependent variables is nullified. Other component failure events such as valve closed have the effect of introducing a disturbance into the system; in this case a -10 deviation to the mass flow (M2) out of the valve. A digraph for the air-to-close control valve including the valve stuck, valve reversed and valve closed failure modes is shown in Fig. 1(d).

2.2 Construction of the system digraph

Drawing the system digraph is a very similar process to constructing a fault tree. The digraph is developed backwards from the process variable whose disturbance represents the undesired or top event. Initially the system schematic diagram is examined and local input variables are identified which have the ability to cause deviations in the top event process variable. Local variables are those which can directly change the value of the variable under consideration. These events are placed on the digraph and linked via the relevant edge relationship. Any variables which themselves have inputs can be further developed and are then traced in the

digraph construction. The digraph edge relationships can usually be established by linking together the component unit model digraphs. If control loops exist then the same variables may be encountered twice and in this situation, variables which have been previously developed should not be retraced. Where variables appear on conditional edges they are expanded in the same manner as input variables and the process is terminated when all inputs cannot be further developed.

3 CONTROL LOOPS

The main advantage which the digraph method exhibits over conventional fault tree construction methods is its ability to deal with control loops. The three main components of a control loop are: the sensor, the controller and the control device. The sensor measures the value of a process variable and communicates this value to the controller. At the controller the actual value of the sensed variable is compared with the desired value and a corrective signal for any deviation is transmitted to the control device. The corrective action is taken by the control device in order to counteract the disturbance in the sensed variable by adjusting the manipulated variable.

There are two basic forms of control loops:

Negative feedback loops (NFBL) and
Negative feedforward loops (NFFL)

3.1 Feedback loops

A negative feedback loop has the ability to correct moderate disturbances in the process variable. It senses a disturbance in the sensed variable and commands the manipulated variable to change in such a manner as to counteract the measured disturbance.

An example of a NFBL and its associated digraph is given in Fig. 2. In order to identify the location of the variable the process stream is divided into discrete sections and each section is numbered. The portions of the system schematic which are numbered are generally the connections between components such as pipes and wires which do not in themselves cause changes in the process variable values. On a digraph a NFBL can be identified as a path which starts and ends at the same node and for which the product of the normal gains is negative.

In Fig. 2 the control loop senses flow at location 2 and adjusts the air-to-open valve in order to maintain the flow at the set point value. To construct the digraph we start at location 3 and find all the possible causes for changes in M3 in terms of local variables. It can be seen that the only possible cause is a change in M2 and that the variables M2 and M3 are connected by a +1 gain. Tracing the next step it can be seen that the controller air pressure in P5 and the mass flow into the loop, M1, can cause deviations in M2. An increase in either M1 or P5 will cause M2 to

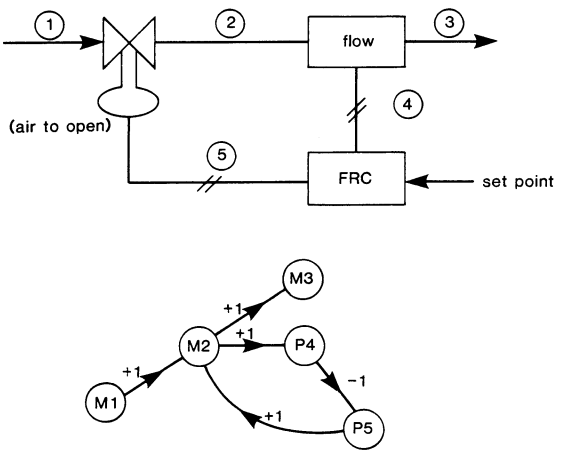

Fig. 2. Flow control negative feedback loop.

increase and so both edges have a +1 gain. Since the controller provides the corrective action from the signal it receives, the gain between P4 and P5 is −1. The relationship between M2 and P4 is +1 and this completes the loop. On examination it is apparent that as the loop starts and ends at node M2 and has a net gain of −1 it therefore exhibits the characteristics which categorise it as a NFBL.

If the gain on such a loop were to be positive then the loop would be categorised as a positive feedback loop (PFBL) and would have the property of increasing deviations in process variables, rather than cancelling them. As such, the smallest amount of noise would be amplified and drive the control loop high or low. In practice a PFBL would normally occur as a result of a poor design, or bad installation or maintenance. A PFBL should be detected during commissioning or during the start-up of the plant following maintenance.

3.2 Feedforward loops

The main disadvantage of feedback control is that the disturbance exists for some finite time before the loop can cancel its effect. Feedforward control, if working perfectly, can exactly cancel a disturbance by sensing an upstream variable and manipulating a downstream variable. On the digraph, downstream means in the same direction as the arrows. Generally, in the process industries, feedforward control would be combined with feedback control.

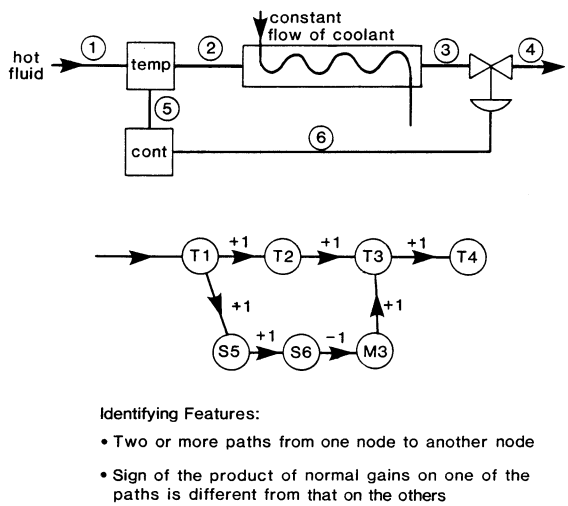

Fig. 3. The digraph representation of a negative feedforward loop.

In order to illustrate the structure of a NFFL on a digraph an example relating to a heat exchanger is shown in Fig. 3. A negative feedforward loop (NFFL) is identified by two features:

(1) Two or more paths from one node to another node.
(2) The sign of the products of the normal gains on one path is different from that on the others.

Disturbances can propagate along the path with the net positive gain, termed the *causative branch*, and can be controlled or cancelled on the path with the net negative gain called the *corrective branch*.

4 FAULT TREE CONSTRUCTION

Having achieved the intermediate result of the digraph it is then possible to construct the fault tree. However, before fault tree construction can commence, two requirements are necessary. The top event must be represented in terms of a disturbance in one of the system process variables and all the control loops in the system must be identified and classified. In general, if a system digraph contains no control loops or conditional edge statements then the fault tree consists of all OR gates with basic events representing either disturbances in process variables, equipment failure, human error, or environmental conditions. When constructing fault trees from digraphs with control loops, the fault is traced backwards through the digraph until the first node on each loop is encountered. Operators derived from each type of loop are applied to construct the fault tree. The derivation of the loop operators, initially developed by Lambert,[6] is given in the Appendix. Lapp and Powers[4,5] utilise a different operator which is used recurrently node-by-node around the loop. It yields essentially the same result as Lambert but the present authors have found that it is easier to apply an operator which considers the loop in its entirety. Consequently, the Lambert operator was used in the application presented in the next section. A similar application had been considered by Dunglinson and Lambert.[10]

5 APPLICATION TO A BUTANE VAPORISING SYSTEM

5.1 System description

The schematic diagram of the butane vaporising system is shown in Fig. 4. It is effectively one stream of a two-stream peak load plant, which provides butane–air to augment the supply of natural gas in the British Gas distribution system in times of high demand. Two independent automatically controlled natural gas fired burners heat the butane in the 'hair pin' heating tube bundle. The vaporiser has a maximum capacity of 210 000 $ft^3 h^{-1}$ of butane at a delivery pressure of 70 psig.

Liquid butane is supplied from its storage tank by a pump (P1) and a manifold at a pressure of 300 psig. Regulation of the supply is provided by means of a pressure control valve (V1) which is adjusted to deliver liquid at a pressure between 70 and 110 psig, dependent upon the demand. From

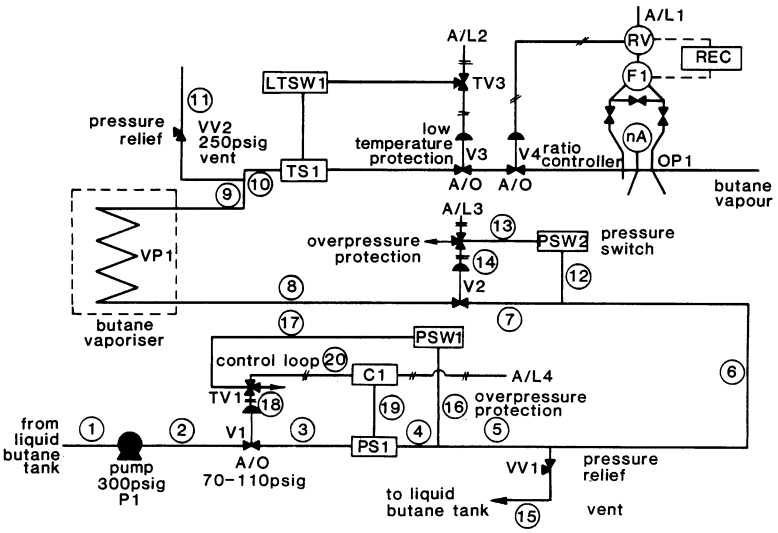

Fig. 4. Schematic diagram of butane vaporising system.

this point the butane is fed along a 4 in line into the vaporiser (VP1). Overpressure protection features are provided on the feed into the vaporiser such as the override slam shut facility on the pressure control valve, a slam shut valve (V2) on the inlet to the vaporiser and a pressure relief valve (VV1) near the pump. On activation of the pressure relief valve the butane is returned to the storage tank. The vaporiser coil is rated at 250 psig and since the pump can deliver 300 psig another relief valve (VV2) has been added downstream of the vaporiser, to protect against overpressure.

In order to maintain the supply integrity a low temperature trip (valve V3) has also been provided to avoid the possibility of liquid butane entering the main distribution system. This is activated by any temperature monitored below 82 °C. In this system the low temperature protective loop and the slam shut protection (V2) were both regulating valves modified to perform as quick acting trip valves by the introduction of a three-way valve with a rapid venting action.

Control of the mixing of the butane and natural gas streams is by flow ratio control. The relative flows are sensed and the butane adjusted to give the desired ratio.

The study was carried out to investigate the possibility of high pressure liquid butane passing through the vaporiser and venting at the outlet

VV2. On investigation it can be seen that one cause of liquid venting to the atmosphere is that the vaporiser heater has failed and the low temperature liquid butane triggers the safety valve V3. The back pressure generated would cause the venting action. A second cause would be the passage of butane at such a high flow rate that the vaporiser does not have the capacity to deal with it. In this case it may be that the pressure surge on its own will vent the liquid. Therefore the top event is chosen as a very low temperature at the outlet of the vaporiser caused by liquid butane passing through the coils. Venting can also occur if either valve V3 or V4 spuriously shuts and a back pressure builds up. But in this instance, as the burners will be firing, it will be a vapour that is expelled from the vent and it is therefore not considered.

5.2 Digraph construction for the butane vaporiser

Before the construction of the system digraph could commence, the precise function of each component in the system was clearly defined. This included the identification of the modes of failure and the effect that each failure would have on the component performance. Information for each component was then collated to form individual unit model digraphs.

As discussed in the previous section the hazardous event associated with the butane vaporising system was the passage of liquid butane through the vaporiser. This is represented in a top event of very low temperature at the outlet of the vaporiser. Having explicitly established both the top event and formed a complete understanding of the action of each system component, the digraph was then constructed.

The first step was to number all the sections of the schematic process diagram shown in Fig. 4. In this case the main butane stream was numbered first, followed by each of the loop structures starting from the vaporiser and working back towards the pump. The top event of very low temperature (-10) at the outlet of the vaporiser (T9) could then be written in digraph notation as T9 (-10). As each digraph is dependent upon the top event the construction process starts at the top event process variable and develops all possible local process variables which have the ability to cause a deviation in the selected variable. In this case, the mass flow into the vaporiser and vaporiser failures were the only events to affect the output temperature in stream 9. Attention was then switched to all the new nodes added to the digraph and these were in turn developed until all the variables within the system boundary had been considered. Links

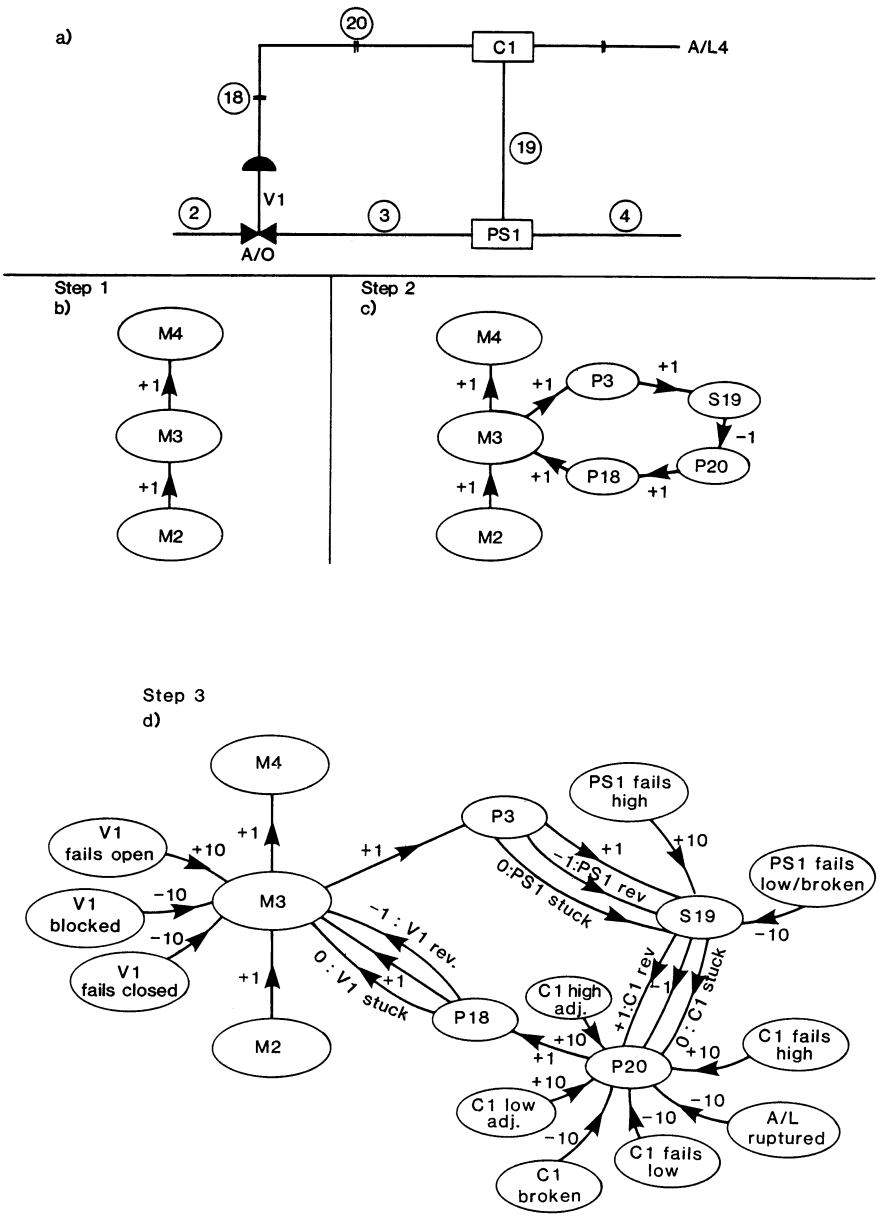

Fig. 5. Digraph construction of control loop.

between the nodes and the appropriate gains, were added by referring to the unit model digraphs constructed earlier or by considering the physical equations governing the process.

To illustrate the technique for the digraph construction a detailed explanation is given for the control loop structure located at the outlet of the pump. From this the remainder of the digraph construction process can be deduced. Construction of the digraph for the feedback loop, which is illustrated in Fig. 5(a), was accomplished in three stages:

Step 1. The first step (Fig. 5(b)) was the development of the digraph back along the main stream from the output node M4, tracing mass flow through the control loop. The edges M2 to M3 and M3 to M4 can be seen to represent the valve and pressure sensor components, respectively. Gains on the loop were obtained from the unit component models.

Step 2. Step two (Fig. 5(c)) included all normal edge relationships which complete the loop and shows how all the other process variables interrelate to give the control action. Starting at node M3 and following the loop round, M3 to P3 is the physical relationship between the mass flow and pressure at the valve outlet. P3 to S19 shows the loop gain given for the pressure sensor; as the pressure increases so will the signal to the controller, resulting in a gain of $+1$. The control action is provided by comparing the signal S19 against the required value and adjusting the air pressure, indicated by a gain of -1 between the nodes S19 and P20. The air pressure causes the valve to regulate the mass flow to its desired value.

Step 3. By examination of the unit component models, the remainder of the digraph was completed by adding the nodes or conditions which represent the component failure modes (Fig. 5(d)). Component failure modes appear on the digraph as either nodes which input disturbances, or conditional edges which change the relationship between process variables.

The complete digraph for the butane vaporiser was developed in a similar way and is shown in Fig. 6.

5.3 Fault tree construction

Having constructed the system digraph, the next step is the formulation of the fault tree. For this, the procedure used is dependent upon the type of

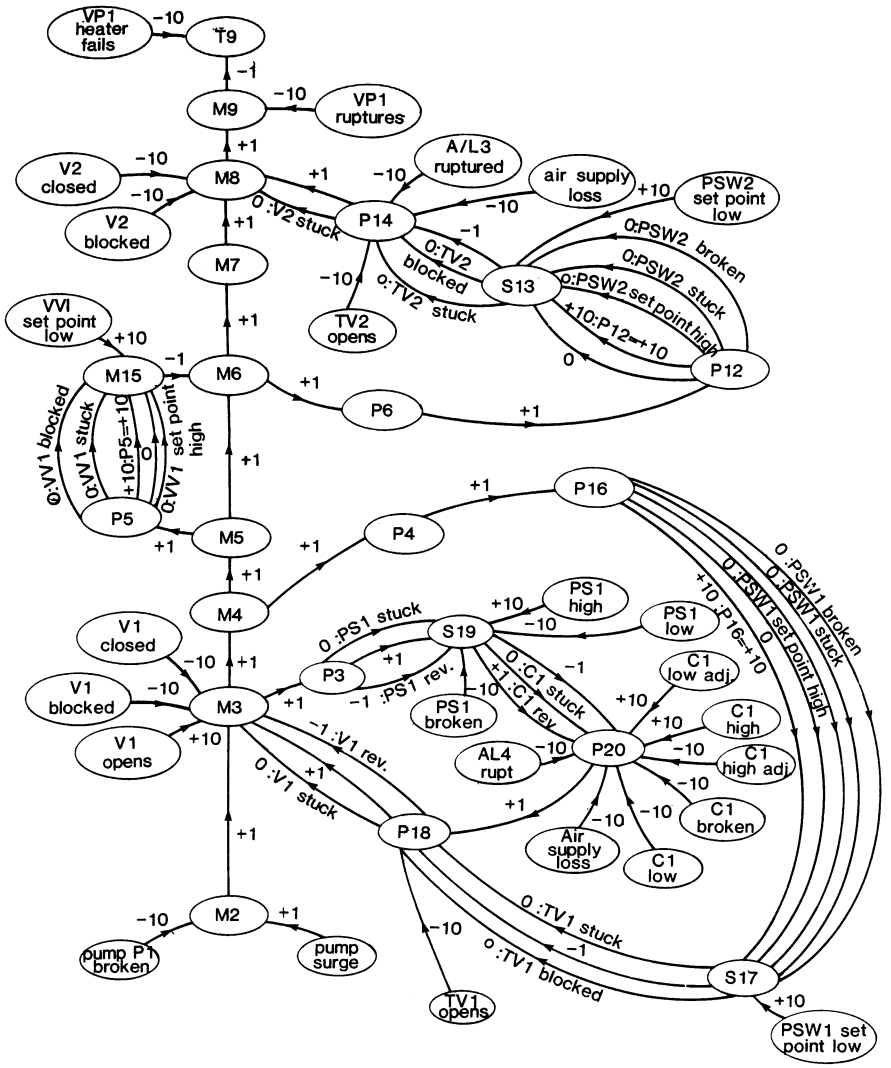

Fig. 6. Digraph of butane vaporisation process.

loops appearing in the digraph. Identification and classification of the control loops as either feedback of feedforward is therefore very important.

Construction of the fault tree starts with the top event variable (i.e. low temperature at the exit of the vaporiser). By examining the information flow on the digraph, the disturbance is traced back to other possible local

causes. These local variables which have inputs are again further developed until events which have no inputs, i.e. basic events, are reached. If control loops exist on the system and are encountered during the tracing back process, they may result in variables being traced which have been developed previously. To avoid this problem of repeated events, operators are applied whenever a control loop is present. In general if a digraph has no control loops or conditional edges then the fault tree will consist of only OR gates.

As shown in Fig. 5 a feedback control loop can be identified at node M3, consisting of nodes M3, P3, S19, P20 and P18. There are also three protection loops in the system which are identified as having a normal gain on the protective branch of zero but a ± 10 gain when called upon to act. In fact node M3 has nested control and protection loops which have valve V1 as a common component.

The top event, low temperature at the outlet of the vaporiser, can be expressed in digraph notation as $T9(-10)$. Tracing the causes of this event back through the digraph gives local causes as either $M9(+10)$, a high flow rate of butane which cannot be vaporised, or failure of the vaporiser heating system, which are linked via an 'OR' gate to the top event as shown in Fig. 7. Failure of the vaporiser heating system can then be expressed in terms of failure of the two burners while $M9(+10)$ is further developed upstream to add the next level to the fault tree. M8 is connected to M9 by an edge with a $+1$ gain and so the only cause of $M9(+10)$ is $M8(+10)$. $M8(+10)$ is the output node on a protection loop. As a protection loop cannot generate a disturbance, for the output to go high, then a high disturbance must enter the loop (i.e. node M6), and the loop must be inactive. This is developed and included in the fault tree as shown.

Construction of the fault tree continues in this manner developing failures associated with the remaining protective loops, which have as their output nodes M6 and M4, respectively. These correspond to the vent valve VV1 and the slam shut override system which operates V1. When the variable M3 is encountered this has been previously classified as the first node on a NFBL. The operator for this is presented in Fig. A2 and must be applied at this stage, taking care to account for the protective loop which also operates V1.

The loop under consideration is the protection loop on the digraph consisting of nodes M4, P4, P16, S17, P18 and M3. Slam shut protection is activated if the pressure switch PSW1 monitors a high pressure (P16).

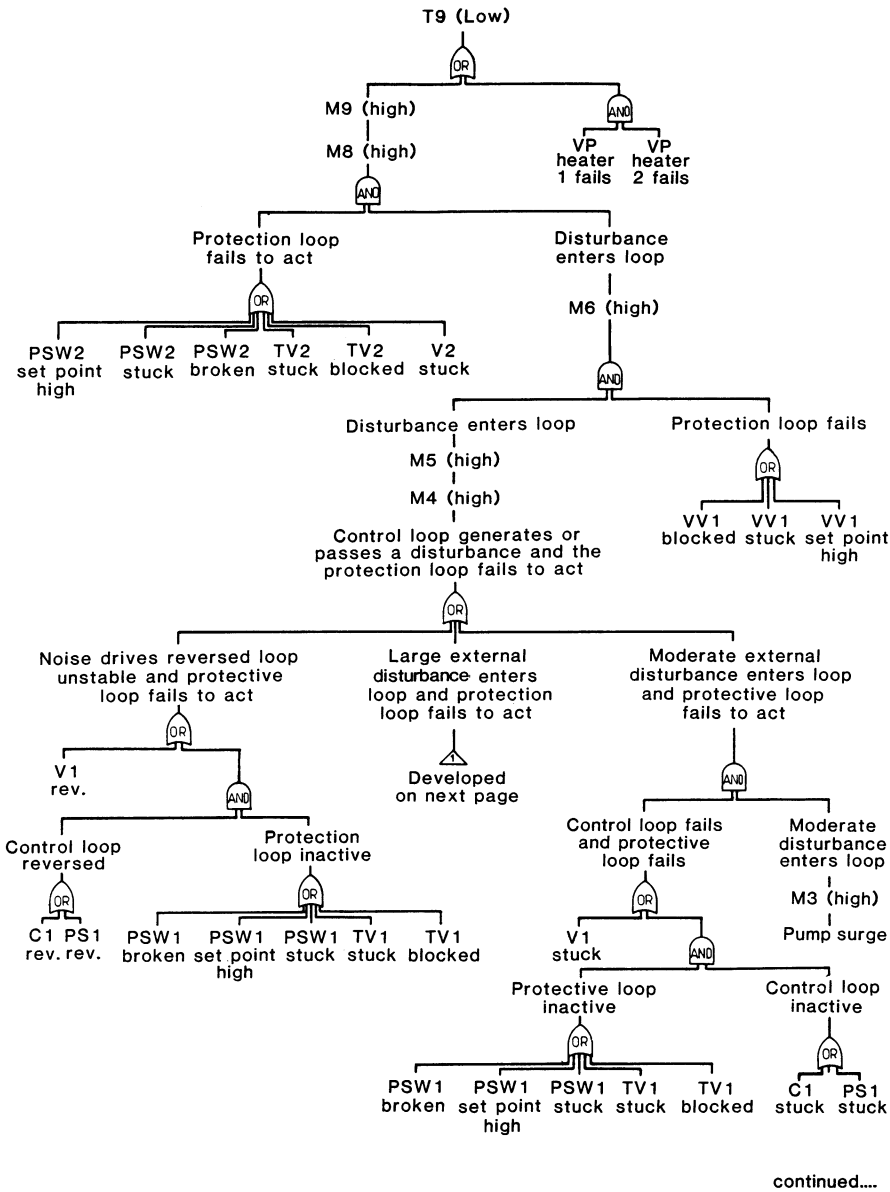

Fig. 7. Complete fault tree.

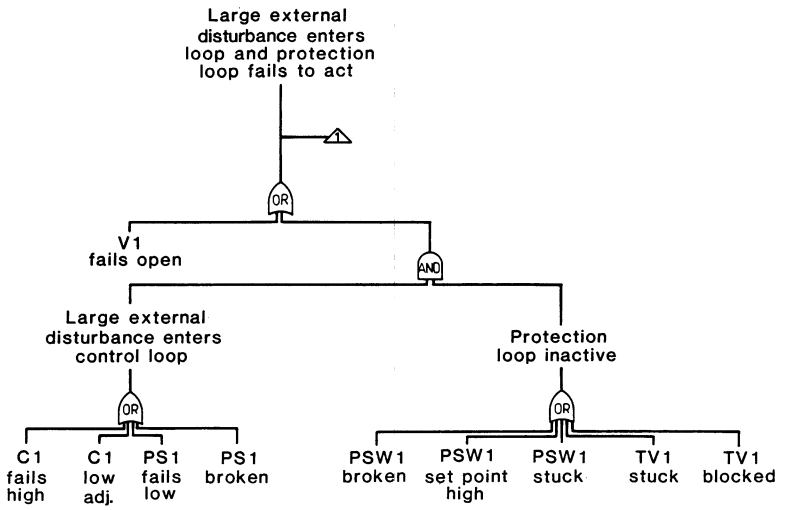

Fig. 7.—*contd.*

On activation, the pressure switch output signal (S17) is removed causing the three-way valve (TV1) to vent the compressed air supply. The result of the venting is a sudden loss of pressure to the valve actuator which is of the air-to-open type and the valve (V1) slams shut.

The control action for valve V1 is provided by the NFBL consisting of nodes M3, P3, S19, P20 and P18. There are three ways that a NFBL either causes or passes a very large disturbance. Developing each of the three branches as shown in Fig. 7, accounting for failures of the protection loop, yields the final fault tree. To complete the study, the failure modes (minimal cut sets) of the system were determined and the undesired event probability was calculated using computer programs.

6 DISCUSSION

Digraph analysis has been shown to provide a good intermediate step in the process of fault tree construction. The algorithm which converts the digraph to the fault tree has been found to yield good results when systems have contained control loops. The main advantage of the technique is its requirement for the analyst to have a rigorous understanding of the process and the way it is controlled. Component failure modes must be clearly identified and their effect on the system clearly defined. It is this

stage which requires the fault tree analyst to liaise with the design engineer in order to gain an accurate model of the plant.

It is felt by the authors that the construction algorithms must be carefully validated before widespread use of the digraph method is made in the form of a computer implementation. As such, some doubt must be cast on the confidence which can be placed in codes which automate the technique. It is also felt that the main advantage of applying the technique is the insight gained into the functioning of a system. This is partly lost in an automatic computerised approach.

For many applications the digraph technique provides an excellent aid to manual fault tree construction, but it is felt that the published algorithms need further development before being suitable for use.

ACKNOWLEDGEMENT

This paper is published by permission of the British Gas Corporation. The authors would like to acknowledge and thank their colleagues in the Production and Supply Division for the opportunity to apply the technique; without their co-operation the work would not have been possible. Thanks are also due to Dr Howard Lambert who provided constructive comments on the application of the digraph techniques presented in this paper.

REFERENCES

1. Morgan, J. M. and Andrews, J. D. Assessment of safety systems using fault tree analysis, *IGE Communication 1242*, presented at 50th Autumn meeting, November 1984.
2. Taylor, J. R. *IEEE Trans. Reliab.*, **R-31** (2), (1982), p. 137.
3. Martin-Solis, G. A., Andow, P. K. and Lees, F. P. *Trans. I. Chem. E.*, **60** (1982), p. 14.
4. Lapp, S. A. and Powers, G. J. *IEEE Trans. Reliab.*, **R-26** (April 1977), p. 2.
5. Lapp, S. A. and Powers, G. J. *Ind. Eng. Chem. Process Dies. Dev.*, **16** (4) (1977), p. 27.
6. Lambert, H. E. *IEEE Trans. Reliab.*, **R-28** (1) (1979), p. 6.
7. Allen, D. J. *Ind. Eng. Chem. Fundam.*, **23** (1984), p. 175.
8. Allen, D. J. and Rae, M. S. *Ind. Eng. Chem. Fundam.*, **19** (1) (1980), p. 79.
9. Andow, P. K. *IEEE Trans. Reliab.*, **R-29** (1) (1980), p. 2.

10. Dunglinson, C. and Lambert, H. E. *IEEE Trans. Reliab.*, **R-32** (2) (1983), p. 150.
11. Haasl, D. F. Fault tree handbook, *Report No. NUREG-0492*, US Nuclear Regulatory Commission, Washington, DC, January 1981.

APPENDIX: DERIVATION OF LOOP OPERATORS

Negative feedback loop (NFBL) operator

When establishing the possible causes for a NFBL to either pass or generate a disturbance then it is necessary to consider both component failure modes and categories of the input disturbance. In general, components which constitute the control are considered to have three possible classifications of failure mode:

Inactive—Causing a zero gain on the NFBL and providing no control action.
Reversal—Causing normal gain to be reversed. This is usually a revealed failure as the control loop is in an unstable condition.
Fail high or low—This type of component failure can actually initiate a disturbance within a loop.

In order to produce fault trees for NFBLs an operator has been developed by Lambert[6] which considers the loop in its entirety and gives combinations of component failures and input disturbances which can cause the output from the loop to deviate from its normal value. From these permutations there are three ways in which a NFBL can either cause or pass a disturbance.

(1) A device in the control loop can be in a reversed mode causing a reversal of the gain between two modes. This transforms the loop into a positive feedback loop (PFBL). In this situation the loop causes a disturbance as it amplifies noise and drives the loop unstable. Any odd number of devices reversed will cause this. But as fault tree analysis is concerned with the evaluation of the least number of individual failures which cause the undesired event and, as one reversal is sufficient, only single component reversals are included. Also failures allowing an even number of reversals to rectify the control loop are not allowed, since this violates Haasl's[11] rule, which does not allow fortunate failure combinations to be considered. The effect of this rule is to produce conservative results.

(2) An external disturbance too large or fast for the control loop to correct enters the loop. Such disturbances are sufficient to fail the NFBL on their own. Depending on the node in the loop at which these disturbances enter, they will either cause the output to deviate in a very high or very low manner. It is therefore necessary to select those disturbances of magnitude 10 which cause the output event currently being traced to go high or low. Typical events which appear under this category are the control loop components failing in high or low modes and disturbances of large magnitude (± 10) entering via the process variables.

(3) A moderate external disturbance can enter the loop and the loop be inactive because one or more control devices are inactive. By definition moderate (± 1) disturbances are those which the NFBL is able to cancel. Therefore if the disturbance is to pass through the loop without rectification, special attention must be given to where the disturbance enters the loop and which devices need to be inactive to prevent correction. If a deviation through the NFBL is achieved the following conditions must be met:

(i) No control devices should be inactivated from the point the disturbance enters the loop downstream to the loop variable under development.

(ii) At least one control device is inactive on the remainder of the loop.

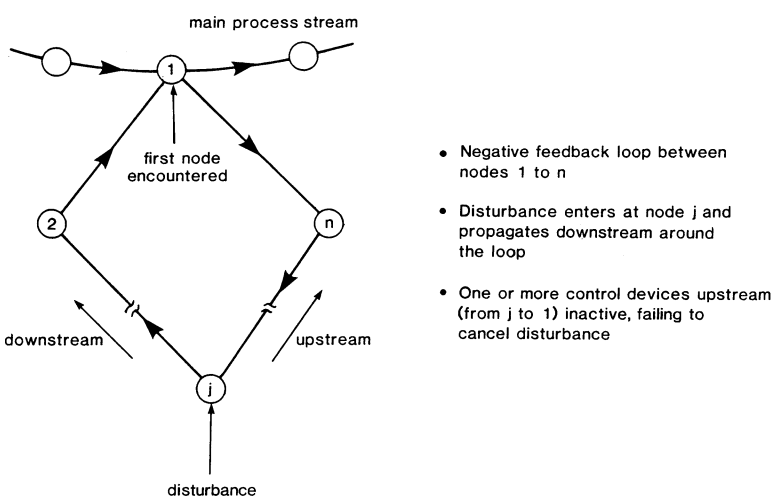

Fig. A1. Failure of NFBL for external moderate disturbances.

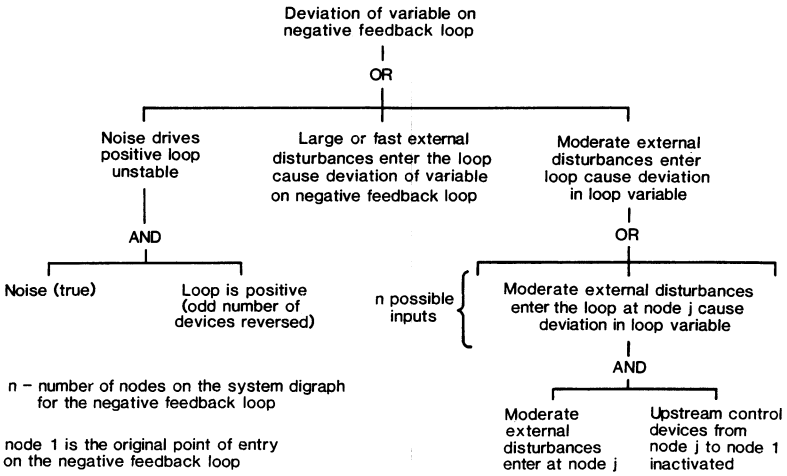

Fig. A2. Negative feedback loop operator.

As shown in Fig. A1, condition (i) allows the disturbance to propagate down the loop to the output node, whilst condition (ii) makes the loop inactive so that no corrective action is possible.

These three causes for a NFBL to pass or cause a disturbance are given in the form of an operator in Fig. A2. The operator is applied at the first instance a node on a NFBL is encountered. This first variable is called the original point of entry on the NFBL. Checks for logical consistency become important in applying the operator in fault tree construction.

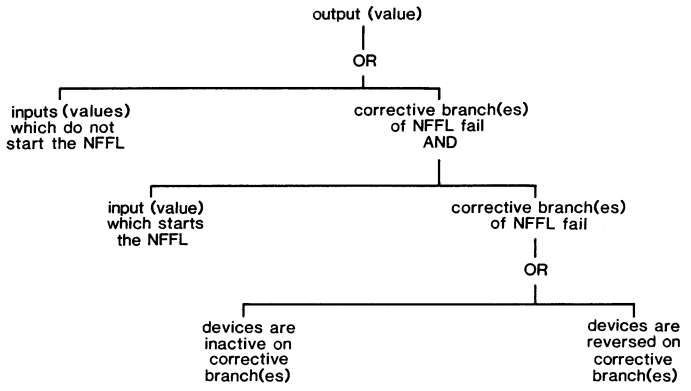

Fig. A3. Negative feedforward loop operator.

Negative feedforward loop (NFFL) operator

A NFFL has the ability to cancel disturbances only when they enter at the node which starts the NFFL. Disturbances encountered elsewhere on the loop will propagate through it. Working backwards on a digraph the node which terminates the NFFL is the first to be encountered. A disturbance at this point means that the NFFL has failed to give corrective action. This means that the disturbance entered the NFFL, propagated down the causative branch, and the corrective branch failed to cancel it. Reasons for failure of the corrective branch are as follows:

(1) A control device on the corrective branch is inactive (zero gain events) causing the NFFL to be inactive.
(2) A control device on the corrective branch is reversed, causing the loop to be positive.

The operator for a NFFL is given in Fig. A3. If a disturbance is traced to a node on the NFFL which does not terminate the loop the operator is not applied in this instance.