Studies on the Digraph-Based Approach for Fault-Tree Synthesis. 1. The Ratio-Control Systems

Chuei-Tin Chang* **and Kuo-Shu Hwang**

Department of Chemical Engineering, National Cheng Kung University,
Tainan, Taiwan 70101, Republic of China

The development of a systematic diagraph-based fault-tree synthesis procedure for complex ratio-control systems is presented in this paper. First, the feasibility of the established techniques in handling the single-NFBL (NFBL = negative feedback loop) ratio-control systems is verified with an example. Next, the diagraph structure of systems with multiple NFBLs is described and analyzed in detail. On the basis of qualitative simulation of the fault propagation patterns, the corresponding generalized fault-tree structures are then established. It can be observed clearly from the results of steady-state analysis that none of the existing procedures are capable of producing the correct fault trees for the more complex ratio-control systems. Also, to demonstrate the effectiveness of our techniques, successful application of the proposed structure to a caprolactam reaction process is shown. Finally, the resulting fault tree is compared with one obtained from a single-NFBL system and the trade-off between the two in terms of system safety is assessed accordingly.

Introduction

Ratio control is a standard control technique implemented routinely in numerous important chemical processes. Basically, it is a special type of feedforward control where two disturbances (loads) are measured and held in a constant ratio to each other. In most instances, ratio-control strategy is applied to control the flow ratio of two streams, e.g., it is used to (i) control the ratio of two reactants entering a reactor at a desired value, (ii) keep the fuel/air ratio in a burner at its optimum, (iii) hold the reflux ratio constant in a distillation column, (iv) sustain a constant ratio of flow rates associated with the purge stream and recycle stream in a chemical plant, and (v) maintain a constant ratio of the liquid flow rate to the vapor flow rate in an absorber (in order to achieve the desired composition in the exit vapor stream), etc. From these examples, one can see that a ratio-control system is needed to ensure the proper operation of many pieces of essential processing equipment. Malfunctions in these processes may have serious consequences. It is thus in our interest to evaluate the risk of possible hazardous events in ratio-control systems using fault-tree analysis.

In previous publications (Chang and Hwang, 1992; Chang *et al.*, 1993), the authors proposed a fault-tree synthesis algorithm which is quite effective in many realistic applications. This algorithm is essentially an improved version of the popular digraph-based method (Lapp and Powers, 1977; Shaeiwitz *et al.*, 1977; Chamow, 1978; Lambert, 1979; Lapp and Powers, 1979; Allen and Rao, 1980; Cummmings *et al.*, 1983; Allen, 1984; Andrew and Morgan, 1986, Andrew and Brennan, 1990). In particular, generalized fault-tree structures (operators) corresponding to various digraph configurations, i.e., tree, feedforward loop (FFL), and feedback loop (FBL), were developed for systems with coupled control and *process* loops. Also, in a series of papers concerning the propagation of faults in process plants, Lees and his co-workers reported similar results obtained with a different approach (Hunt *et al.*, 1992a-f).

In a simple ratio-control system, the flow rates of the two streams are both measured but only one is controlled, e.g., see Figure 1a. Generally speaking, the fault trees for such systems can be constructed by existing techniques without difficulties. However, problems may arise in more complex cases. If, for example, the throughput of the process is required to be maintained at a constant rate, then the flow rates of both streams should be controlled. In the corresponding system digraph, a negative feedforward loop (NFFL) is tangled with two negative feedback loops (NFBLs). A direct application of the procedure

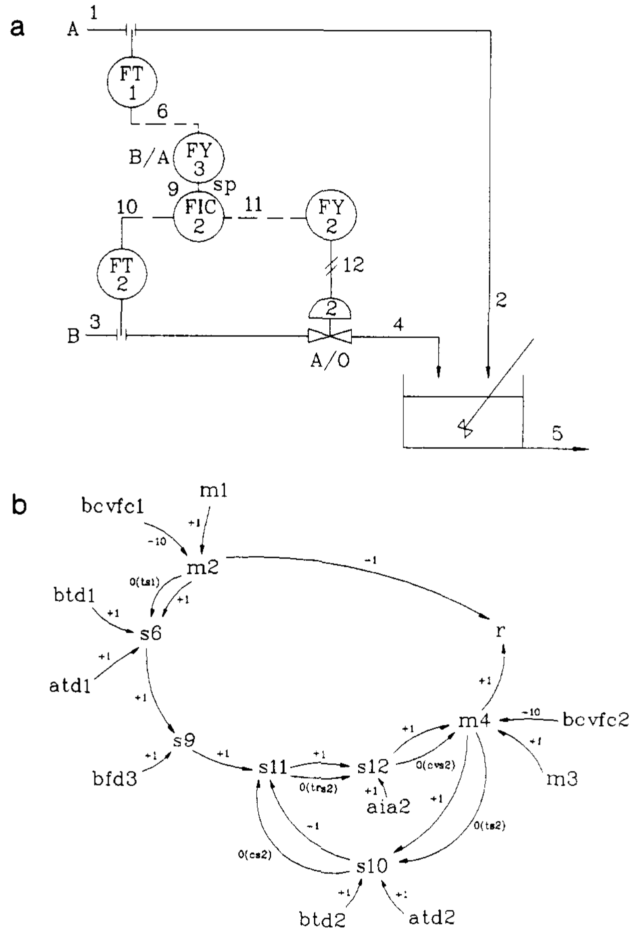

Figure 1. *(a) P&ID of the caprolactam reactor with a single-NFBL ratio-control system.* (b) Digraph of the single-NFBL ratio-control system in part a.

* Author to whom correspondence should be addressed. E-mail: NCKUT047@TWNMOE10.BITNET.

0888-5885/94/2633-1520$04.50/0

suggested by Chang and Hwang (1992) or Lees (Hunt *et al.*, 1992c) fails to produce correct results due to the presence of unique failure mechanisms not considered before. Notice that still more complicated digraph configurations can be found in other ratio-control systems, e.g., the "full metering control" of the air/fuel ratio to a boiler (Smith and Corripio, 1985) in which a NFFL is coupled with three NFBLs. The conventional fault-tree synthesis method is certainly not applicable to those problems either. Thus, there is a definite need to modify the present approach for constructing fault trees corresponding to these more complex ratio-control systems.

We have developed a systematic procedure for this purpose. In this paper, the feasibility of the established techniques in handling the simple single-NFBL ratio-control systems is first verified with an example. Next, the digraph structure of systems with multiple NFBLs is described and analyzed in detail. On the basis of qualitative simulation of the fault propagation behaviors (Oyeleye and Kramer, 1988; Chang and Hwang, 1992), the derivation of the generalized fault-tree structures is then presented. It can be observed clearly from the results of our qualitative steady-state analysis that none of the existing procedures are capable of producing the correct fault trees for complex ratio-control systems. Also, to demonstrate the effectiveness of our techniques, successful application of the proposed structure to a caprolactam reaction process is shown next. Finally, the resulting fault tree is compared with one obtained from a single-NFBL system. As a result of this exercise, the trade-off between the two in terms of system safety can be easily determined.

Fault-Tree Synthesis Procedure for Ratio-Control Systems with a Single NFBL

For illustration purposes, a simple example is used throughout this paper. Let us consider the production of caprolactam with cyclohexanone oxime (reactant A) and oleum (reactant B) in a continuous reactor. The feed ratio of B to A is required to be maintained at some desired value. If this ratio is considerably lower, the hazardous condition of high reactor temperature may occur due to rapid polymerization of cyclohexanone oxime. For the moment, let us assume that it is not necessary to control the throughput and, thus, only a simple ratio-control system is sufficient for operating the reactor. The piping and instrumentation diagram (P&ID) of this process is presented in Figure 1a. In this system, the flow of stream A cannot be controlled, just measured. This flow is usually referred to as a "wild flow." The measurement signal of the wild flow obtained from the sensor–transmitter FT1 is multiplied by the desired value in the ratio station FY3 to calculate the required flow of stream B. The output of FY3 is then used as the set point of the flow controller for stream B, FIC2. The controller FIC2 receives the measurement signal of stream B from sensor–transmitter FT2 and manipulates the control valve through a converter FY2 which transforms the electrical signal to a pneumatic signal.

The corresponding system digraph is presented in Figure 1b. The physical meanings of the symbols used in this digraph can be found later in the Nomenclature section. Since the digraph convention adopted here has already been well documented in the literature, e.g., Lapp and Powers (1977), no further explanations will be provided in this paper. From Figure 1b, one can observe in this system that the NFFL

$$\left\{\begin{array}{l} m2 \xrightarrow{-1} r \\ m2 \xrightarrow{+1} s6 \xrightarrow{+1} s9 \xrightarrow{+1} s11 \xrightarrow{+1} s12 \xrightarrow{+1} m4 \xrightarrow{+1} r \end{array}\right\} \qquad (1)$$

is coupled with a NFBL, i.e.,

$$s11 \xrightarrow{+1} s12 \xrightarrow{+1} m4 \xrightarrow{+1} s10 \xrightarrow{-1} s11 \qquad (2)$$

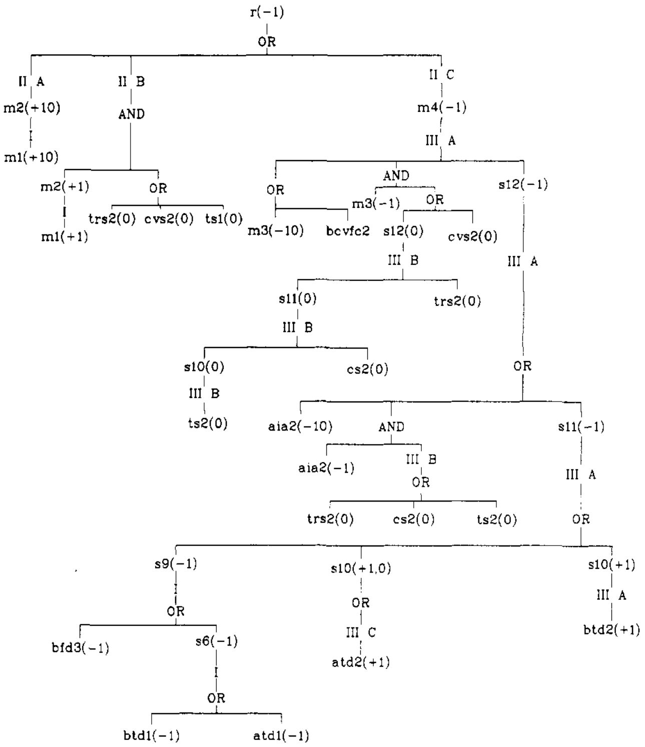

Figure 2. Fault tree of the single-NFBL ratio-control system shown in Figure 1.

To construct the fault tree associated with the top event High Reactor Temperature, it is necessary to identify the causes of $r(-1)$, which are associated with the event Low Flow Ratio. Notice that r is the end node of the NFFL (1) and three of the nodes, $s11$, $s12$, and $m4$, on the second path of this NFFL are also on the NFBL (2). This would normally imply that the disturbances entering the NFFL from $m2$ cannot pass through the second path of (1) owing to the regulatory action of (2). However, it should also be noted that the input to $s11$ on this path is $s9$. Unlike other off-NFBL inputs, the effects of the disturbances originated from $s9$ are uncontrollable. This is due to the fact that $s9$ represents the set-point value and a change in $s9$ is guaranteed to pass through the feedback control loop. More specifically, the results of $s9(+1)$ are $s11(+1)$, $s12(+1)$, $m4(+1)$, and $s10(+1)$. Therefore, the NFBL (2) can be considered as the "slave" of the master control loop NFFL (1). The control action of the NFFL is unaffected by the NFBL if all its components function properly. As a result, the fault-tree structures (structures I–III) proposed by Chang and Hwang (1992) are directly applicable in this situation. For illustration purposes, they are also included in Appendix A of this paper. The implementation procedure of these structures is essentially the same as that adopted in all the previous publications and, thus, will not be detailed here for the sake of brevity.

For this present example, the fault tree obtained with the above approach can be found in Figure 2. Notice that the event $m2(+10)$ is placed under substructure IIA. This is due to our assumption that the flow-control loop of stream B is saturated by such a large deviation in $m2$.

Also, under substructure IIC, events associated with nodes on the NFBL (2) must be included. In developing such events, the standard fault-tree structure, structure III, can be applied without modifications. Notice that the detailed synthesis process of these three structures is labeled clearly in this fault tree.

The Digraph Structure of Ratio-Control Systems with Multiple NFBLs

In order to achieve the production target of a plant, it is often necessary to maintain the throughput of the reactor at a desired rate. If this constraint is required in operating the caprolactam reactor, then an additional flow control system must be installed on stream A (Figure 3a). The diagraph for this system is shown in Figure 3b. Here, one can observe that two NFBLs exist:

$$m2 \xrightarrow{+1} s6 \xrightarrow{-1} s7 \xrightarrow{+1} s8 \xrightarrow{+1} m2 \tag{3}$$

and

$$m4 \xrightarrow{+1} s10 \xrightarrow{-1} s11 \xrightarrow{+1} s12 \xrightarrow{+1} m4 \tag{4}$$

In addition, there are two feedforward loops:

$$\left\{\begin{array}{l} m2 \xrightarrow{-1} r \\ m2 \xrightarrow{+1} s6 \xrightarrow{+1} s9 \xrightarrow{+1} s11 \xrightarrow{+1} s12 \xrightarrow{+1} m4 \xrightarrow{+1} r \end{array}\right\} \tag{5}$$

and

$$\left\{\begin{array}{l} s6 \xrightarrow{-1} s7 \xrightarrow{+1} s8 \xrightarrow{+1} m2 \xrightarrow{-1} r \\ s6 \xrightarrow{+1} s9 \xrightarrow{+1} s11 \xrightarrow{+1} s12 \xrightarrow{+1} m4 \xrightarrow{+1} r \end{array}\right\} \tag{6}$$

Notice that, although (5) and (6) are feedforward loops, the existing techniques (Chang and Hwang, 1992; Hunt *et al.*, 1992c) are not suitable for developing fault trees corresponding to the event $r(-1)$. This is due to the fact that the starting nodes of both loops, $m2$ and $s6$, are located on the same NFBL (3) and, thus, their effects cannot be considered independently.

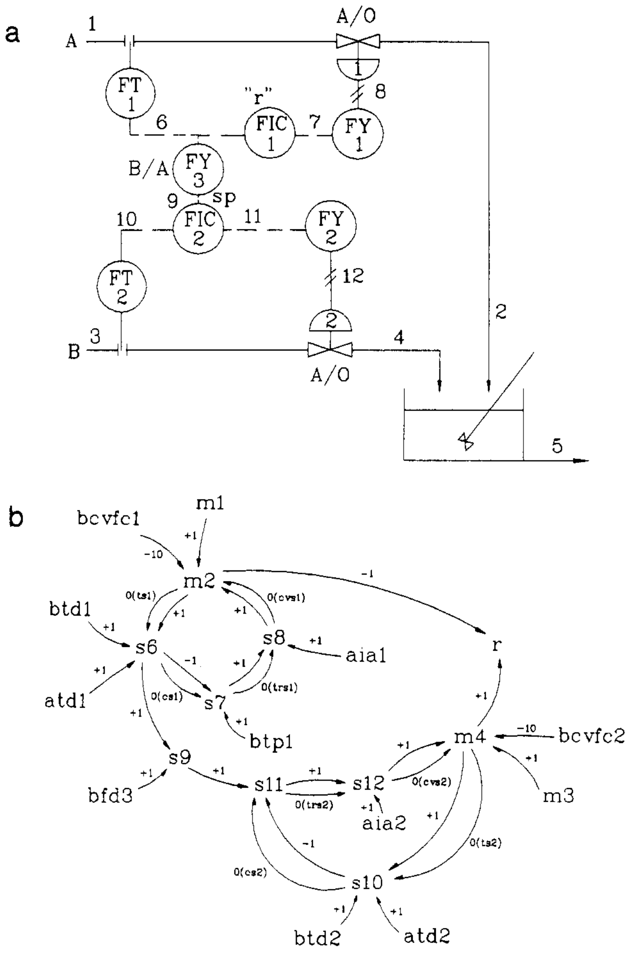

Figure 3. (a) P&ID of the caprolactam reactor with a double-NFBL ratio-control system. (b) Digraph of the double-NFBL ratio-control system in part a.

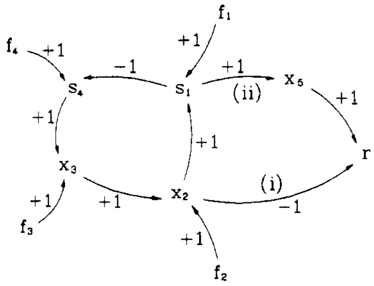

Figure 4. Standard digraph of a double-NFBL ratio-control system.

In this study, a modified fault-tree synthesis procedure has been developed for digraphs with the standard configuration shown in Figure 4. In this figure, there are two FFLs and one NFBL. The two FFLs end at the same node r which is obviously corresponding to the controlled variable of the entire system, i.e., the ratio. The starting nodes of the two FFLs are located on the NFBL $s1 \rightarrow x2 \rightarrow x3 \rightarrow s4 \rightarrow s1$, which will be referred to as the *starting NFBL* in this discussion. In this NFBL, $s1$ is the sensor signal, $x2$ represents the controlled variable, $x3$ is the manipulated variable, $s4$ denotes the output signal from the controller, and $f1$, $f2$, $f3$, and $f4$ represent faults or failures whose effects enter the control loop at their respective locations. For our example, one can clearly see that $x2 = x3 = m2, x5 = m4$, and r is the flow ratio between $m4$ and $m2$. Also, as indicated in the last section, the effects of a change in the flow rate of stream A cannot be eliminated by the slave NFBL (4). Thus, the slave feedback loop can actually be neglected in the development of the general fault-tree structure. For the convenience of illustration, the two paths between the starting NFBL and the end node r are labeled. The one originated from the manipulated variable $x2$ of the starting NFBL is referred to as path i and the other one (originated from the sensor output $s1$) is referred to as path ii. Notice that the products of the gains on these two paths are opposite in sign under normal operating conditions. It should also be emphasized that, in realistic applications, the corresponding digraphs may not be exactly the same as the one shown in Figure 4 in terms of the values of the gains and the number of nodes and edges. However, the approach developed in this study should be applicable as long as the basic structural features remain unchanged.

As mentioned in the Introduction, still more complex configurations can be found in other realistic ratio-control systems. For example, the temperatures sensor signal from the reactor may be used to manipulate the set point of FIC1 assuming that the *normal* reaction between cyclohexanone oxime and oleum is exothermic and the coolant circulation rate is constant. For the sake of brevity, specific solutions corresponding to these situations are not presented in this paper. However, it should be noted that, although our attention is developed only to the standard case of Figure 4, the fault trees of ratio-control systems with more than two NFBLs can be constructed with the same principles.

Table 1. Qualitative Steady-State Analysis of a Ratio-Control System with Double NFBLs: Results Associated with the Type A Faults or Failures on the Starting NFBL

fault/ failure	$s1$	$x2$	$x3$	$s4$	r	r_D
$f_1(+1)$	(+1,0)	(−1,−1)	(−1,−1)	(−1,−1)	+1	+1
$f_2(+1)$	(+1,0)	(+1,0)	(−1,−1)	(−1,−1)	0	0
$f_3(+1)$	(+1,0)	(+1,0)	(+1,0)	(−1,−1)	0	0
$f_4(+1)$	(+1,0)	(+1,0)	(+1,0)	(+1,0)	0	0
$f_1(+10)$	(+10,+1)	(−10,−10)	(−10,−10)	(−10,−10)	+10	+1
$f_2(+10)$	(+10,+1)	(+10,+1)	(−10,−10)	(−10,−10)	0	−10
$f_3(+10)$	(+10,+1)	(+10,+1)	(+10,+1)	(−10,−10)	0	−10
$f_4(+10)$	(+10,+1)	(+10,+1)	(+10,+1)	(+10,+1)	0	−10

Qualitative Steady-State Analysis

To develop the fault-tree structure corresponding to the digraph presented in Figure 4, it is necessary to identify the mechanisms by which the event $r(-1)$ could occur. Thus, the technique of qualitative simulation (Oyeleye and Kramer, 1988; Chang and Hwang, 1992) becomes extremely helpful for this purpose. In this work, all possible faults and failures are classified into four different types (A, B, C, and D) according to the criteria suggested by Himmelblau (1978) and Chang and Hwang (1992). For illustration purposes, their definitions are repeated in Appendix B. Following is a detailed qualitative steady-state analysis of their effects in the standard system described by Figure 4.

Effects of Faults or Failures on the Starting NFBL under the Condition That All Components on Paths i and ii Function Normally. From Figure 4, one can see clearly that the effects of any of the faults or failures on the starting NFBL must propagate through both paths i and ii and may cause the flow ratio to change. An analysis of these effects has been carried out first in our study.

Generally speaking, a digraph model explicitly describes the cause–effect relationships between deviations in process variables (represented by 0, ±1, and ±10) and component failures (represented by 0, 1, and 10). The effects of a type A fault (or failure) on the starting NFBL can thus be determined by first assigning a nonzero value (±1 or ±10) to f_i ($i = 1, 2, 3,$ or 4) and then evaluating the values of all other variables. In a simple digraph, any of these variables can normally be obtained by mutiplying their input value(s) with the corresponding edge gain(s). However, this approach becomes unfeasible if the system digraph contains NFBLs. Specifically, the values of loop variables generated with the above calculation procedure can be both positive and negative. This is certainly unacceptable. To describe the behaviors of the loop variables more accurately, their states are represented with symbols of the form (δ_0, δ_∞) in our study. This symbol is interpreted as the state of a loop variable which would have a value δ_0 *without feedback* but approaches δ_∞ at the new steady state due to the regulatory action of the feedback control loop.

The results of qualitative corresponding to faults or failures of type A on the starting NFBL are summarized in Table 1. From Table 1, one can observe that the ratio r in the sixth column is affected only when $s1$ is the direct output of an off-NFBL type A fault or failure, e.g., a drift in the sensor's zero. This fault/failure in general causes the measurement signal of the controlled variable to deviate from its actual value. If the fault is "controllable," i.e., its magnitude equals 1, then the sensor output $s1$ can be controlled at its normal level. However, to achieve such a purpose, the actual value of the controlled variable must be different from the set point. As a result, the fault propagates *only* through path i to cause a change in r. On the other hand, if the fault is uncontrollable with a magnitude of 10, then the sensor output cannot be brought back to the set point and its eventual value should be ±1. This is due to the assumption that type A faults with magnitude 10 saturate the control loop. In such cases, the magnitude of deviation in the ratio is 10 since the disturbances along both path i and path ii cause r to deviate toward the same direction. It should also be noted that, although their failure mechanisms are quite different, the outcomes of these two sensor faults are similar. Essentially, the signs of the resulting ratio change in both cases are the same. They can only be differentiated by the extent of deviation.

Table 2. Qualitative Steady-State Analysis of a Ratio-Control System with Double NFBLs: Results Associated with Type B Failures on the Starting NFBL

failure	$s1$	$x2$	$x3$	$s4$	r	r_D
$f_1(+1)$	+1	−10	−10	−10	+10	+1
$f_2(+1)$	+1	+1	−10	−10	0	−10
$f_3(+1)$	+1	+1	+1	−10	0	−10
$f_4(+1)$	+1	+1	+1	+1	0	−10

Table 3. Qualitative Steady-State Analysis of a Ratio-Control System with Double NFBLs: Results Associated with Simultaneous Occurrence of a Type C Failure and a Type A Fault on the Starting NFBL

type C failure	type A fault/failure	$s1$	$x2$	$x3$	$s4$	r	r_D
$x2 \xrightarrow{0} s1$	$f_1(+1)$	×	×	×	×	×	×
	$f_2(+1)$	0	+1	0	0	−1	−1
	$f_3(+1)$	0	+1	+1	0	−1	−1
	$f_4(+1)$	0	+1	+1	+1	−1	−1
$x3 \xrightarrow{0} x2$	$f_1(+1)$	+1	0	−10	−10	+1	−1
	$f_2(+1)$	+1	+1	−10	−10	0	−10
	$f_3(+1)$	0	0	+1	0	0	0
	$f_4(+1)$	0	0	+1	+1	0	0
$s4 \xrightarrow{0} x3$	$f_1(+1)$	+1	0	0	−10	+1	−1
	$f_2(+1)$	+1	+1	0	−10	0	−10
	$f_3(+1)$	+1	+1	+1	−10	0	−10
	$f_4(+1)$	0	0	0	+1	0	0
$s1 \xrightarrow{0} s4$	$f_1(+1)$	+1	0	0	0	+1	−1
	$f_2(+1)$	+1	+1	0	0	0	−10
	$f_3(+1)$	+1	+1	+1	0	0	−10
	$f_4(+1)$	+1	+1	+1	+1	0	−10

Notice that a fault or failure of type A does not change the structure of the NFBL, i.e., the feedback mechanism of the control system is still intact. However, if a component failure of type B or C occurs on the starting NFBL, this regulatory function will be lost completely. In these situations, the use of state (δ_0, δ_∞) is no longer necessary in describing the behaviors of the loop variables. The results of qualitative simulation corresponding to type B failures are summarized in Table 2, and those associated with the simultaneous occurrence of a type C failure and a type A fault (or failure) are given in Table 3. The inclusion of type A faults/failures is essential in assessing the effects of type C failures, since a type C failure alters only the structure of the NFBL and the state variables of the system remain at the normal levels without additional disturbances.

Again, one can observe from the sixth column of Table 2 and the seventh column of Table 3 that a change in the ratio r occurs only when the values of $s1$ and $x2$ are different. From Table 2, it can be concluded that such a consequence can be caused by a type B failure associated with the sensor. On the other hand, the results in Table 3 reveal that r may also be changed by combinations of type A and type C faults/failures under the following two

Table 4. Qualitative Steady-State Analysis of a Ratio-Control System with Double NFBLs: Results Associated with Type D Failures on the Starting NFBL

failure	$s1$	$x2$	$x3$	$s4$	r	r_D
$x2 \xrightarrow{-1(rev)} s1$	(+1,+10)	(−1,−10)	(−1,−10)	(−1,−10)	+10	+1
	(−1,−10)	(+1,+10)	(+1,+10)	(+1,+10)	−10	−1
$x3 \xrightarrow{-1(rev)} s2$	(+1,+10)	(+1,+10)	(−1,−10)	(−1,−10)	−1	−10
	(−1,−10)	(−1,−10)	(+1,+10)	(+1,+10)	+1	+10
$x4 \xrightarrow{-1(rev)} s3$	(+1,+10)	(+1,+10)	(+1,+10)	(−1,−10)	−1	−10
	(−1,−10)	(−1,−10)	(−1,−10)	(+1,+10)	+1	+10
$x1 \xrightarrow{-1(rev)} s4$	(+1,+10)	(+1,+10)	(+1,+10)	(+1,+10)	−1	−10
	(−1,−10)	(−1,−10)	(−1,−10)	(−1,−10)	+1	+10

conditions: First, if the gain associated with the edge $x2 \rightarrow s1$ is changed to zero due to a type C failure (e.g., sensor stuck), then the type A fault/failure originated from the off-NFBL nodes f_2, f_3, or f_4 can cause a discrepancy between the values of $s1$ and $x2$. The corresponding results are presented in the second, third, and fourth rows of Table 3. Notice that the results corresponding to f_1, i.e., the first row, are omitted. This is due to the fact that, in this case, type A and type C failures are usually associated with two different failure modes of the same sensor and they are, of course, mutually exclusive events. The second possible situation can be found in the fifth, nineth, and thirteenth rows of Table 3. We can see from these results that a change in ratio can also be caused by the simultaneous occurrence of a type C failure corresponding to an edge *other than* $x2 \rightarrow s1$ and a type A failure associated with $f1$. In this case, the value of the controlled variable $x2$ remains unchanged and the variation in r is caused by a deviation in the sensor output $s1$. In our reactor example, this is corresponding to the scenario that the type A sensor failure in the flow-control system of stream A affects only the flow rate of stream B. Due to a type C failure in the controller or control valve, the flow rate of stream A remains unchanged. However, it should also be noted that type A sensor failure *alone* is sufficient for creating the same change in r (see row 1 of Table 1). In this latter case, the manipulated variable of the starting NFBL deviates from its normal level but the sensor output is controlled at the set-point value. As a result, the former causes, i.e., those described in rows 5, 9, and 13 of Table 3, cannot be regarded as the minimum cut sets and, thus, it seems reasonable to neglect them in synthesizing the fault tree.

It has been well documented in the previous studies (Lapp and Powers, 1977; Chang and Hwang, 1992) that the control loop becomes unstable if a type D failure occurs. Thus, corresponding to each location in the loop, two possible outcomes may be created by such a failure. The results of qualitative simulation are presented in Table 4. Notice that the values of $s1$ and $x2$ are different only when the failure is associated with the edge $x2 \rightarrow s1$. However, the flow ratio still deviates from its normal level if a type D failure occurs at any other location. This is due to the assumption that a change in $x5$ (the flow rate of stream B) is unable to compensate for a large deviation in $x2$ (the flow rate of stream A), i.e., the NFFL is saturated in this situation.

Effects of Faults or Failures on the Starting NFBL under the Condition that a Type C or Type D Failure Occurs on Path i or ii. Notice that the above discussions are concerned only with the effects of the faults and failures that affect the starting NFBL. Further, these results can only be obtained under the assumption that none of the components on the two paths, i and ii, fail at the same time. However, if a failure of type C or D does occur on these paths, the above-mentioned effects will be different and, thus, the qualitative steady-state analysis should be carried out again for these cases.

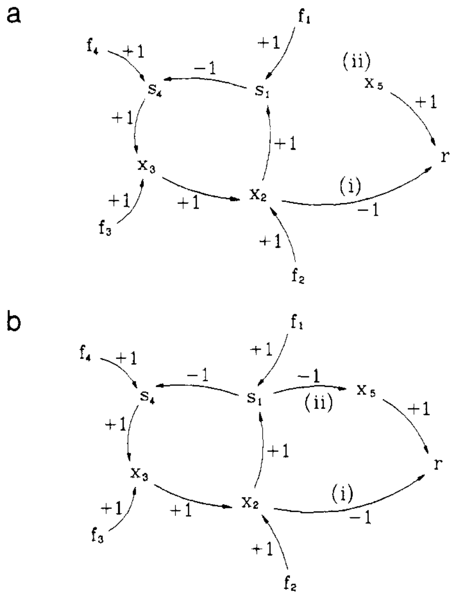

Figure 5. Standard digraph of the double-NFBL ratio-control system with (a) a type C failure on path ii and (b) a type D failure on path ii.

In a ratio-control system, it is not possible to have type C or type D failures on path i because there are no physical components between $x2$ and r. r is simply a calculated parameter believed to be affected by $x2$ and can cause a drastic increase in reactor temperature if it drops below a certain level. Thus, let us first consider only the digraph when a type C failure is known to occur on path ii. An example is given in Figure 5a. In this example, it is assumed that path ii in Figure 4 is broken due to type C controller or sensor failure on the slave flow-control loop. As a result, the NFFL in the original ratio-control system does not exist any more. The corresponding digraph becomes very simple, i.e., it contains only one NFBL and nothing else. Although it appears that structure III (see Appendix A) should be sufficient for describing the fault propagation behavior in this situation, there are still some subtle details calling for additional attention. In this example, the ratio change is essentially caused by a fault passing through *only* path i, i.e., $x2 \rightarrow r$. Notice also that this same phenomenon can actually be observed in scenarios corresponding to row 1 of Table 2 and rows 2–4 of Table 3. Thus, in constructing the corresponding part of the fault tree, special care must be taken in implementing structure III to avoid repetition. This point will be elaborated in the next section.

The system behavior is more complicated after a type D failure develops on either of the two paths mentioned previously. Let us consider the case when such a failure exists on path ii due to human error in installing the computing relay of the ratio station. The digraph corresponding to Figure 4 is shown in Figure 5b. Notice that the products of the gains on both paths are negative in this example and, in addition, the effects of faults or failures on the starting NFBL can propagate through both the controlled variable $x2$ and the sensor output $s1$ to produce a change in the variable associated with the end node of the FFLs. A qualitative steady-state analysis has been performed, and the corresponding results are also presented in Tables 1–4. To differentiate the results obtained from two different digraphs (i.e., Figure 4 and Figure 5b), a symbol r_D is used for the cases associated with a type D failure occurring on path ii. One can see clearly that, in

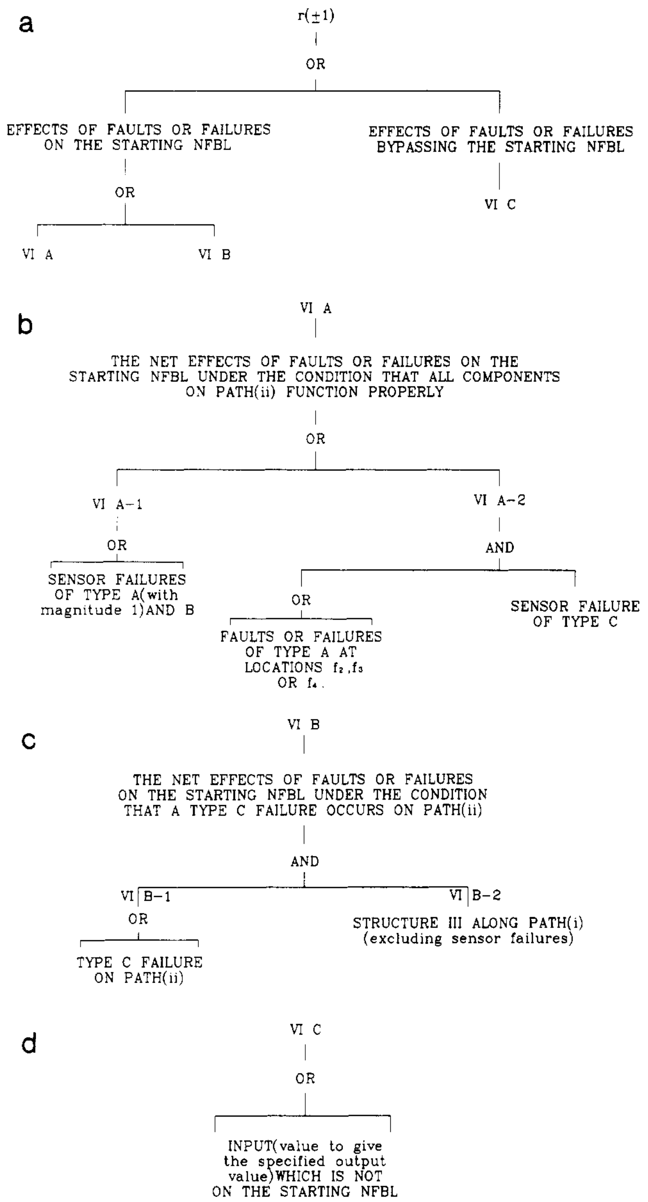
a
r(±1)
OR
EFFECTS OF FAULTS OR FAILURES ON THE STARTING NFBL
EFFECTS OF FAULTS OR FAILURES BYPASSING THE STARTING NFBL
OR
VI A
VI B
VI C
b
VI A
THE NET EFFECTS OF FAULTS OR FAILURES ON THE STARTING NFBL UNDER THE CONDITION THAT ALL COMPONENTS ON PATH(ii) FUNCTION PROPERLY
OR
VI A-1
VI A-2
OR
AND
SENSOR FAILURES OF TYPE A(with magnitude 1)AND B
OR
SENSOR FAILURE OF TYPE C
FAULTS OR FAILURES OF TYPE A AT LOCATIONS f₂,f₃ OR f₄.
c
VI B
THE NET EFFECTS OF FAULTS OR FAILURES ON THE STARTING NFBL UNDER THE CONDITION THAT A TYPE C FAILURE OCCURS ON PATH(ii)
AND
VI B-1
VI B-2
OR
STRUCTURE III ALONG PATH(i) (excluding sensor failures)
TYPE C FAILURE ON PATH(ii)
d
VI C
OR
INPUT(value to give the specified output value)WHICH IS NOT ON THE STARTING NFBL

Figure 6. Framework of (a) structure VI, (b) substructure VIA, (c) substructure VIB, (d) substructure VIC.

this situation, almost all faults or failures on the starting NFBL can cause the ratio to deviate from its desired value.

Effects of Faults or Failures Bypassing the Starting NFBL. Finally, other than the cases already discussed, ratio change may also be caused by a fault which does not affect the starting NFBL. In essence, if it enters the FFLs through one of the nodes on path i or ii, then only one of the paths is under its influence. It is a straightforward task to model such phenomena. The implementation techniques used for structure IIC can be directly adopted in developing the corresponding portion of the fault tree.

General Fault-Tree Structure for Ratio-Control Systems with Double NFBLs

As a summary of the analysis presented in the previous section, a general fault-tree structure has been developed for ratio-control systems with double NFBLs. Its substructures are presented in Figure 6. Notice that this structure is referred to as structure VI, since five other general fault-tree structures have already been established for simpler systems in a previous study (Chang and Hwang, 1992). From Figure 6a, it is clear that the framework of the fault trees associated with the double-NFBL ratio-control systems is essentially the same as that of a NFFL (see Figure 9a in Appendix A). In a simple NFFL, the branches under IIA (Figure 9b) and IIB (Figure 9c) are associated with the effects of the faults or failures that enter the NFFL from the starting node. In the present case, however, the corresponding branches under VIA (Figure 6b) and VIB (Figure 6c) are concerned with the effects of faults or failures affecting the *starting* NFBL. Notice also that the events under substructures IIA and IIB-1 correspond to deviations in the same variable which is associated with the starting node of the NFFL. The only difference between these two events is that the deviations may be opposite in direction or of different magnitudes. On the other hand, the events under VIA and VIB-1 are of totally different nature.

Substructure VIA should be considered as a summary of the results presented in column 6 of Tables 1 and 2 and column 7 of Table 3. Basically, one can see from these results that, if all the components on paths i and ii function properly, then there can be only *one* way for the effects of a fault or failure (of type A, B, or C) on the starting NFBL to reach the end node r, i.e., the fault/failure causes the controlled variable and the sensor signal of the starting NFBL to be different in value. In other words, the events included in VIA are only associated with various different failure modes of the sensor on the starting NFBL. The results presented in the sixth column of Table 1 and the seventh column of Table 3 are included under VIA-1. On the other hand, substructure VIA-2 contains the conclusions obtained from an analysis of the results in Table 2. Notice that the scenario described in the fifth row of Table 1 is neglected in VIA-1. This is due to the rationale that, since type A sensor faults of magnitude 1 have already been included as a cause of ratio change, the addition of the same fault with magnitude 10 is redundant and, further, the resulting cut sets must be mutually exclusive.

Substructure VIB addresses the need to consider the possibility of a fault or failure on the starting NFBL propagating through path i only, i.e., path ii is broken due to a type C failure. In such cases, any cause that can produce a change in the controlled variable of the starting NFBL will affect the ratio. As concluded in the previous section, structure III is suitable for modeling the corresponding failure mechanisms. However, it should be noted that, in developing this part of the fault tree, sensor failures should be omitted even when they are required as inputs in applying the standard structure III. The reason is that, since any of the failures listed under VIB-1 already prevent the fault from propagating through path ii, there is no need to AND the events under VIB-2 which have the same effect.

The implications of substructures VIA and VIB are interesting. Intuitively, one would expect that if the effects of a fault/failure can propagate through the starting NFBL, i.e., it causes a change in the controlled variable and/or the sensor output, the ratio r should be affected also. However, this is not so in most cases. As indicated by substructure VIB, they must be ANDed with a type C failure on path ii. This can be attributed to, of course, the control action of the NFFL in the ratio-control system. But, on the other hand, not all faults/failures on the starting NFBL can be handled by the NFFL. Such exceptions are listed under substructure VIA. Thus, it is clear that the existing operators, i.e., substructure II and III, cannot be used *directly* to construct fault trees for multiple-NFBL ratio-control systems.

The branches under VIC (Figure 6d) are concerned with faults or failures which do not produce any effect on the starting NFBL. Thus, the corresponding fault-tree construction procedure is the same as that of substructure IIC. In the process of developing the nonbasic events in substructure VIC along the two paths i and ii in the ratio-control system, nodes on the starting NFBL will be encountered. Since their effects have already be considered in VIA and VIB, the corresponding input events should be deleted from this part of the fault tree. In addition, if its output does not have any other input attached after the deletion, the output should be removed also. The same steps must be repeated until the above condition, i.e., the output is without inputs after deletion, cannot apply.

Notice, in this general fault-tree structure, that component malfunctions that reverse the signs of edge gains (a type D failure) are not included at all. This is because of the fact that these kinds of failures can be almost always eliminated by preventive inspection before the start-up of the system, and thus, the possibility of their occurrences is omitted in the fault tree. If one is interested in assessing the risk associated with type D failures, the fault tree obtained with structure VI can always be expanded according to the results of qualitative steady-state analysis presented in the previous section. Finally, it should also be noted that the possibilities of the simultaneous occurrence of more than one type B or C failure within the *same* NFBL or NFFL are ignored in the general structure. This practice is mainly due to the fact that, in most cases, such a combination of failures produces the same outcome as that caused by one of them. In other words, these combinations usually do not result in minimum cut sets. If these possibilities are nonetheless included, the corresponding fault tree can be very large and unmanageable. Since the probability of simultaneous failures should be quite low, it was our decision to exclude such events so that the best results can be obtained within a reasonable amount of time.

Application of the Proposed Fault-Tree Structure

To demonstrate the use of structure VI, it has been applied to the ratio-control system presented in Figure 3 parts a and b. The top event for this example is chosen to be $r(-1)$. After identifying various sensor failures on the starting NFBL, the fault tree corresponding to substructure VIA can be easily constructed (Figure 7a). In this example, there are only two type C failures that satisfy the conditions specified in VIB, i.e., $trs2(0)$ (converter FY2 stuck) and $cvs2(0)$ (control valve No. 2 stuck). Under the condition that one of them occurs, the fault tree under VIB can be developed along path i. In particular, structure IIIA should be applied to the event $m2(+1)$. This portion of the fault tree is presented in Figure 7b. Notice that the branches under the symbol "×" are severed on the ground that they are sensor failures on the starting NFBL. Finally, the fault tree corresponding to VIC is presented in Figure 7c. Notice, in the process of developing this portion of the fault tree, the node $m4$ must be reached eventually. Since $m4$ is a node on the slave NFBL, a standard structure III can be applied without modifications. Again, the symbol "×" in Figure 7c denotes the branches that must be deleted from the fault tree. In this case, they are associated with nodes on the starting NFBL.

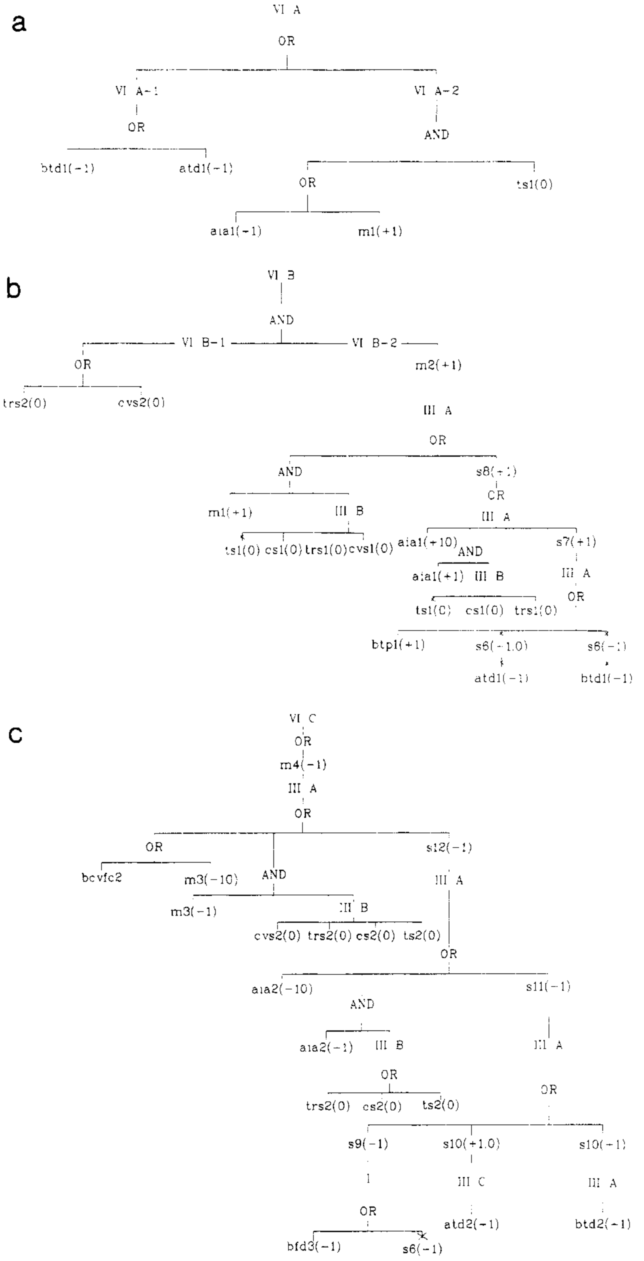

Figure 7. Fault tree of the double-NFBL ratio-control system shown in Figure 3 parts a and b: (a) part VIA, (b) part VIB, and (c) part VIC.

The fault tree in Figure 7 can be compared with Figure 2. We can see that the two are really very similar. Especially, the branches under VIC in Figure 7c are indentical to those under IIC in Figure 2 except that the latter contains two more events, i.e., $atd1(-1)$ and $btd1(-1)$. These two events are actually included elsewhere in the fault tree presented in Figure 7a (under VIA-1). It should be emphasized that, although they are associated with the same sensor in both cases, their respective failure mechanisms are in fact different. Also, it can be observed from IIB (Figure 2) and VIA-2 (Figure 7a) that $\{ts1(0), m1(+1)\}$ is the cut set of both fault trees.

On the one hand, we can also see that several causes of ratio change in the single-NFBL system are avoided by adding the additional starting NFBL. In particular, the cut sets $\{m1(+10)\}$,$\{m1(+1),trs2(0)\}$ and $\{m1(+1), cvs2(0)\}$ are excluded in a double-NFBL system and, thus, the risk associated with upstream disturbances in the flow rate of reactant A becomes insignificant. However, this improvement is brought about at the cost of introducing cut sets not included in the single-NFBL system. Naturally, they are associated with the starting NFBL, i.e., $\{aia(-1), ts1(0)\}$ under VIA and all the causes under VIB. Thus, in

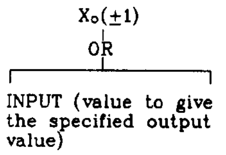

Figure 8. Generalized fault-tree structure for digraphs with the configuration of a tree (structure I).

terms of safety, there is really no guarantee that one of the two is better in general. The issue of trade-off can be addressed more propoerly on the basis of quantitative risk calculation according to the fault trees presented in Figure 2 and Figure 7.

Conclusions

A systematic procedure has been developed in this work to synthesize fault trees for complex ratio-control systems. On the basis of qualitative simulation of the fault propagation behavior in the corresponding digraphs, unique failure mechanisms of a standard double-NFBL system have been identified and summarized in a generalized fault-tree structure. This structure can be easily extended to other realistic ratio-control systems with the steady-state analysis techniques described in this paper. It is also clear from our analysis of the standard system that the existing operators of the NFFL and NFBL are not adequate for constructing fault trees associated with the multiple-NFBL systems. Thus, the results presented here represent a significant improvement of the conventional digraph-based methods.

Nomenclature

*aia*1, *aia*2 = sudden variations in the instrument air pressure supply to the electric/pneumatic signal converter FY1 and FY2 respectively (type A faults)

*atd*1, *atd*2 = sensor failures of type A (i.e., a drift in the zero) corresponding to FT1 and FT2 respectively

*bcvfc*1, *bcvfc*2 = the control valves 1 and 2 failing close, respectively (type B failures)

*bfd*3 = a type B failure causing abnormal deviations in the output of ratio station FY3

*btd*1, *btd*2 = type B failures corresponding to sensor FT1 and FT2, respectively

*btp*1 = a set-point change in controller FIC1

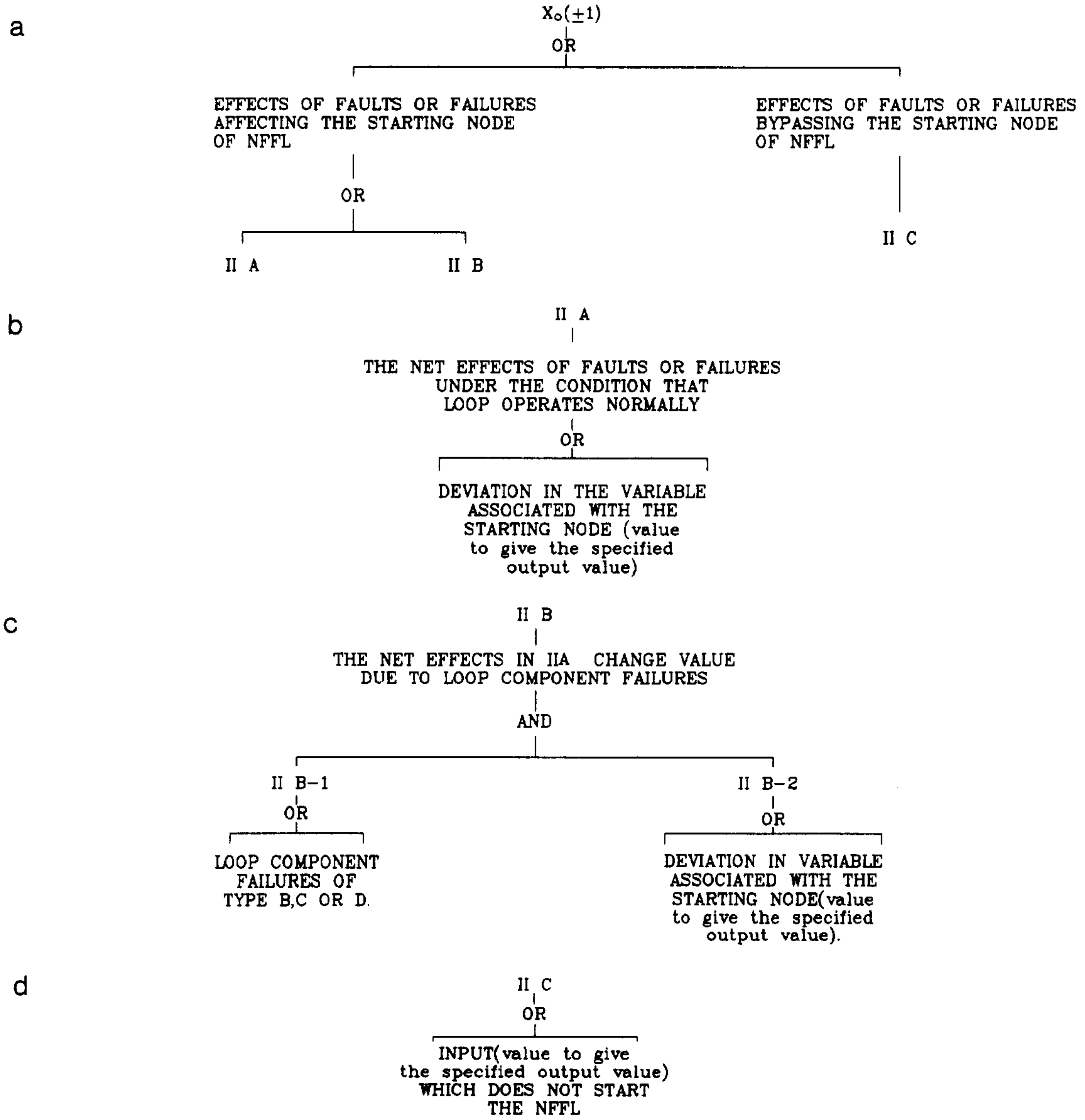
a
X₀(±1)
OR
EFFECTS OF FAULTS OR FAILURES AFFECTING THE STARTING NODE OF NFFL
OR
II A
II B
EFFECTS OF FAULTS OR FAILURES BYPASSING THE STARTING NODE OF NFFL
II C
b
II A
THE NET EFFECTS OF FAULTS OR FAILURES UNDER THE CONDITION THAT LOOP OPERATES NORMALLY
OR
DEVIATION IN THE VARIABLE ASSOCIATED WITH THE STARTING NODE (value to give the specified output value)
c
II B
THE NET EFFECTS IN IIA CHANGE VALUE DUE TO LOOP COMPONENT FAILURES
AND
II B-1
OR
LOOP COMPONENT FAILURES OF TYPE B,C OR D.
II B-2
OR
DEVIATION IN VARIABLE ASSOCIATED WITH THE STARTING NODE(value to give the specified output value).
d
II C
OR
INPUT(value to give the specified output value) WHICH DOES NOT START THE NFFL

Figure 9. Generalized fault-tree structure for the variable associated with the end node of a NFFL: (a) structure II, (b) substructure IIA, (c) substructure IIB, and (d) substructure IIC.

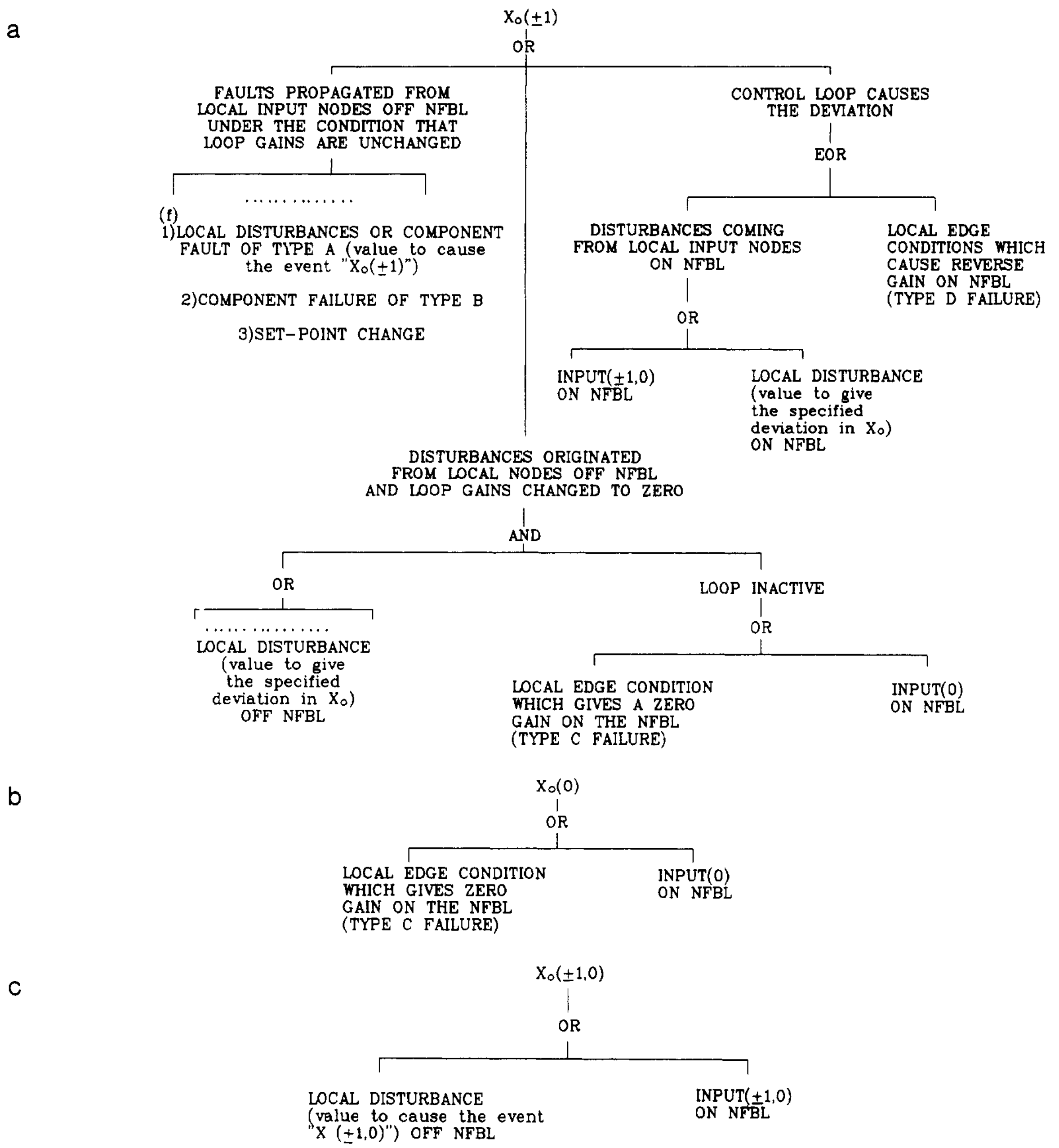
a
Xo(±1)
OR
FAULTS PROPAGATED FROM LOCAL INPUT NODES OFF NFBL UNDER THE CONDITION THAT LOOP GAINS ARE UNCHANGED
(f)
1)LOCAL DISTURBANCES OR COMPONENT FAULT OF TYPE A (value to cause the event "Xo(±1)")
2)COMPONENT FAILURE OF TYPE B
3)SET-POINT CHANGE
CONTROL LOOP CAUSES THE DEVIATION
EOR
DISTURBANCES COMING FROM LOCAL INPUT NODES ON NFBL
OR
INPUT(±1,0) ON NFBL
LOCAL DISTURBANCE (value to give the specified deviation in Xo) ON NFBL
LOCAL EDGE CONDITIONS WHICH CAUSE REVERSE GAIN ON NFBL (TYPE D FAILURE)
DISTURBANCES ORIGINATED FROM LOCAL NODES OFF NFBL AND LOOP GAINS CHANGED TO ZERO
AND
OR
LOCAL DISTURBANCE (value to give the specified deviation in Xo) OFF NFBL
LOOP INACTIVE
OR
LOCAL EDGE CONDITION WHICH GIVES A ZERO GAIN ON THE NFBL (TYPE C FAILURE)
INPUT(0) ON NFBL
b
Xo(0)
OR
LOCAL EDGE CONDITION WHICH GIVES ZERO GAIN ON THE NFBL (TYPE C FAILURE)
INPUT(0) ON NFBL
c
Xo(±1,0)
OR
LOCAL DISTURBANCE (value to cause the event "X (±1,0)") OFF NFBL
INPUT(±1,0) ON NFBL

Figure 10. (a) Generalized fault-tree structure used for a moderate deviation (±1) in the variable associated with a node on NFBL (structure IIIA). (b) Generalized fault-tree structure used for no deviation (0) in the variable associated with a node on NFBL (structure IIIB). (c) Generalized fault-tree structure used for the deviation (±1, 0) in the variable associated with a node on NFBL (structure IIIC).

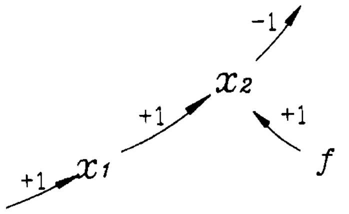

Figure 11. Digraph representation of a type A fault or failure.

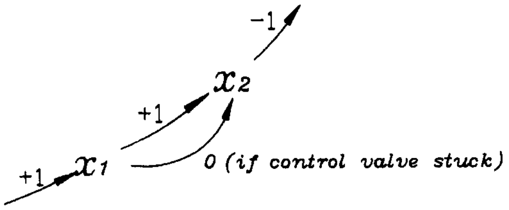

Figure 12. Digraph representation of a type C failure.

*cs*1(0), *cs*2(0) = the controllers FIC1 and FIC2 stuck, respectively (type C failures)
*cvs*1(0), *cvs*2(0) = the control valves 1 and 2 stuck, respectively (type C failures)
*m*1–*m*5 = the mass flow rates in pipelines 1–5, respectively
r = ratio
*s*6–*s*12 = the electric or pneumatic signals in lines 6–12, respectively
*ts*1(0), *ts*2(0) = the sensors FT1 and FT2 stuck, respectively (type C failures)
*trs*1(0), *trs*2(0) = the electric/pneumatic signal converters FY1 and FY2 stuck, respectively (type C failures)

Appendix A: The Generalized Fault-Tree Structures for Three Digraph Configurations

In a previous study, Chang and Hwang used three generalized structures to develop fault trees for three types of digraph configurations. They are presented in Figure 8–10 for the trees, the negative feedforward loops (NFFLs), and the negative feedback loops (NFBLs), respectively.

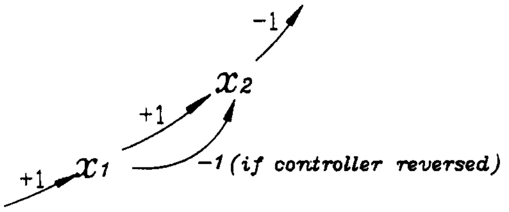

Figure 13. Digraph representation of a type D failure.

Appendix B: Classification of Faults and Failures

The definitions of faults and failures suggested by Himmelblau (1978) are followed in this work. The word *fault* is used to designate the departure from an acceptable range from a measurable process variable or calculated parameter associated with an equipment. *Failure*, on the other hand, is taken to mean complete inoperability of an equipment for its intended purpose. Further, they are classified into four types based on their digraph representations and, also, the patterns of their propagation in the system.

Type A. For faults such as disturbances in the process variables or partial component failures (i.e., degradation in the equipment's performance) such as a small leak or a partial plug in a control valve, the corresponding digraph representation should be a node without inputs. The outward edges of such nodes are directed to process variables. A typical digraph model can be found in Figure 11, where x_1 and x_2 are process variables and f is the fault or failure of type A. The effects of these types of faults/failures can be determined by assigning a nonzero value (±1 or ±10) to f, and the values of the other variables in the digraph can then be evaluated accordingly. Notice that, in analyzing these effects for the purpose of classification, the implied assumption is that no other failures exist simultaneously. Further, it should also be noted that, if *both* $x1$ and $x2$ are on the same FBL, the value of x_2 can be affected not only by f but also by x_1.

Type B. The digraph configuration of component failures such as sensor failing high or control valve failing close is actually the same as that of type A. However, their effects should be analyzed differently. If a failure of type B (f) occurs and both x_1 and x_2 are variables on the same NFBL, then x_2 is always affected by f alone and should be independent of the input x_1.

Type C. Component failures such as sensor stuck or control valve stuck should be modeled by conditional edges with zero gain. An example can be found in Figure 12. The occurrence of a failure of this type only changes the configuration of the system digraph, i.e., the edge between x_1 and x_2 can be considered as nonexistent. The state variables of the system remain at the normal levels without additional disturbances.

Type D. Component failures such as controller reversed (from direct action to reverse action or vice versa) or control valve reversed (from air-to-open to air-to-close or vice versa) can also be represented by conditional edges. An example of such failures is presented in Figure 13, which is also represented by a change in the configuration only. Obviously, the occurrence of a failure of type D changes the direction of the effects of an additional fault (if it occurs) propagating from x_1 to x_2.

Literature Cited

Allen, D. J. Digraphs and Fault Trees. *Ind. Eng. Chem. Fundam.* **1984**, *23*, 175.

Allen, D. J.; Rao, M. S. M. New Algorithms for the Synthesis and Analysis of Fault Trees. *Ind. Eng. Chem. Fundam.* **1980**, *19*, 79.

Andrews, J. D.; Morgan, J. M. Application of Digraph Method of Fault Tree Construction to Process Plant. *Reliab. Eng.* **1986**, *14*, 85.

Andrews, J. D.; Brennan, G. Application of the Digraph Method of Fault Tree Construction to a Complex Control Configuration. *Reliab. Eng. Syst. Saf.* **1990**, *28*, 357.

Chamow, M. F. Directed Graph Techniques for the Analysis of Fault Trees. *IEEE Trans. Reliab.* **1978**, *R-27*, 7.

Chang, C. T.; Hwang, H. C. New Developments of the Digraph-Based Techniques for Fault-Tree Synthesis. *Ind. Eng. Chem. Res.* **1992**, *31*, 1490.

Chang, C. T.; Hwang, H. C.; Hwang, D. M. Fault-Tree Synthesis Techniques for Process Systems with Coupled Feedforward and Feedback Loops. Presented at International Conference on Safety, Health and Loss Prevention in the Oil, Chemical and Process Industries, Singapore, February 1993.

Cummings, D. L.; Lapp, S. A.; Powers, G. J. Fault Tree Synthesis From a Directed Graph Model for a Power Distribution Network. *IEEE Trans. Reliab.* **1983**, *R-32*, 140.

Himmelblau, D. M. *Fault Detection and Diagnosis in Chemical and Petrochemical Processes*; Elsevier: New York, 1978.

Hunt, A.; Kelly, B. E.; Mulhi, J. S.; Lees, F. P.; Rushton, A. G. The Propagation of Faults in Process Plants: 6, Overview of, and Modelling for, Fault Tree Synthesis. *Reliab. Eng. Syst. Saf.* **1992a**, *39*, 173.

Hunt, A.; Kelly, B. E.; Mulhi, J. S.; Lees, F. P.; Rushton, A. G. The Propagation of Faults in Process Plants: 7, Divider and Header Units in Fault Tree Synthesis. *Reliab. Eng. Syst. Saf.* **1992b**, *39*, 195.

Hunt, A.; Kelly, B. E.; Mulhi, J. S.; Lees, F. P.; Rushton, A. G. The Propagation of Faults in Process Plants: 8, Control Systems in Fault Tree Synthesis. *Reliab. Eng. Syst. Saf.* **1992c**, *39*, 211.

Hunt, A.; Kelly, B. E.; Mulhi, J. S.; Lees, F. P.; Rushton, A. G. The Propagation of Faults in Process Plants: 9, Trip Systems in Fault Tree Synthesis. *Reliab. Eng. Syst. Saf.* **1992d**, *39*, 229.

Hunt, A.; Kelly, B. E.; Mulhi, J. S.; Lees, F. P.; Rushton, A. G. The Propagation of Faults in Process Plants: 10, Fault Tree Synthesis-2. *Reliab. Eng. Syst. Saf.* **1992e**, *39*, 243.

Lambert, H. E. Comments on the Lapp-Powers 'Computer-Aided Synthesis of Fault Trees.' *IEEE Trans. Reliab.* **1979**, *R-28*, 6.

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

Lapp, S. A.; Powers, G. J. Update of Lapp-Powers Fault Tree Synthesis Algorithm. *IEEE Trans. Reliab.* **1979**, *R-28*, 12.

Oyeleye, O. O.; Kramer, M. A. Qualitative Simulation of Chemical Process Systems: Steady State Analysis. *AIChE J.* **1988**, *34*, 1441.

Shaeiwitz, J. A.; Lapp, S. A.; Powers, G. J. Fault Tree Analysis of Sequential Systems. *Ind. Eng. Chem. Process Des. Dev.* **1977**, *16*, 529.

Smith, C. A.; Corripio, A. B. *Principles and Practice of Automatic Process Control*; John Wiley & Sons, Inc.: New York, 1985.

Received for review September 21, 1993
Revised manuscript received February 23, 1994
Accepted March 8, 1994[⊗]

[⊗] Abstract published in *Advance ACS Abstracts*, April 15, 1994.