Application of the diagraph method of fault tree construction to a complex control configuration

This item was submitted to Loughborough University's Institutional Repository by the/an author.

Citation: ANDREWS, J.D. and BRENNAN, E.G., 1989. Application of the diagraph method of fault tree construction to a complex control configuration. [Presented at:] Reliability `89 : the National Reliability Conference, number 4C/4, London, UK, June.

Additional Information:

- This is a conference paper.

Metadata Record: [https://dspace.lboro.ac.uk/2134/3989](https://dspace.lboro.ac.uk/2134/3989)

Please cite the published version.
This item was submitted to Loughborough’s Institutional Repository (https://dspace.lboro.ac.uk/) by the author and is made available under the following Creative Commons Licence conditions.

For the full text of this licence, please go to: http://creativecommons.org/licenses/by-nc-nd/2.5/
APPLICATION OF THE DIGRAPH METHOD OF FAULT TREE CONSTRUCTION TO A COMPLEX CONTROL CONFIGURATION

J.D. Andrews,
Midlands Reliability Centre, Department of Mechanical and Production Engineering, Birmingham Polytechnic.
E.G. Brennan, Midlands Research Station, British Gas plc.

This paper describes the application of the digraph method of fault tree construction to a two-stream gas regulating system. The system features a complex, nested, control loop structure which makes the sequential use of the "operators" developed for the conventional application of this method inappropriate. Two new methods were developed which overcome this difficulty and retain the basic digraph formulation. The validity of implementing the digraph technique on a computer for automatic fault tree construction is discussed.

INTRODUCTION

In recent years fault tree analysis has become a well established, standard method for assessing the probability and frequency of occurrence of selected system failures. It has been extensively applied to determine the causes of unsafe or hazardous events associated with systems utilised in many industries such as aerospace, nuclear and chemical. Whilst the advantages of using such techniques are well known, especially if applied at the system design stage, there are also disadvantages. The major disadvantage is the time taken to perform this type of analysis. Once constructed, a fault tree can be analysed using one of the many programs currently available. However, for all but the simplest of systems the fault tree construction will be a very time consuming process. Also the logic used by different engineers during the construction will in all probability be different. This leads to trees which are not repeatable and consistent in their structure. There is therefore a considerable incentive to produce a fault tree construction algorithm which could be implemented on a computer and enable the whole of the fault tree analysis task to be automated and become less dependent on the experience of the engineer performing the analysis.

Various automated approaches have been devised to avoid the errors and tedium associated with manual fault tree construction. Salem, Apostolakis and Okrent\textsuperscript{1} implemented an automatic construction method called CAT (Computer Aided Tree) based on decision tables. Several more complex procedures have been proposed which resulted in the computer codes RIKKE\textsuperscript{2} and FAULTFINDER\textsuperscript{2}. The digraph or directed graph method is an algorithm developed for automating the construction process. It was first developed at Carnegie-Mellon University in the mid 1970's by Lapp and Powers\textsuperscript{8,9} with "operators" to deal with control loops added by Lambert\textsuperscript{10}. More recent developments have been proposed by Allen\textsuperscript{11,12}. A digraph provides an intermediate step which explicitly describes the relationships between process variables. The fault tree is then constructed by examining the cause-effect relationships indicated on the digraph. This method provides a consistent approach to fault tree construction which is well suited for modelling systems which include control loops. For computer programs formulated using the digraph algorithm the digraph must first be constructed and entered as input data. A digraph closely follows the system topology and can be easily constructed from a system flowsheet or engineering line diagram.

The basic digraph formulation has some pitfalls which have been identified by Andow\textsuperscript{13}, Andrews and Morgan\textsuperscript{14} and more recently by Kohda and Henley\textsuperscript{15}. Difficulties are encountered for systems where it is necessary to model the two way flow of information. Also when control loops are nested the conventional "operators" do not always produce a fault tree whose logical reduction gives cut sets which are both minimal and complete.

The gas regulation system analysed in this paper features a complex, nested control structure for which conventional "operators" are inadequate. In order to overcome these difficulties it was necessary to develop new approaches to construct the fault tree. Two methods were devised, the
first based on the control devices, the second on the control loop structures. A comparison of
the results obtained using both algorithms is made. Both approaches enable the retention of the
basic digraph formulation for manual application. The suitability of implementing the algorithm
on a computer is also discussed.

THE DIGRAPH METHOD

Fault tree construction based on the digraph method is a two step process. The digraph itself
provides an intermediate step in formulating a fault tree for some particular undesired system
event which is represented by the deviation in a process variable. Initially the digraph is
constructed to represent both the normal function of the system and also the effect of component
failures and deviations in the inputs to the system.

Fault tree construction is then carried out by tracing the causes of undesired deviations in the
top event process variable back through the system. The main features of this method are given
in the following sections. A more detailed description of the method can be found in references
8-10 and 14.

A digraph is a set of nodes together with a set of edges or lines which are drawn from one node
to another. The nodes are used to represent process variables in the system or events such as
components failing. When one process variable has the ability to affect another, a directed edge
is used to connect them. The direction of the edge is from the independent variable to the
dependent variable. Each edge has an associated number, termed gain, used to represent the
relationship between the nodes. Where numbers appear on their own the relationship is normally
true. In some situations conditions which define when the relationship applies are also
indicated.

The logic system used for digraphs consists of the numbers -10, -1, 0, +1 and +10 and these are
used in two distinct senses to represent both deviations in process variables and the gain
associated with edges.

Deviations. These are the discrete states which are used to express disturbances in the process
variables. When a variable achieves its normal expected value then the disturbance is
represented by 0. A disturbance of magnitude 1 indicates a range of values that is considered
moderate, that is an expected deviation which the system has the ability to control. Large
disturbances are indicated by a magnitude of 10 and these are defined as being beyond the
capacity of the system to rectify. The sign of the disturbance indicates whether it is above (+)
or below (-) the normal value.

Component failure states are represented by the nodes on the digraph the logic values 1 and
0 are used to indicate that the failure state exists or does not exist respectively.

Gains. Gains are the numbers placed on the directed edges to show the strength of relationships
between two variables. Values of 1 and 10 indicate moderate and strong relationships
respectively. If an edge links variable X to variable Y then the gain can be interpreted as
{\text{X} \rightarrow \text{Y}}. Therefore the sign is used to indicate the direction in which the dependent variable
changes when the independent variable is increased. A zero gain is used to indicate a
nullification of the relationship between two variables.

To obtain the deviation in the dependent process variable caused by a deviation in the
independent variable the general rule is to multiply the value of the independent variable
disturbance by the gain. For example if nodes representing variables X and Y are connected by an
edge with a gain of +1 and the deviation in X is 1 then Y is also found to have a 1 deviation.
When applying this rule it must be remembered that the maximum deviation magnitude is 10. So an
input of +10 to the independent node in a connected pair where the gain is +10 results in a
disturbance of +10 at the dependent node.

DIGRAPH CONSTRUCTION

To construct a digraph which can be used to develop a fault tree for a specific undesired event,
the first step is to identify the process variable deviation which represents the top event. The
digraph is then developed back from the top event process variable by considering both the
actions of components which could cause deviations in this variable and the laws of physics.
New, local variables which are added to the digraph and connected to the top event variable by
the appropriate edges are in turn further developed in the same manner.
The construction of the digraph is terminated when all the undeveloped variables on the diagram are those corresponding to inputs at the boundary of the system. Permissible deviations in these boundary variables should also be stated and may appear in the fault tree as basic events. Causes of these events are outside of the scope of the analysis and are not further developed.

**FAULT TREE CONSTRUCTION**

For simple systems which do not feature any control loops, fault trees can be developed very quickly by tracing the potential causes of a deviation in the top event variable back through the system digraph. In this situation the fault tree structure will be very simple with process deviations being combined by OR gates unless conditional edges are encountered. For a conditional edge the output variable deviation only occurs when the correct input deviation occurs and the stated condition exists.

However the main advantage of the digraph method is to analyse systems which do contain control loops. Simpler systems do not warrant the additional effort required to construct any intermediate steps. For complex systems fault tree construction can only proceed when all the control loops in the system have been identified and classified as either negative feedback or negative feedforward.

**Negative Feedback Loops**

When the loop is categorised as a negative feedback loop (NFBL) then it has the ability to correct moderate disturbances in the sensed process variable. 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.

This type of loop requires a special approach when encountered during fault tree construction. When tracing causes of the top event back through the digraph, on encountering the first node on such a loop an "operator" developed by Lambert is applied. The "operator" is essentially a list of all the ways in which NFBLs can generate or pass a disturbance. These are summarised below and illustrated in figure 1.

1. A NFBL causes a disturbance when the net gain is positive, ie an odd number of devices in the loop are reversed. In practice as one reversed device is sufficient to produce the minimal cut sets, only single reversals are considered. When the loop becomes positive it acts as an amplifier and will be driven unstable by noise.

2. A NFBL passes a disturbance if it is too large or fast for the control loop to correct.

A NFBL will pass a correctable disturbance if one or more control devices on the loop are inactive, provided they do not halt the propagation of the disturbance.

**Negative Feedforward Loops**

Whereas feedback loops correct disturbances which currently exist in the system a negative feedforward loop (NFFL) can, in theory, prevent the disturbance progressing through the system. It achieves this by sensing an upstream variable and manipulating a downstream variable. On a digraph a NFFL can be identified as having:

- Two or more paths from one node to another node.
- The sign of the product of the normal gains on one path is different from that of the others.
- Disturbances propagate along the path with the net positive gain, termed the causative branch, are controlled or cancelled by the path with the net negative gain, the corrective branch.

A NFFL can only cancel disturbances which enter at the node which starts the loop i.e. the sensed source disturbance enters the loop at some point other than the first node. These disturbances are not sensed by the NFFL and pass uncorrected through the system.
2. A correctable source disturbance enters the loop at the sensed node but the WFPL fails to correct them. The failure of the loop can be caused by either inactive or reversed devices.

**APPLICATION TO A PRESSURE/VOLUMETRIC REGULATION SYSTEM**

The digraph method is demonstrated by its application to the pressure/volumetric regulation system described below.

**System Description**

The system analysed is a typical configuration used for high reliability pressure/volumetric regulation installations which connects the national gas transmission system to the regional streams, one stream normally in operation, the other on standby and brought on-line in the event of a failure. Each stream consists of three elements, a slam shut valve (SS), a pressure control valve (PCV) and a flow control valve (FCV) as shown in figure 4.

In normal operation constant flow is maintained by a volumetric controller (VC), which is a direct acting electrical-pneumatic controller. The VC receives its input signal from the on FCV which control unacceptable pressure levels. PCL controls at the minimum low pressure and having pneumatic input and output. The FCV controlling signal is chosen by two signal selectors in series and these are pneumatic relays. The first selector takes the highest signal from VC and PCL and the second takes the lowest of this signal and the one from PCH.

The pressure control valve PCV maintains the correct pressure in the line. PCV is normally controlled by PC but also has an on-ride controller PGO. PC and PGO are both direct acting pneumatic controllers with PGO set at a value above PC such that if the PCV fails open, PGO will shut down PCV accordingly.

The final level of protection is given by the slam-shut valve (SS) controlled by the pressure switch PS. SS will close if the pressure is unacceptably high and once shut requires manual reset.

In the standby stream the slam-shut valve is normally open. PCV is normally closed (manually), but receives its signal from the same VC as the on-line stream. The pressure control valve on the redundant stream is also left closed, with its controller PGO set lower than that on the other stream. In the event of a failure on one stream the outlet pressure decays and the second stream is activated by PGO. Once the standby stream is selected P.C.V. responds to the signal from VC and control is re-established.

Two failure events were considered. The first is the situation where all three valves on either stream are open giving rise to a high flow rate through the system. The second event is that which causes control to pass to the standby stream i.e. no mass flow at the outlet. Any valve closing on the stream would give rise to this transition. The causes of both of these outcomes have been deduced by modelling a single stream of the system.

Table A gives a list of the component failure modes assumed in the analysis and also the code names used to represent them.

**Digraph Construction**

Having identified the failure modes for each component and the effect that each of these types of failure would have on the system performance, the component models can be collated to form the system digraph.

The first step is to number all the sections of the schematic process diagram as shown in figure 4 for a single stream of the pressure regulation system. In this example, the main flow stream sections were numbered first followed by the loop structures nested on each of the three valves starting at the valve nearest the outlet and working back towards the inlet. Both undesired events for which a fault tree was to be constructed related to the flow rate condition at (low), stream closed. As each digraph is dependent upon the top event the construction processes can cause a deviation in this variable. The result of this procedure is initially to trace digraph are also developed in this way until the digraph contains no undeveloped nodes. At this point the system digraph represents the functioning of the regulation system under normal working conditions. The final stage to obtain the complete system digraph is to add the effects
### TABLE A: Component Failure Modes

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
<th>Failure Modes</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS</td>
<td>Slam shut valve (A/C)</td>
<td>Stuck open</td>
<td>SSO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fails closed</td>
<td>SSc</td>
</tr>
<tr>
<td>PCV</td>
<td>Pressure control valve (A/C)</td>
<td>Fails open</td>
<td>PCVO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fails closed</td>
<td>PCVC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fails stuck</td>
<td>PCVS</td>
</tr>
<tr>
<td>FCV</td>
<td>Flow control valve (A/O)</td>
<td>Fails Open</td>
<td>PCVO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fails closed</td>
<td>PCVC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fails stuck</td>
<td>PCVS</td>
</tr>
<tr>
<td>PZ</td>
<td>Slam shut valve controller switch</td>
<td>Reversed</td>
<td>PZR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set point low</td>
<td>PZSPH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set point high</td>
<td>PZSPH</td>
</tr>
<tr>
<td>PCO</td>
<td>Pressure control valve override controller</td>
<td>Reversed</td>
<td>PCOR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set point low</td>
<td>PCOSPL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set point high</td>
<td>PCOSPH</td>
</tr>
<tr>
<td>PC</td>
<td>Pressure control valve controller.</td>
<td>Reversed</td>
<td>PCR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set point low</td>
<td>PCSPH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set point high</td>
<td>PCSPH</td>
</tr>
<tr>
<td>PCH</td>
<td>Flow control valve high pressure override controller.</td>
<td>Reversed</td>
<td>PCHR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set point low</td>
<td>PCHSPL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set point high</td>
<td>PCHSPH</td>
</tr>
<tr>
<td>PCL</td>
<td>Flow control valve low pressure override controller.</td>
<td>Reversed</td>
<td>PCLR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set point low</td>
<td>PCLSPH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set point high</td>
<td>PCLSPH</td>
</tr>
<tr>
<td>VC</td>
<td>Flow controller</td>
<td>Broken (no signal out)</td>
<td>VCB</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set point low</td>
<td>VCSPL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set point high</td>
<td>VCSPH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reversed</td>
<td>VCR</td>
</tr>
<tr>
<td>S1</td>
<td>Selector relay 1 (between PCO and PC)</td>
<td>Broken (no signal out)</td>
<td>S1B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stuck on channel A (PCO)</td>
<td>S1SPCO</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stuck on channel B (PC)</td>
<td>S1SPC</td>
</tr>
<tr>
<td>S2</td>
<td>Selector relay 2 (between VC and PCL)</td>
<td>Broken (no signal out)</td>
<td>S2B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stuck on channel A (VC)</td>
<td>S2SVC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stuck on channel B (PCL)</td>
<td>S2SPCL</td>
</tr>
<tr>
<td>S3</td>
<td>Selector relay 3 (between S2 and PCH)</td>
<td>Broken (no signal out)</td>
<td>S3B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stuck on channel A (S2)</td>
<td>S3SS2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Stuck on channel B (PCH)</td>
<td>S3SPCH</td>
</tr>
</tbody>
</table>
contributed by each failure mode of each component. These additions will take the form of modified edge relationships or input disturbances depending on the nature of the failure condition.

To illustrate the technique a detailed explanation is given for the most complex control loop configuration in the system, that which controls the Flow Control Valve (FCV). From this explanation the method used to construct the remainder of the digraph will be apparent.

Figure 5a shows the initial stage of the development of the digraph where the relationships affecting the mass flow along the main process stream have been developed. The gain between nodes representing mass flow in each section must be the same, so a variation in one section is communicated through the whole stream. The rate at which the fluid enters the regulation station, M0 is monitored and a signal representing its value is sent from the station flow meter (failures of which are not included in this analysis) to the volumetric controller VC. Therefore the variable M0 affects the variable S19, the signal level at location 19 as shown in Figure 5b. On examination it is found that if M0 increases the signal level decreases. This results in a gain of -1 between these two nodes. The volumetric controller itself is a direct acting electrical-pneumatic controller which receives the electrical signal S19 and varies the pneumatic pressure in location 18. As it is direct acting this results in a +1 gain between these nodes. The system then features the two selector relays which bring in the high pressure and low pressure over-ride systems as necessary. Under normal circumstances these selectors will allow the pressure from VC to manipulate the FCV position so the digraph will feature nodes P17 and P14 whose connecting edges have gains of +1. Valve FCV is of the gas to open variety and so an increase in P14 opens the valve increasing the flow rate in stream 6 (M6). These two nodes are therefore connected with an edge which also has a +1 gain and this path has now rejoined the main process stream. As the two selectors S2 and S3 only pass the signal according to the selection conditions, as explained in the system description, these conditions are also included in the digraph. The two paths now illustrated on the digraph can be categorised by the description given earlier, as representing a negative feed-forward loop. Path M0-M1-M2-M3-M4-M5-M6 is the corrective branch with a net gain of +1 and path M0-S19-P18-P17-P14-M6 is the corrective branch with a negative +1 gain.

The control mechanism on FCV is also dependent upon the high and low pressure regulation circuits. For the high pressure feedback loop the pressure at location 6 is the same as that at location 12. PCH, like PCL, is an inverse acting controller so as the pressure in section 12 increases (decreases) PCH decreases (increases) the pressure in location 13. This pressure is communicated to P14 by the selector S3 providing the pressure is less than that emitted from selector-S2. Figure 5c shows the digraph which includes both this loop and that governing the low pressure situation.

The final stage in digraph development is to include the effects which component failure will have on the system variables. Some of these, such as FCV sticking or PCL reversed will change the way one variable affects another and will change the gain between them.

For example, if the valve sticks then any pressure change on the valve head will not move the valve position and so control action cannot be communicated to affect the flow rate. The relationship normally existing between these two variables is nullified, as represented by the zero gain. In the terminology used in the analysis 'reversed' means that the component is switched from inverse acting to direct acting or vice versa. This type of failure may be introduced during installation or maintenance and it can be argued that on negative feedback control the loop becomes positive feedback and that noise will drive the system high or low, which would be rectified during commissioning or testing. However with nested loop structures such as that controlling FCV this is not the case. The signal selection process means that reversed loops are never utilised.

Component failure modes which introduce disturbances to the system can also be illustrated by the FCV. If the valve fails closed the mass flow at the outlet will be zero i.e. a very low level which control action cannot rectify (-10 in digraph terminology). Similarly a very high uncontrollable flow rate, +10, results if the valve drives wide open. These component failure modes are included as events which introduce disturbances to the system. The component failure modes for the control system for FCV have been included on the digraph in Figure 5d.

Consideration of the control processes for SS and FCV in the same manner results in the complete system digraph illustrated in Figure 5e.
Fault Tree Construction

Construction of the fault tree then proceeds by examining the information flow on the digraph and determining the immediate causes of the undesired deviation in the top event variable. The disturbance is traced back to other possible local causes. These local variable deviations are in turn further developed until all events in the tree have been considered. If control loops exist in the system and are encountered during the fault tree development the correct "operator" is applied. The procedure is therefore dependent upon the type of loops appearing on the digraph. Identification and classification of the control loop as either feedback or feedforward is therefore very important.

When systems which feature simple feedback or feedforward control are encountered then the algorithm applying the "operators" as developed by Lambert has been successful in producing accurate fault trees. However, as noted by Andrews and Morgan and Kohda and Henley, when complex overlapping or nested control loops are present the direct application of these "operators" is not appropriate. As will be discussed later it is also difficult for automatic fault tree construction computer codes which are based on the digraph algorithm to classify control loops as feedforward or feedback.

The flow regulation system features complex control loops which fall into the category of those which prohibit the direct application of "operators". To construct the fault tree for this system two approaches were used and each was carried out by a different analyst.

Method 1

The first method was based on engineering knowledge of the system together with the information contained on the digraph. Prior to the fault tree construction all loops were identified and classified as either feedback or feedforward. Causes of deviations in the top event process variable were then traced in the normal manner until a control loop was encountered. Attention was then focussed on the control devices rather than the whole loop structure. Whatever the nature of loop structures which exist in a system, process variables can only be manipulated or changed by the control devices i.e. in this case the valve. Once the action of the control device which contributes to the top event is identified the causes of this action can then be traced. This method results in an "expanded operator" applied to the loops nested on each control device. Detailed development of each of the branches is then completed by tracing the deviations in the process variables which manipulate the control device.

The fault tree structures obtained from this method for both top events high mass flow at the outlet and low mass flow at the outlet are illustrated in figures 6 and 7 respectively.

Method 2

As with the first method the nature of the control loops was established prior to the fault tree construction. Also an "operator" based on the overall control structure was developed and applied. However in this method the "operator" was derived in terms of the failure modes of each control loop structure rather than the loop components as used in the conventional failure modes method. This means that branches of the "operator" featured failure modes for each control loop for which the "mini-operators" developed by Lambert were then used to further develop the tree. Account must be taken of contradicting states of components common to more than one loop.

To help illustrate this method, the tree structure for failures of the nested control loops have been included down to the level where the conventional "operators" are applied. These are shown for high mass flow at the outlet in figure 8 and for low outlet mass flow in figure 9. The full fault trees are not included in this paper as they were larger and not as well structured as those derived using the first method.

Both methods produced identical minimal cut sets for each top event, indicating that the logic for both approaches was consistent.

COMPUTER IMPLEMENTATION OF THE DIGRAPH METHOD

Experience gained in utilizing the digraph method of fault tree construction for several different engineering systems has indicated some areas of difficulty where the rigour of the method is called into question. Below, some of these situations are illustrated and discussed using small systems commonly found in engineering.
a) The Mixer Tee

Figure 10a illustrates a simple mixer tee where liquids flowing in inlet streams A and B are combined into one outlet stream C. The digraph showing the normal relationship for mass flow in this system is shown in figure 10b. In a process where the event "no mass flow at outlet" was of importance difficulties may arise if a fault tree was constructed using a digraph algorithm automated on a computer. The top event can only be expressed in digraph terms as very low mass flow at outlet stream C i.e. M3(-10). The fault tree for this event should then be:

```
No Mass Flow at Outlet
  |                 
  (M3 (-10))       
  |                 
AND                
  M1 (-10)         
  |                 
  M2 (-10)         
```

As NO flow at the outlet can only occur if there is no flow in either inlet stream, this requires the tree to have an AND gate.

However, as this can only be represented as M3 (-10) in digraph terminology a submission of this digraph to an automatic algorithm would give the fault tree:

```
(M3 (-10))  
 |           
OR          
  M1 (-10)  
  |           
  M2 (-10)  
```

This would be correct if the event to be traced was "very low flow at outlet" rather than "zero flow at outlet". The inability of the technique to deal explicitly with the zero level within its five discrete categories and distinguish between these two events can lead to totally erroneous cut sets. This is particularly true if the situation occurred at a position high in the fault tree structure.

b) Disturbances beyond the ability of the control loop to rectify

Deviations in process variables which are of magnitude 10 are defined as being beyond the capacity of a control loop to rectify. Very low (-10) and very high (+10) disturbances are traced through the digraph in the same way. However these two categories do not always behave in the same way. For example consider two MFBL's in series used to control the flow rate of a liquid as illustrated in figure 11. Failure of a component in the first loop in such a mode as to produce a very high mass flow out of the loop (e.g. valve fails open) results in the output node attaining the value M(+10).

It has a +10 value because the disturbance is beyond the ability of the first loop to control. However this is a definition local to the first loop since if the second loop is working correctly it should have the ability to rectify the disturbance. Therefore the M(+10) value at the exit of the first loop needs to be considered as a moderate, correctable disturbance on entry to the second.

This is not the case for a very low disturbance, of magnitude -10. Again, considering the series system of loops shown in figure 11, the event valve fails closed on the first loop causes a disturbance to the mass flow process variable which, since the loop cannot rectify the situation, is -10. However in this case since very low flow will exist beyond the first control valve even a fully open valve later in the stream cannot provide correcting action. Hence in this case the -10 magnitude is a global definition, since it cannot be rectified by the second loop and should not be converted to a moderate, -1, deviation in following its effect through the system.

4C/4/8
Inclusion of this type of consideration would not be directly available when automating the standard digraph/fault tree method.

c) Control loop identification

Consider the two control loops illustrated in figure 12a and 13a. The loops are both used to control the flow rate and comprise a sensor, a controller and a control valve. The first loop, system A, senses the flow rate and manipulates the upstream control device to correct disturbances. System B is very similar to system A but in this case the control action is provided downstream of the sensor. Digraphs are illustrated for both of these systems and fault trees developed to provide causes for the event low mass flow at the outlet of each loop.

From the digraph of system A (figure 12b) control action is categorised as being an NFPL since it has a path which starts and terminates at the same node, M2, and whose normal net gain is negative. The fault tree is drawn for this system using the appropriate NFPL "operator" and is shown in figure 12c. The minimal cut sets resulting from this fault tree are shown in figure 12d.

Investigation of the digraph of system B (figure 13b), shows that there are two paths between nodes M1 and M3. Path M1-M2-M3 and M1-P1-P4-P5-M3. The normal gains on these paths are of opposite sign. This categorises the loop structure as an NFPL where the first path is the propagation path and the second is the corrective path. Applying the appropriate "operator" to this yields the fault tree illustrated in figure 13c whose resulting minimal cut sets are also given (fig 13d).

The cut sets for the two systems are different. This is due to the categorisation of system B as a NFPL. However negative feedforward loops do not have the characteristic of generating disturbances. The loop labelled system B could do this if an odd number of devices were reversed creating a positive loop. The error in the digraph constructed for this system is that edges should also exit directed backwards along the path M3-M2-M1 thus revealing it as an NFPL. The edges can be directed backwards because mass flow must be equal at all points in the pipe and changes will propagate in both directions.

It may be easy to identify manually the occurrence of incorrect loop classification for such a simple system but this becomes more difficult for more complex situations. If additional edges were included to model the two-way communication of flow then automatic application of an algorithm to identify and classify control loops would now find an NFPL structure situated on node M2 and also a NFPL existing between nodes M1 and M3. This situation exists for the flow regulation system; consider the loops paths M0-H1-M2-M3-M4-M5-M6 and M0-S19-P18-P17-P14-M6 in figure 5e. Were all bi-directional relationships to be included on a digraph it would become cluttered and complex and would make the identification of loops more difficult rather than clarify the situation. As the digraph stands this loop is erroneously categorised as feedforward.

d) The pressure/mass flow relationship

Difficulties have also been encountered using the digraph method to model relationships between pressure and mass flow. An increase in pressure at any point in the system does not necessarily increase the flow rate as it is the pressure difference which is the governing influence. The digraph formulation does not facilitate the representation of this situation.

CONCLUSIONS

The major advantage to be gained by the manual application of the digraph method to fault tree construction is the knowledge of the system imparted to the engineer whilst carrying out the investigation. The technique also forces a structured approach whereby different analysts are more likely to produce fault trees of consistent logic for the same system. Even for systems which contain complex control loop configurations, such as the gas regulation system, accurate, well structured fault trees can be developed.

Whilst the technique works well when used manually, it is not yet refined to the degree of complexity where it is rigorous enough for implementation on a computer for automatic fault tree construction. In particular difficulties are encountered in the following areas:

1) The five discrete states used do not adequately allow the distinction between a zero level and a very low level disturbance of a process variable.
ii) The distinction between controllable and uncontrollable disturbances is difficult to define in a consistent manner at all positions within the system.

iii) It is difficult to ensure the correct identification of control loop's or to construct the digraph in such a way that control loops can be correctly identified under all circumstances.

REFERENCES


ACKNOWLEDGEMENT

This paper is published by permission of British Gas plc. The authors would like to acknowledge and thank Mr C Musgrave in the Production and Supply Division without whose co-operation the work would not have been possible and Miss J. Adamson, formerly of Midlands Research Station, for her contribution to the system analysis.
FIG. 1 NEGATIVE FEEDBACK LOOP OPERATOR
FIG. 2 NEGATIVE FEEDFORWARD LOOP OPERATOR
FIG. 3 TYPICAL ARRANGEMENT OF A VOLUMETRIC REGULATOR
FIG. 5a DIGRAPh CONSTRUCTION FOR VOLUMETRIC REGULATOR STAGE 1

FIG. 5b DIGRAPh CONSTRUCTION FOR VOLUMETRIC REGULATOR STAGE 2
FIG. 5c  DIGRAPH CONSTRUCTION FOR VOLUMETRIC REGULATOR STAGE 3
FIG. 5d DIGRAPH CONSTRUCTION FOR VOLUMETRIC REGULATOR STAGE 4
FIG. 5e  COMPLETE SYSTEM DGRAPH FOR VOLUMETRIC REGULATOR
FIG. 6  FAULT TREE FOR HIGH PRESSURE AT VOLUMETRIC REGULATOR OUTLET
FIG. 7  FAULT TREE FOR LOW FLOW AT VOLUMETRIC REGULATOR OUTLET
FIG. 8 NESTED LOOP "EXTENDED OPERATOR" FOR HIGH MASS FLOW AT VOLUMETRIC REGULATOR OUTLET
FIG. 9 NESTED LOOP "EXTENDED OPERATOR" FOR LOW MASS FLOW AT VOLUMETRIC REGULATOR OUTLET
FIG. 10a  MIXER TEE

FIG. 10b  DIGRAPh OF NORMAL FUNCTIONING OF MIXER TEE
FIG. 11 SYSTEM OF TWO N.F.B.L.'S IN SERIES
FIG. 12a CONTROL LOOP SYSTEM A

FIG. 12b CONTROL LOOP DIGRAPH FOR SYSTEM A

FIG. 12c FAULT TREE FOR LOW FLOW AT OUTLET OF SYSTEM A
1) CONT. REV
2) VALVE REV
3) CONT. BROKEN
4) CONT. SET PT LOW
5) VALVE CLOSED
6) M1(LOW), VALVE STUCK

FIG. 12d MINIMAL CUT SETS FOR SYSTEM A
FIG. 13a CONTROL LOOP SYSTEM B

FIG. 13b CONTROL LOOP DIGRAPH FOR SYSTEM B

FIG. 13c FAULT TREE FOR LOW FLOW AT OUTLET OF SYSTEM B
1) VALVE CLOSED
2) CONT. BROKEN
3) CONT. SET PT LOW
4) CONT. SET PT HIGH, VALVE REV
5) SEN. BROKEN, CONT. REV
6) SEN. BROKEN, VALVE REV
7) VALVE STUCK, M1(LOW)
8) VALVE REV, M1(LOW)
9) CONT. REV, M1(LOW)

FIG.13d MINIMAL CUT SETS FOR SYSTEM B