Constructing Fault Trees for Advanced Process Control Systems—Application to Cascade Control Loops

Shi-Ning Ju, Cheng-Liang Chen, and Chuei-Tin Chang

***Abstract*—A systematic approach to construct fault trees for advanced process control systems is presented in this paper. For illustration purpose, the proposed method is explained with a specific feedback scheme, i.e., the cascade control strategy. The digraph configuration of a standard system is first described and analyzed in detail. On the basis of a series of qualitative simulation studies, all failure mechanisms can be identified and summarized with a set of generalized fault-tree structures. The fault trees produced with the conventional digraph-based techniques are shown to be not as comprehensive as the ones constructed with the proposed approach. To demonstrate the correctness of our analysis, the successful application of the proposed structures to a heat exchange process is presented. In addition, the resulting fault tree is compared with one obtained from a single-loop feedback control system and the trade-off between the two in system reliability and control performance is assessed accordingly.**

***Index Terms*—Cascade-control system, digraph, fault tree analysis, qualitative simulation.**

ACRONYMS[1]

FRC =	feedback controller.
NFBL =	negative feedback loop.
NFFL =	negative feed forward loop.
PI, PID =	abbreviations for controller types (P $\equiv$ proportional, I $\equiv$ integral, D $\equiv$ derivative).
TRC =	temperature controller.
$aia =$	a sudden variation in the instrument air pressure supply to the current-to-pneumatic signal converter FY (a type A fault).
$bcvfc =$	the control valve failing close (a type B failure).
$btp =$	a set-point change in the temperature recorder/controller TRC.
$g =$	the gain associated with an arc in digraph.
$tatd, fatd =$	the sensor failures of type A, i.e., a drift in the zero, corresponding to temperature sensor TT and flow sensor FT respectively.
$tbtd, fbtd =$	the type B failures corresponding to sensors TT and FT respectively.
$tbias, fbias =$	the biases in outputs from controllers TRC and FRC respectively (type A faults).
$v_{\rm in}, v_{\rm out} =$	the qualitative values of abnormal conditions associated with the input and output nodes of an arc.
CVS(0) =	the control valve sticks (a type C failure).
$trs(0) =$	the signal converter FY sticks (a type C failure).
$tcs(0), fcs(0) =$	the controllers TRC and FRC stick respectively (type C failures).
$ts(0), fs(0) =$	the sensors TT and FT respectively stick (type C failures).
$N(v) =$	the event symbol representing the abnormal condition associated with a node on the fault propagation path, in which N denotes the node label, and v is its qualitative value, $N = v$.
$X(x) \Rightarrow$ $Y(y) =$	the causal relation "event $X(x)$ results in event $Y(y)$."
PO =	the precedence order of a sequence of events, $X_1(x_1) \Rightarrow X_2(x_2) \Rightarrow \cdots$
$[\mathrm{PO}_A] \Rightarrow$ $\mathrm{PO}_B =$	a composite precedence order in which the square bracket denotes that the steady-state conditions in PO_A are fully developed before those in PO_B.

Manuscript received September 19, 2000; revised September 11, 2002. Responsible Editor: T. Kohda.

S.-N. Ju and C.-L. Chen are with the Department of Chemical Engineering, National Taiwan University, Taipei, Taiwan 10617, ROC (e-mail: ccl@ccms.ntu.edu.tw).

C.-T. Chang is with the Department of Chemical Engineering, National Cheng Kung University, Tainan, Taiwan 70101, ROC (e-mail: ctchang@mail.ncku.edu.tw).

Digital Object Identifier 10.1109/TR.2004.823849

[1]The singular and plural of an acronym are always spelled the same.

I. INTRODUCTION

DUE to the self-healing effects of the feedback control systems, such systems behave as if they contained partial redundancy, even though they do not comprise duplicated hardware. Hence, these systems can have nontrivial fault trees. One of the most popular model used in the development of computer-aided method for fault tree analysis is perhaps the digraph. The digraph-based fault-tree synthesis strategy was first proposed by Lapp and Powers [13]. Numerous other studies concerning its applications and modifications have been published in the literature [1]–[6], [9], [12], [14], [16]. Essentially, a digraph provides an intermediate step which gives explicit causal relationships between the process variables, human errors and equipment failures, from which the fault trees can be constructed accordingly. In particular, a set of generalized fault-tree structures (operators) corresponding to various digraph configurations were developed for systems with coupled control and *process* loops.

Although these structures are quite useful and have been applied to a number of realistic processes, difficulties still exist in the application of this approach to complex advanced process control systems, e.g., the ratio control systems, the override control systems, and the cascade control systems. A direct implementation of the existing operators often fails to produce correct results [7], [8], [10]. This failure is mainly due to a fundamental deficiency of digraph. The dynamic nature of chemical processes cannot be fully captured with such cause-and-effect models. Consequently, the knowledge embedded in a digraph must be complemented with the insights obtained from qualitative simulation [6], [15] to develop proper fault trees for the advanced process control systems.

The need to incorporate a thorough analysis of the fault propagation behavior in processes with complex dynamics is demonstrated with a cascade control system in the present paper. Cascade control is a strategy which improves the performance of feedback control. In most cases, two controllers are adopted for its implementation. Specifically, the output of a *master* controller is used to manipulate the set point of another *slave* controller. Each controller has its own measurement input, but only the former can have an independent set point, and only the latter has an output to the process. The two corresponding feedback loops are nested, with the secondary (slave) control loop located inside the primary (master) control loop. Conceivably, if the inner loop is much faster than the outer loop, the disturbances arising within the secondary loop may be corrected long before they can influence the primary controlled variable. Thus, in processes with slow dynamics and/or too many upsets, it is sensible to adopt cascade control to achieve satisfactory performance.

It is apparent from the above description that the drastic difference between the response speeds of the inner and outer loops cannot be accounted for with the "static" digraph only. A series of comprehensive qualitative simulation studies are thus indispensable in developing the modified fault-tree structures for the cascade control systems. The rest of this article is thus organized as follows. First, the structural characteristics embedded in the digraph model of cascade control systems are described and analyzed in detail. The procedures and results of a series of exhaustive qualitative simulation studies are then presented. It can be observed that the existing procedures are indeed incapable of producing fault trees that incorporate all accident scenarios considered in this work. On the basis of simulation results, the generalized fault-tree structures are then derived. To demonstrate the correctness and effectiveness of our techniques, a realistic example, i.e., a heat exchange system with cascade temperature control, is shown next. The corresponding fault tree is compared with one obtained on the basis of a single-loop feedback control system. It is clear that the trade-off between the two in terms of reliability, cost and performance can be easily determined as a result of this exercise.

II. Digraph Model of Cascade Control Systems

For illustration purpose, a simple example is used throughout this paper. Let us consider the heat exchange system presented in Fig. 1. The exit temperature of the cold process stream is the controlled variable in this case. If the standard single-loop feedback control strategy is adopted for this task, only a temperature controller (TRC) is required for manipulating the control valve on the steam line. However, notice that a flow controller (FRC) is also added here to compensate disturbances in the steam pressure. The result is a cascade control system, in which TRC is the master controller and FRC is the slave controller. The corresponding digraph model can be found in Fig. 2. The symbols $T_n, p_n,$ & m_n in this figure denote respectively the temperature, pressure, & flow rate of process stream n; and S_l represents the measurement or control signal on line l. The other nodes in this model are defined in the Notation section.

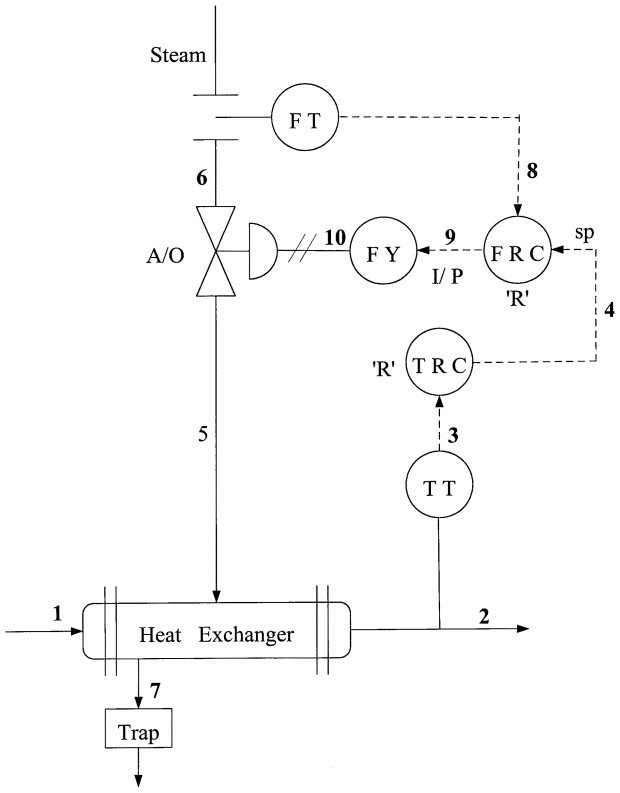

Fig. 1. The flow diagram of a heat-exchange process with cascade control (TT≡temperature sensor/transmitter; FT≡flow sensor/transmitter; TRC≡temperature recorder/controller; FRC≡flow recorder/controller; FY≡signal converter; 'R'≡reverse action mode; I/P≡current to pneumatic; A/O≡air to open).

Two negative feedback loops (NFBLs) can be identified in the digraph:

1) the primary loop: $T_2 \rightarrow S_3 \rightarrow S_4 \rightarrow S_9 \rightarrow S_{10} \rightarrow m_5 \rightarrow T_2$, and
2) the secondary loop: $m_5 \rightarrow S_8 \rightarrow S_9 \rightarrow S_{10} \rightarrow m_5$.

These two loops share a common path $S_9 \rightarrow S_{10} \rightarrow m_5$. It should be noted that one of the inputs to the output of slave controller S_9 is the output of master controller S_4. Because the latter represents the set point of FRC, a change in S_4 should always drive the variables in the secondary loop away from their original steady-state values. In other words, its effects are *not* the same as those due to other inputs of S_9. Consequently, in developing the fault tree of a cascade control system, one must take this relation between the primary and secondary loops into account. The traditional method [13] is really not applicable in this case.

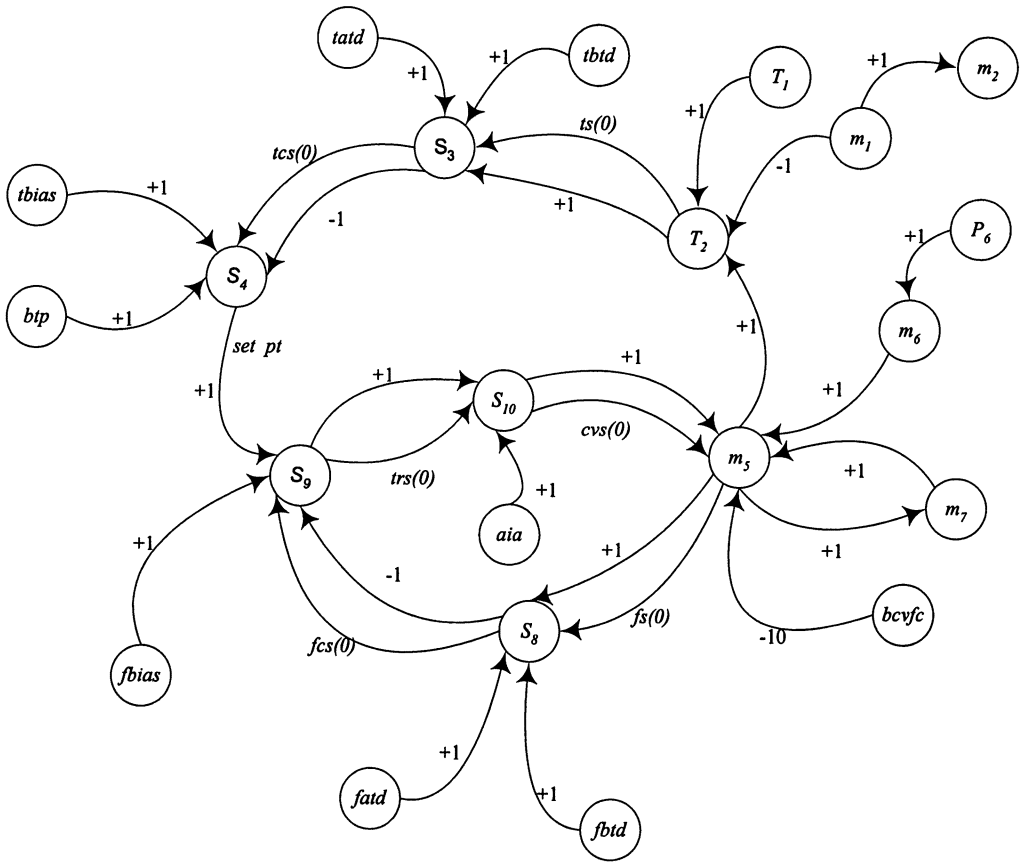

Fig. 2. The digraph model of a heat-exchange process with cascade control.

To derive a set of generalized fault-tree structures for all cascade control systems, let us consider the standard digraph model presented in Fig. 3 instead.

- S_{1o}, S_{4o}, & X_{2o} denote respectively the sensor output, controller output, & controlled variable in the primary loop;
- S_{1i}, S_{4i}, & X_{2i} denote respectively the sensor output, controller output, & controlled variable in the secondary loop;
- X_3 is the only manipulated variable in the cascade system;
- f_j represents the fault or failure affecting the loop variable at position j.

Notice that, if the inner loop is associated with a flow-control system, then $X_3 = X_{2i}$.

The two NFBL in Fig. 3 can be identified easily. Specifically, the primary loop in the standard digraph is $X_{2o} \rightarrow S_{1o} \rightarrow S_{4o} \rightarrow S_{4i} \rightarrow X_3 \rightarrow X_{2i} \rightarrow X_{2o}$, and the secondary loop is $X_{2i} \rightarrow S_{1i} \rightarrow S_{4i} \rightarrow X_3 \rightarrow X_{2i}$. To facilitate our later discussion, the loops are further divided into three paths in this study:

1) $X_{2i} \rightarrow X_{2o} \rightarrow S_{1o} \rightarrow S_{4o} \rightarrow S_{4i}$,
2) $S_{4i} \rightarrow X_3 \rightarrow X_{2i}$, and
3) $X_{2i} \rightarrow S_{1i} \rightarrow S_{4i}$.

III. Qualitative Simulation

To develop fault-tree structures corresponding to the standard digraph, it is necessary to gain a thorough understanding of the fault propagation behaviors in the cascade control system. All possible initiating faults & equipment failures can be classified into four different types (A, B, C, and D) according to the criteria suggested by Himmelblau [11], and Chang & Hwang [6]. For the sake of completeness, their definitions are repeated in Appendix A.

To reduce the number of scenarios which must be included in the fault trees, the following assumptions are adopted:

- Either the PI or the PID control strategy is adopted in the master and slave controllers. Both controllers are well designed and tuned.
- Component malfunctions which reverse the signs of edge gains in the digraph, i.e., type D failures, do not exist in the system.
- The probability of the simultaneous occurrence of two or more type B and/or C failures within the same control system is negligible.

The assumption of a well designed & tuned cascade control system implies that its inner loop is *much faster* than its outer loop and, if controllable, any disturbance entering the former can be eliminated within the loop. On the other hand, type D failures are excluded because they can be almost always eliminated by preventive inspection before startup. Finally, the third assumption is justified by the fact that the probability of a single type B or C failure is usually very low, and that of multiple such failures should be even lower. It is thus only necessary to consider the effects of a single type A fault or type B failure, and the combined effects of a type A fault & a type C failure.

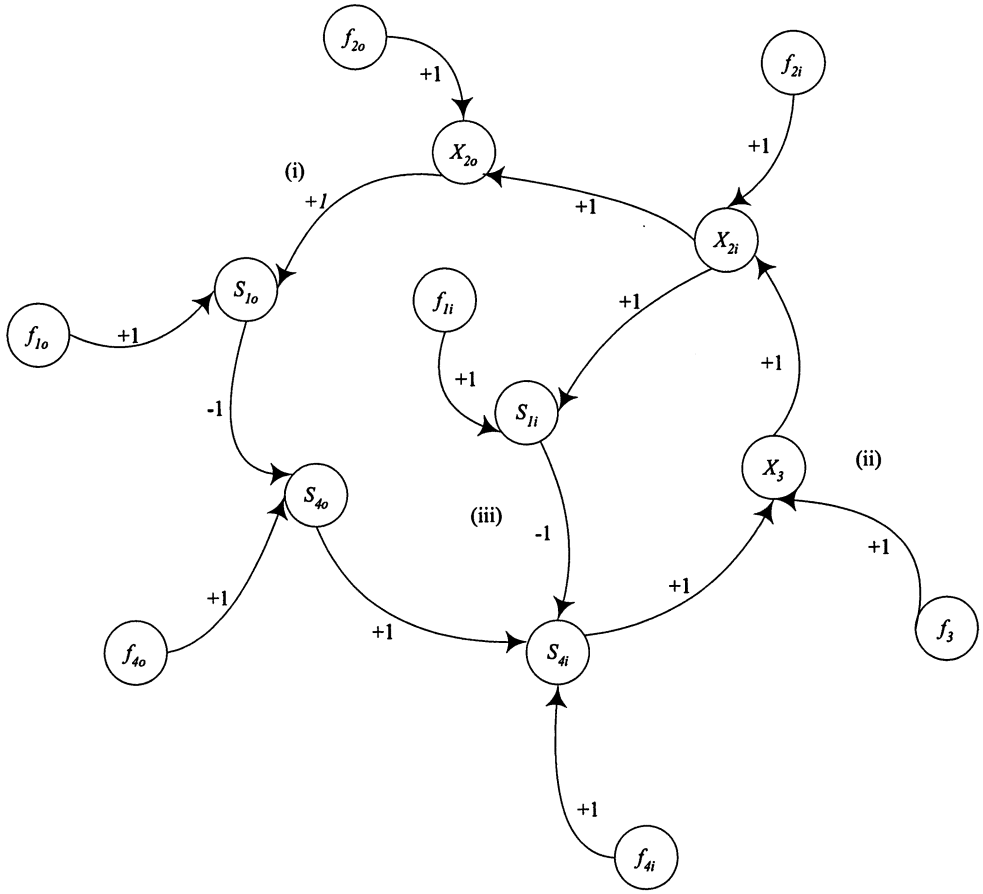

Fig. 3. The standard digraph model of cascade control systems.

Generally speaking, a digraph model explicitly describes the cause-effect relationships between deviations in process variables (represented by 0, ± 1, & ± 10), and component failures (represented by 0, 1, & 10). The effects of a type A fault can thus be determined by first assigning a nonzero value (± 1 or ± 10) to the corresponding node variable f_j, and then evaluating the values of all other affected variables. In a simple loop-free digraph, any of these variables can be determined by multiplying its input value with the corresponding edge gain. In other words, the output value of an arc can be computed according to the following equation:

$$v_{\text{out}} = \begin{cases} g \cdot v_{\text{in}} & \text{if } -10 \le g \cdot v_{\text{in}} \le +10 \\ +10 & \text{if } g \cdot v_{\text{in}} > +10 \\ -10 & \text{if } g \cdot v_{\text{in}} < -10 \end{cases} \quad (1)$$

where g, v_{in}, & v_{out} denote respectively the gain, input, & output values. This evaluation process is generally referred to as *qualitative simulation* in the present study.

However, for a stationary or quasistationary analysis as performed here, this approach becomes infeasible if the system digraph contains NFBL. In particular, two opposite effects on the loop variables are caused by an external disturbance. To describe the behaviors of the loop variables more accurately, Chang & Hwang [6] proposed an improved procedure to simulate qualitatively the corresponding fault propagation sequences in a *single* NFBL. For the sake of completeness, a brief description of the additional computation rules used for qualitative simulation is included in Appendix B.

Notice that a fault of type A does not change the structure of NFBL; the feedback mechanism of the control system is still intact. However, if a component failure of type B occurs on a NFBL, the regulatory function of the corresponding control loop will be lost completely. In these situations, the simulation approach should be the same as that for a simple digraph without loops.

Finally, notice that every type C failure is described with a conditional edge in the digraph. Because the corresponding gain is always zero, the connection between its input & output is essentially severed by such a failure. In other words, the digraph configuration is modified by such a failure. If, in addition, a type A fault occurs, then the combined effects can be evaluated by determining the fault propagation behavior in the *modified* digraph.

The qualitative simulation techniques for the above two types of fault propagation scenarios in a single NFBL are also explained in Appendix B.

IV. The Fault Propagation Patterns in Cascade Control Loops

The qualitative simulation techniques can be applied to the cascade control systems with the understanding that the disturbance propagation speed in the inner loop is much faster than that in the outer loop. The results of a series of comprehensive simulation studies are presented in the following.

TABLE I
SIMULATION RESULTS: A TYPE A FAULT

fault origin	S_{1o}	X_{2o}	X_{2i}	X_3	S_{4i}	S_{1i}	S_{4o}
$f_{1o}(+1)$	(+1, 0)	(-1, -1)	(-1, -1)	(-1, -1)	(-1, -1)	(-1, -1)	(-1, -1)
$f_{2o}(+1)$	(+1, 0)	(+1, 0)	(-1, -1)	(-1, -1)	(-1, -1)	(-1, -1)	(-1, -1)
$f_{2i}(+1)$	((0, 0), 0)	((0, 0), 0)	((+1, 0), 0)	((-1, -1), -1)	((-1, -1), -1)	((+1, 0), 0)	((0, 0), 0)
$f_3(+1)$	((0, 0), 0)	((0, 0), 0)	((+1, 0), 0)	((+1, 0), 0)	((-1, -1), -1)	((+1, 0), 0)	((0, 0), 0)
$f_{4i}(+1)$	((0, 0), 0)	((0, 0), 0)	((+1, 0), 0)	((+1, 0), 0)	((+1, 0), 0)	((+1, 0), 0)	((0, 0), 0)
$f_{1i}(+1)$	((0, -1), 0)	((0, -1), 0)	((-1, -1), 0)	((-1, -1), 0)	((-1, -1), 0)	((+1, 0), +1)	((0, +1), +1)
$f_{4o}(+1)$	(+1, 0)	(+1, 0)	(+1, 0)	(+1, 0)	(+1, 0)	(+1, 0)	(+1, 0)
$f_{1o}(+10)$	(+10, +1)	(-10, -10)	(-10, -10)	(-10, -10)	(-10, -10)	(-10, -10)	(-10, -10)
$f_{2o}(+10)$	(+10, +1)	(+10, +1)	(-10, -10)	(-10, -10)	(-10, -10)	(-10, -10)	(-10, -10)
$f_{2i}(+10)$	((0, +1), +1)	((0, +1), +1)	((+10, +1), +1)	((-10, -10), -10)	((-10, -10), -10)	((+10, +1), +1)	((0, -1), -10)
$f_3(+10)$	((0, +1), +1)	((0, +1), +1)	((+10, +1), +1)	((+10, +1), +1)	((-10, -10), -10)	((+10, +1), +1)	((0, -1), -10)
$f_{4i}(+10)$	((0, +1), +1)	((0, +1), +1)	((+10, +1), +1)	((+10, +1), +1)	((+10, +1), +1)	((+10, +1), +1)	((0, -1), -10)
$f_{1i}(+10)$	((0, -10), -1)	((0, -10), -1)	((-10, -10), -1)	((-10, -10), -1)	((-10, -10), -1)	((+10, +1), +10)	((0, +10), +10)
$f_{4o}(+10)$	(+10, +1)	(+10, +1)	(+10, +1)	(+10, +1)	(+10, +1)	(+10, +1)	(+10, +1)

A. *Effects of a Type a Fault*

The results of qualitative simulation corresponding to various faults of type A are summarized in Table I. The effects of the controllable (magnitude 1), & uncontrollable (magnitude 10) disturbances are included in rows 1 through 7, & rows 8 through 14 respectively.

Let us consider the results of controllable disturbances first. Notice that the values of loop variables in rows 1, 2, & 7 are expressed in the form of (v_0, v_∞). As explained in Appendix B, these results indicate that the loop variables behave like those in a single feedback loop. This behavior is due to the fact that the corresponding disturbances (f_{1o}, f_{2o}, & f_{4o}) enter the primary loop at the interior nodes on path 1. It is clear that any of them can cause a change in S_{4o}. Because S_{4o} is the set point of the slave controller, these disturbances are bound to propagate through the secondary loop.

Notice that the simulation results can be interpreted more clearly in terms of the *precedence order* defined in Appendix B. Specifically, the fault propagation sequence caused by f_{2o} can be written as:

$$f_{2o}(+1) \Rightarrow X_{2o}(+1) \Rightarrow S_{1o}(+1) \Rightarrow S_{4o}(-1) \Rightarrow [\mathrm{PO}_{A1,\mathrm{inner}}] \Rightarrow X_{2o}(0) \Rightarrow S_{1o}(0) \Rightarrow S_{4o}(-1) \quad (2)$$

where $\mathrm{PO}_{A1,\mathrm{inner}}$ denotes the precedence order in the inner loop, i.e.,

$$\mathrm{PO}_{A1,\mathrm{inner}} \equiv S_{4i}(-1) \Rightarrow X_3(-1) \Rightarrow X_{2i}(-1) \Rightarrow S_{1i}(-1) \quad (3)$$

It should be noted that the propagation sequence listed in (3) should be fully developed *before* the outer-loop variables reach their final steady-state values in (2).

On the other hand, if an external disturbance enters at any node on the secondary loop, i.e., f_{2i}, f_3, f_{4i}, or f_{1i}, its effects can always be compensated first with the slave controller, and then the master controller. The corresponding results are presented in rows 3 through 6 of Table I. Notice that the value of each loop variable is now written in a new format, $((v_0, v_x), v_\infty)$, to reflect the fact that the inner loop is much faster than the outer loop. The value v_0 can be regarded as the state of a loop variable without feedback in both the primary & secondary loops; v_x can be considered as the temporary steady-state value achieved in a short time period with the faster secondary loop; v_1 is the value corresponding to the final steady state reached in the cascade control system. For example, the precedence order of fault propagation associated with a type A fault at f_3 is

$$f_3(+1) \Rightarrow [\mathrm{PO}_{A2,\mathrm{inner}}] \Rightarrow X_{2o}(0) \Rightarrow S_{1o}(0) \Rightarrow S_{4o}(0) \quad (4)$$

where the symbol $\mathrm{PO}_{A2,\mathrm{inner}}$ again denotes the fully developed precedence order in the inner loop, i.e.,

$$\mathrm{PO}_{\mathrm{A2,inner}} \equiv X_3(+1)X_{2i}(+1) \Rightarrow S_{1i}(+1)S_{4i}(-1) \Rightarrow X_3(0) \Rightarrow X_{2i}(0) \Rightarrow S_{1i}(0) \Rightarrow S_{4i}(-1) \quad (5)$$

The results listed in rows 8 through 14 of Table I can be generated in a similar fashion. By definition, the "uncontrollable" type A faults saturate the control system. This is reflected in the column under S_{1o}. The sensor output of the outer loop cannot be brought back to the set point, and its eventual value should be ± 1. Because the same simulation procedure is used for both controllable & uncontrollable disturbances, the precedence orders of the latter cases are not discussed in this paper for the sake of brevity.

TABLE II
SIMULATION RESULTS: A TYPE B FAILURE

fault origin	S_{1o}	X_{2o}	X_{2i}	X_3	S_{4i}	S_{1i}	S_{4o}
$f_{1o}(+1)$	+1	-10	-10	-10	-10	-10	-10
$f_{2o}(+1)$	+1	+1	-10	-10	-10	-10	-10
$f_{2i}(+1)$	+1	+1	+1	-10	-10	+1	-10
$f_3(+1)$	+1	+1	+1	+1	-10	+1	-10
$f_{4i}(+1)$	+1	+1	+1	+1	+1	+1	-10
$f_{1i}(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	+1	oscil.
$f_{4o}(+1)$	+1	+1	+1	+1	+1	+1	+1

TABLE III
SIMULATION RESULTS: A TYPE A FAULT AND A TYPE C FAILURE ON PATH (1)

type C failure	type A fault	S_{1o}	X_{2o}	X_{2i}	X_3	S_{4i}	S_{1i}	S_{4o}
$S_{4o} \xrightarrow{0} S_{4i}$	$f_{1o}(+1)$	+1	0	0	0	0	0	-10
	$f_{2o}(+1)$	+1	+1	0	0	0	0	-10
	$f_{2i}(+1)$	(0, 0)	(0, 0)	(+1, 0)	(-1, -1)	(-1, -1)	(+1, 0)	(0, 0)
	$f_3(+1)$	(0, 0)	(0, 0)	(+1, 0)	(+1, 0)	(-1, -1)	(+1, 0)	(0, 0)
	$f_{4i}(+1)$	(0, 0)	(0, 0)	(+1, 0)	(+1, 0)	(+1, 0)	(+1, 0)	(0, 0)
	$f_{1i}(+1)$	(0, -1)	(0, -1)	(-1, -1)	(-1, -1)	(-1, -1)	(+1, 0)	(0, +10)
	$f_{4o}(+1)$	0	0	0	0	0	0	+1
$S_{1o} \xrightarrow{0} S_{4o}$	$f_{1o}(+1)$	+1	0	0	0	0	0	0
	$f_{2o}(+1)$	+1	+1	0	0	0	0	0
	$f_{2i}(+1)$	(0, 0)	(0, 0)	(+1, 0)	(-1, -1)	(-1, -1)	(+1, 0)	(0, 0)
	$f_3(+1)$	(0, 0)	(0, 0)	(+1, 0)	(+1, 0)	(-1, -1)	(+1, 0)	(0, 0)
	$f_{4i}(+1)$	(0, 0)	(0, 0)	(+1, 0)	(+1, 0)	(+1, 0)	(+1, 0)	(0, 0)
	$f_{1i}(+1)$	(0, -1)	(0, -1)	(-1, -1)	(-1, -1)	(-1, -1)	(+1, 0)	(0, 0)
	$f_{4o}(+1)$	+1	+1	+1	+1	+1	+1	+1
$X_{2o} \xrightarrow{0} S_{1o}$	$f_{1o}(+1)$	×	×	×	×	×	×	×
	$f_{2o}(+1)$	0	+1	0	0	0	0	0
	$f_{2i}(+1)$	(0, 0)	(0, 0)	(+1, 0)	(-1, -1)	(-1, -1)	(+1, 0)	(0, 0)
	$f_3(+1)$	(0, 0)	(0, 0)	(+1, 0)	(+1, 0)	(-1, -1)	(+1, 0)	(0, 0)
	$f_{4i}(+1)$	(0, 0)	(0, 0)	(+1, 0)	(+1, 0)	(+1, 0)	(+1, 0)	(0, 0)
	$f_{1i}(+1)$	(0, 0)	(0, -1)	(-1, -1)	(-1, -1)	(-1, -1)	(+1, 0)	(0, 0)
	$f_{4o}(+1)$	0	+1	+1	+1	+1	+1	+1
$X_{2i} \xrightarrow{0} X_{2o}$	$f_{1o}(+1)$	+1	0	-10	-10	-10	-10	-10
	$f_{2o}(+1)$	+1	+1	-10	-10	-10	-10	-10
	$f_{2i}(+1)$	(0, 0)	(0, 0)	(+1, 0)	(-1, -1)	(-1, -1)	(+1, 0)	(0, 0)
	$f_3(+1)$	(0, 0)	(0, 0)	(+1, 0)	(+1, 0)	(-1, -1)	(+1, 0)	(0, 0)
	$f_{4i}(+1)$	(0, 0)	(0, 0)	(+1, 0)	(+1, 0)	(+1, 0)	(+1, 0)	(0, 0)
	$f_{1i}(+1)$	(0, 0)	(0, 0)	(-1, -1)	(-1, -1)	(-1, -1)	(+1, 0)	(0, 0)
	$f_{4o}(+1)$	0	0	+1	+1	+1	+1	+1

B. Effects of a Type B Failure

Let us first consider the effects of a type B failure at location f_{1o}, f_{2o}, or f_{4o}. A direct consequence is certainly the breaking of the primary loop. Further, the resulting disturbances should propagate through the secondary loop. This is again due to the fact that the set point of the slave controller S_{4o} is changed. Because by definition the output of the failure node is maintained at ± 1, some of the loop variables may be driven by the integration action of the master controller to the saturation level ± 10. The corresponding simulation results can be found in rows 1, 2, & 7 of Table II.

The outcome of a type B failure at f_{2i} or f_3 is the breaking of both primary & secondary loops. As a result of integrating a constant error term, the outputs of both the master & slave controller (S_{4i} & S_{4o}), should eventually be saturated. The fault propagation patterns of these two failures are presented in the 3rd & 4th row of Table II. On the other hand, notice that S_{4i} is the common output of two loop variables S_{4o} & S_{1i}. The former is a node on the primary loop, and the latter is on the secondary loop. The results given in row 5 were obtained under one assumption: neither S_{4o} nor S_{1i} can affect their output S_{4i} in case a type B failure occurs at f_{4i}.

The most interesting results in this subsection are probably associated with the type B failure at f_{1i} (see row 6 in Table II). The loop variables oscillate as the effects of such a failure propagate through both loops. Let us consider the scenario after the sensor in the inner loop fails, and its output S_{1i} is kept unchanged at $+1$. To compensate the corresponding negative error, the slave controller should try to close the control valve. However, because the sensor output S_{1i} remains constant, and the inner loop is much faster, the error in the secondary loop always exists. The slave controller must be forced to drive the controller output S_{4i} near 0%, and shut the control valve almost completely. Consequently, the controlled variable of the outer loop X_{2o} must be affected and, on the basis of Fig. 3, its deviation is negative. This sustained deviation could activate the master controller, and eventually cause its output S_{4o} reaching 100%. This implies that the set point of the slave controller is raised to a very high level. As a result, the sign of $S_{4o} - S_{1i}$ should be changed from negative to positive eventually. Again, due to the assumption that the response of the secondary loop is quicker, the deviations in inner-loop variables (S_{4i}, X_3, & X_{2i}) should be reversed and then saturated. In other words, the corresponding control-valve position should be wide open at this time. This should inevitably affect the outer-loop variables in the opposite direction. Thus, it

TABLE IV
SIMULATION RESULTS: A TYPE A FAULT AND A TYPE C FAILURE ON PATH (2)

type C failure	type A fault	S_{1o}	X_{2o}	X_{2i}	X_3	S_{4i}	S_{1i}	S_{4o}
$X_3 \xrightarrow{0} X_{2i}$	$f_{1o}(+1)$	+1	0	0	-10	-10	0	-10
	$f_{2o}(+1)$	+1	+1	0	-10	-10	0	-10
	$f_{2i}(+1)$	+1	+1	+1	-10	-10	+1	-10
	$f_3(+1)$	0	0	0	+1	0	0	0
	$f_{4i}(+1)$	0	0	0	+1	+1	0	0
	$f_{1i}(+1)$	0	0	0	-10	-10	+1	0
	$f_{4o}(+1)$	0	0	0	+10	+10	0	+1
$S_{4i} \xrightarrow{0} X_3$	$f_{1o}(+1)$	+1	0	0	0	-10	0	-10
	$f_{2o}(+1)$	+1	+1	0	0	-10	0	-10
	$f_{2i}(+1)$	+1	+1	+1	0	-10	+1	-10
	$f_3(+1)$	+1	+1	+1	+1	-10	+1	-10
	$f_{4i}(+1)$	0	0	0	0	+1	0	0
	$f_{1i}(+1)$	0	0	0	0	-10	+1	0
	$f_{4o}(+1)$	0	0	0	0	+10	0	+1

TABLE V
SIMULATION RESULTS: A TYPE A FAULT AND A TYPE C FAILURE ON PATH (3)

type C failure	type A fault	S_{1o}	X_{2o}	X_{2i}	X_3	S_{4i}	S_{1i}	S_{4o}
$S_{1i} \xrightarrow{0} S_{4i}$	$f_{1o}(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	oscil.	oscil.
	$f_{2o}(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	oscil.	oscil.
	$f_{2i}(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	oscil.	oscil.
	$f_3(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	oscil.	oscil.
	$f_{4i}(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	oscil.	oscil.
	$f_{1i}(+1)$	0	0	0	0	0	+1	0
	$f_{4o}(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	oscil.	oscil.
$X_{2i} \xrightarrow{0} S_{1i}$	$f_{1o}(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	0	oscil.
	$f_{2o}(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	0	oscil.
	$f_{2i}(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	0	oscil.
	$f_3(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	0	oscil.
	$f_{4i}(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	0	oscil.
	$f_{1i}(+1)$	×	×	×	×	×	×	×
	$f_{4o}(+1)$	oscil.	oscil.	oscil.	oscil.	oscil.	0	oscil.

is clear that all loop variables (except S_{1i}) may experience cyclic oscillation after a type B failure occurs at f_{1i}. To facilitate understanding the fault propagation behavior in this case, its precedence order is also provided as follows:

$$f_{1i}(+1) \Rightarrow \left[\mathrm{PO}^{(0)}_{B,\mathrm{inner}}\right] \Rightarrow \left[\mathrm{PO}^{(1)}_{B}\right] \Rightarrow \left[\mathrm{PO}^{(2)}_{B}\right] \Rightarrow \cdots \tag{6}$$

where

$$\mathrm{PO}^{(1)}_{B} = \mathrm{PO}^{(2)}_{B} = \cdots \mathcal{PO}_{\mathcal{B}} \tag{7}$$

$$\mathcal{PO}_{\mathcal{B}} \equiv \left[\mathrm{PO}^{(I)}_{B,\mathrm{outer}}\right] \Rightarrow \left[\mathrm{PO}^{(I)}_{B,\mathrm{inner}}\right] \Rightarrow \left[\mathrm{PO}^{(II)}_{B,\mathrm{outer}}\right] \Rightarrow \left[\mathrm{PO}^{(II)}_{B,\mathrm{innner}}\right] \tag{8}$$

and

$$\mathrm{PO}^{(0)}_{B,\mathrm{inner}} \equiv S_{1i}(+1) \Rightarrow S_{4i}(-1) \Rightarrow X_3(-1) \Rightarrow X_{2i}(-1) \Rightarrow S_{1i}(+1) \Rightarrow S_{4i}(-10) \Rightarrow X_3(-10) \Rightarrow x_{2i}(-10) \tag{9}$$

$$\mathrm{PO}^{(I)}_{B,\mathrm{inner}} \equiv S_{4i}(+1) \Rightarrow X_3(+1) \Rightarrow X_{2i}(+1) \Rightarrow S_{1i}(+1) \Rightarrow S_{4i}(+10) \Rightarrow X_3(+10) \Rightarrow X_{2i}(+10) \Rightarrow S_{1i}(+1) \tag{10}$$

$$\mathrm{PO}^{(II)}_{B,\mathrm{inner}} \equiv S_{4i}(-1) \Rightarrow X_3(-1) \Rightarrow X_{2i}(-1) \Rightarrow S_{1i}(+1) \Rightarrow S_{4i}(-10) \Rightarrow X_3(-10) \Rightarrow X_{2i}(-10) \Rightarrow S_{1i}(+1) \tag{11}$$

$$\mathrm{PO}^{(I)}_{B,\mathrm{outer}} \equiv X_{2o}(-10) \Rightarrow S_{1o}(-10) \Rightarrow S_{4o}(+10) \tag{12}$$

$$\mathrm{PO}^{(II)}_{B,\mathrm{outer}} \equiv X_{2o}(+10) \Rightarrow S_{1o}(+10) \Rightarrow S_{4o}(-10) \tag{13}$$

C. Combined Effects of a Type A Fault and a Type C Failure

As mentioned previously, the tangled loops in a cascade control system can be classified into three paths according the their respective structural characteristics. The discussion here is thus divided into three parts accordingly:

1) The Type C Failure Is on Path 1: The primary loop is broken. Only the secondary loop is left intact in this situation. Because the fault propagation pattern is also dependent upon the location of the type A fault, let us consider the combined effects of the above fault & failure accordingly.

If a type A fault enters the primary loop at one of the interior nodes of path 1, i.e., f_{1o}, f_{2o}, & f_{4o}, neither the primary loop nor the secondary loop is useful in compensating its effects. In some cases, the master controller may even drive its output S_{4o} & downstream nodes to saturation. The corresponding simulation results can be found in Table III.

On the other hand, if a disturbance enters the secondary loop on path 2 or 3, i.e., f_{1i}, f_{2i}, f_3, or f_{4i}, the secondary loop should behave just like a single NFBL. The simulation results for these cases are also presented in Table III. Notice that the final value of S4o in row 6 reaches its saturation level. This occurs because only in this case the controlled variable of the secondary loop, i.e., X_{2i}, is forced to deviate from its normal steady-state value, and thus cause a constant change in the input to the master controller S_{1o}.

Finally, notice that row 15 in Table III is excluded from consideration. In this case, the sensor in the primary loop is subject to two different malfunctions at the same time, i.e., a type A fault & a type C failure. This is of course highly unlikely.

2) The Type C Failure Is on Path 2: The regulatory functions of both the primary & secondary loops are lost due to a type C failure occurring on their common path. Thus, the effects of type A faults can be evaluated in a straightforward fashion. Specifically, the value of each node can be determined by multiplying its input value with the corresponding edge gain. The only exceptions are the two controller outputs S_{4i} & S_{4o}. They should be saturated due to the integration action of controllers. The simulation results are presented in Table IV.

3) The Type C Failure Is on Path 3: The corresponding simulation results are presented in Table V. Observe that the system oscillates as long as a type A fault enters the primary loop after

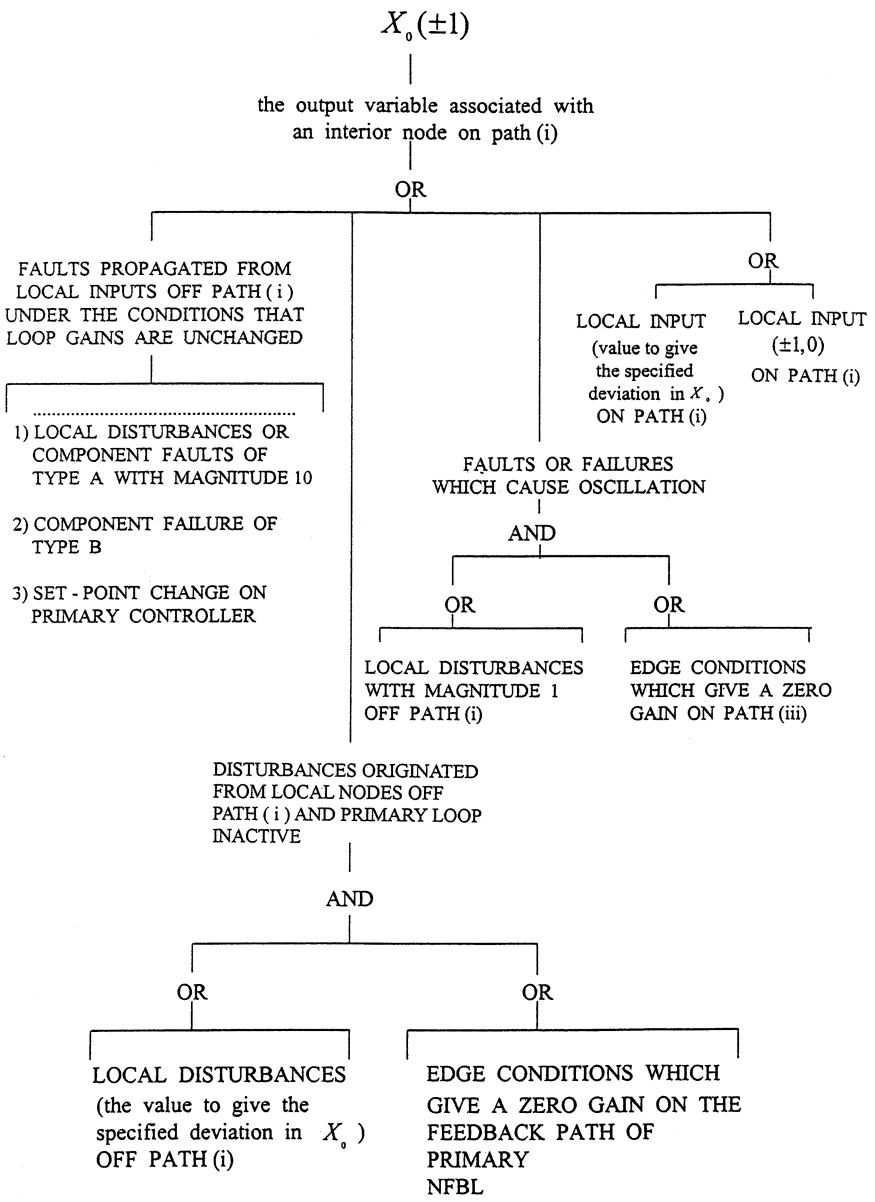

Fig. 4. Structure I.

the occurrence of a type C failure on path 3. This interesting finding has never been reported before.

Let us consider the reason for this unique system behavior. It is obvious that, if a disturbance enters the primary loop, the master controller should always try to adjust its output, or equivalently, the set point of the slave controller S_{4o}. The ultimate goal of this control action is to eliminate the error between the normal set point of the master controller, and the sensor output in the primary loop S_{1o}. However, due to the existence of a type C failure on path 3, the slave controller is incapable of detecting any change in the sensor output of the secondary loop S_{1i}, even after its set point S_{4o} is adjusted. Because a nonzero error $S_{4o} - S_{1i}$ persists, and the inner loop is much faster, the slave controller is forced to increase the magnitude of its output S_{4i} until saturation is reached. Consequently, the controlled variable of the primary loop X_{2o} may be brought back too much to cause a deviation opposite to the original one. To remove this, the master controller is required to alter the direction of its output. In other words, if S_{4o} is increased (or decreased) originally by the master controller, then its value must

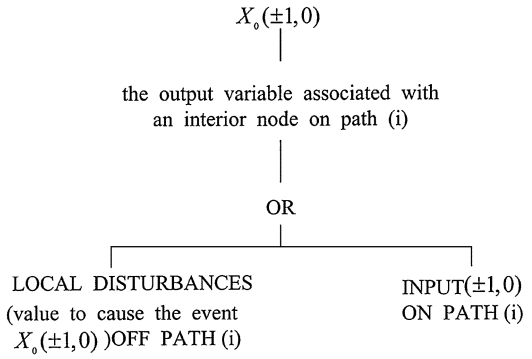

Fig. 5. Structure II.

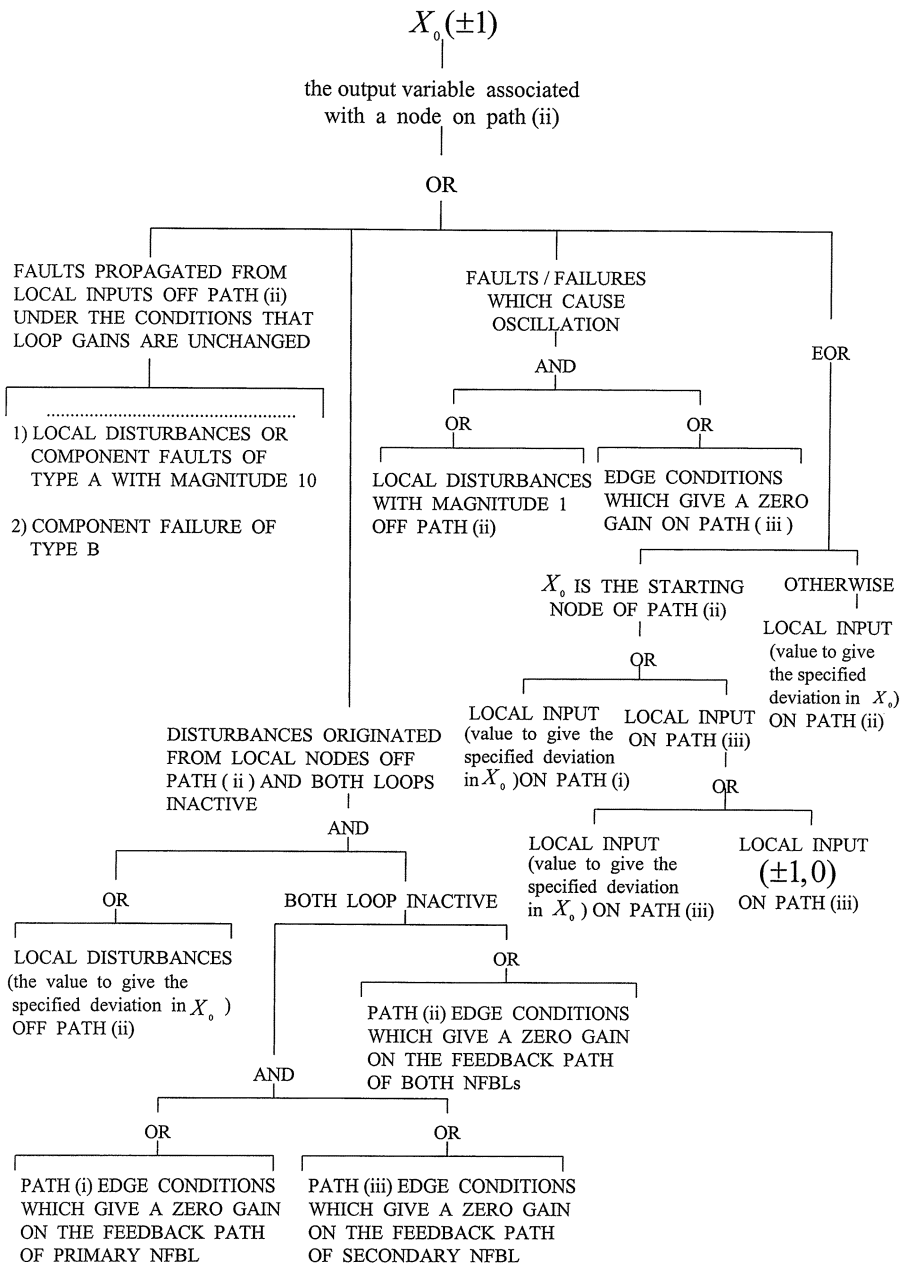

Fig. 6. Structure III.

be decreased (or increased) as soon as the error between the set point & sensor output changes sign. By the same argument, the secondary loop must reach its saturation level again, but in the opposite direction. Consequently, this oscillatory behavior of each outer-loop variable will continue indefinitely. For illustration purpose, let us consider the scenario associated with row 9 of Table V, the combined effects of a type A fault at f_{2o} & a type C failure between X_{2i} & S_{1i}. The corresponding precedence order of fault propagation is

$$f_{2o}(+1) \Rightarrow \left[\mathrm{PO}_{AC}^{(0)}\right] \Rightarrow \left[\mathrm{PO}_{AC}^{(1)}\right] \Rightarrow \left[\mathrm{PO}_{AC}^{(2)}\right] \Rightarrow \cdots \quad (14)$$

where

$$\mathrm{PO}_{AC}^{(0)} \equiv \left[\mathrm{PO}_{AC,\mathrm{outer}}^{(0)}\right] \Rightarrow \left[\mathrm{PO}_{AC,\mathrm{inner}}^{(0)}\right] \quad (15)$$

$$\mathrm{PO}_{AC}^{(1)} = \mathrm{PO}_{AC}^{(2)} = \cdots = \mathcal{PO}_{\mathcal{AC}} \quad (16)$$

$$\mathcal{PO}_{\mathcal{AC}} \equiv \left[\mathrm{PO}_{AC,\mathrm{outer}}^{(I)}\right] \Rightarrow \left[\mathrm{PO}_{AC,\mathrm{inner}}^{(I)}\right] \Rightarrow \left[\mathrm{PO}_{AC,\mathrm{outer}}^{(II)}\right] \Rightarrow \left[\mathrm{PO}_{AC,\mathrm{inner}}^{(II)}\right] \quad (17)$$

The sub-sequences in (15) & (17) can be written as

$$\mathrm{PO}_{AC,\mathrm{outer}}^{(0)} \equiv X_{2o}(+1) \Rightarrow S_{1o}(+1) \Rightarrow S_{4o}(-1) \quad (18)$$

$$\mathrm{PO}_{AC,\mathrm{outer}}^{(I)} \equiv X_{2o}(-1) \Rightarrow S_{1o}(-1) \Rightarrow S_{4o}(+1) \quad (19)$$

$$\mathrm{PO}_{AC,\mathrm{outer}}^{(II)} \equiv X_{2o}(+10) \Rightarrow S_{1o}(+10) \Rightarrow S_{4o}(-10) \quad (20)$$

$$\mathrm{PO}_{AC,\mathrm{inner}}^{(0)} \equiv S_{4i}(-1) \Rightarrow X_3(-1) \Rightarrow X_{2i}(-1) \Rightarrow S_{1i}(0) \Rightarrow S_{4i}(-10) \Rightarrow X_3(-10) \Rightarrow X_{2i}(-10) \Rightarrow S_{1i}(0) \quad (21)$$

$$\mathrm{PO}_{AC,\mathrm{inner}}^{(I)} \equiv S_{4i}(+1) \Rightarrow X_3(+1) \Rightarrow X_{2i}(+1) \Rightarrow S_{1i}(0) \Rightarrow S_{4i}(+10)x_3(+10) \Rightarrow X_{2i}(+10) \Rightarrow S_{1i}(0) \quad (22)$$

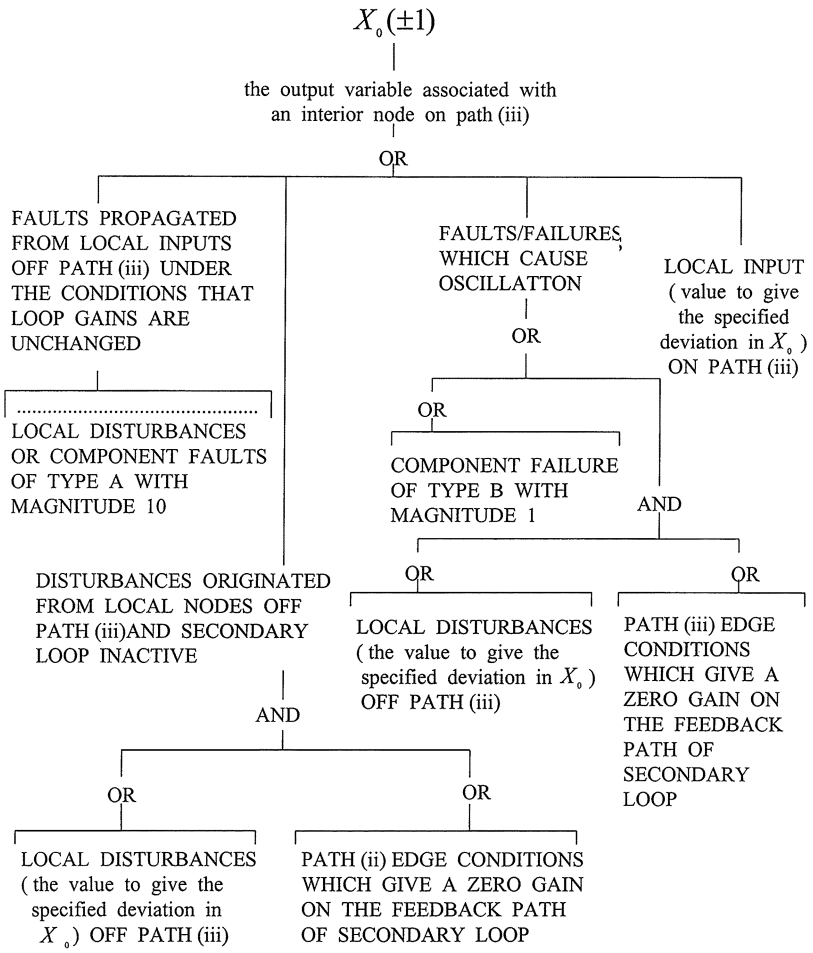

Fig. 7. Structure IV.

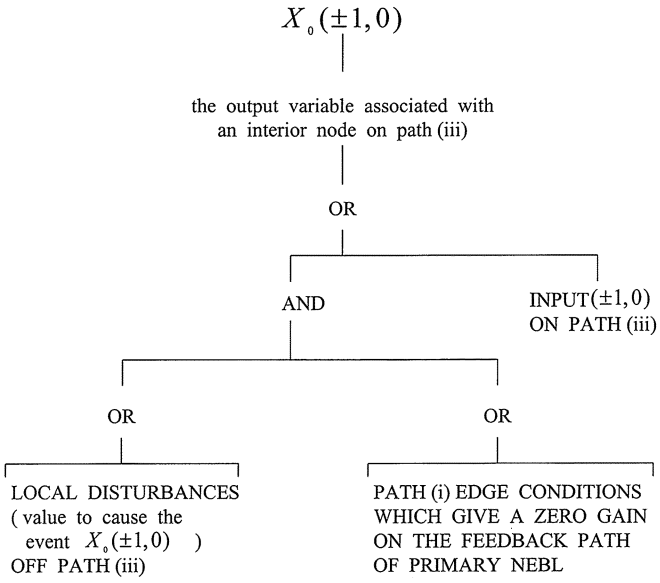

Fig. 8. Structure V.

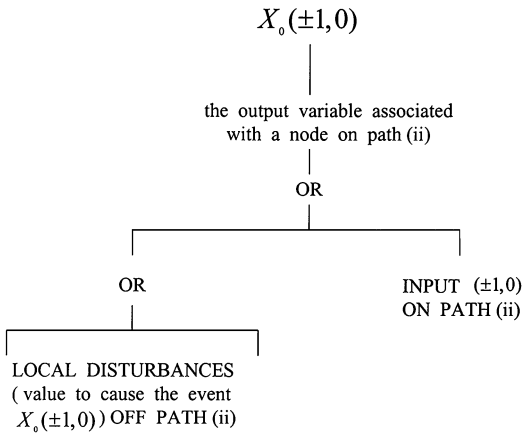

Fig. 9. Structure VI.

$$\begin{aligned} \mathrm{PO}^{(II)}_{AC,\mathrm{inner}} &\equiv S_{4i}(-10) \Rightarrow X_3(-10) \\ &\Rightarrow X_{2i}(-10) \Rightarrow S_{1i}(0) \end{aligned} \tag{23}$$

Finally, notice that row 13 is excluded from our analysis. This is based on the rationale that the occurrence probability of two simultaneous sensor malfunctions in the inner loop is negligibly low.

V. Generalized Fault Tree Structures

The conventional digraph-based approach [13] is followed in this work to synthesize the fault trees. It should be noted first that each intermediate event in a fault tree can be associated with a

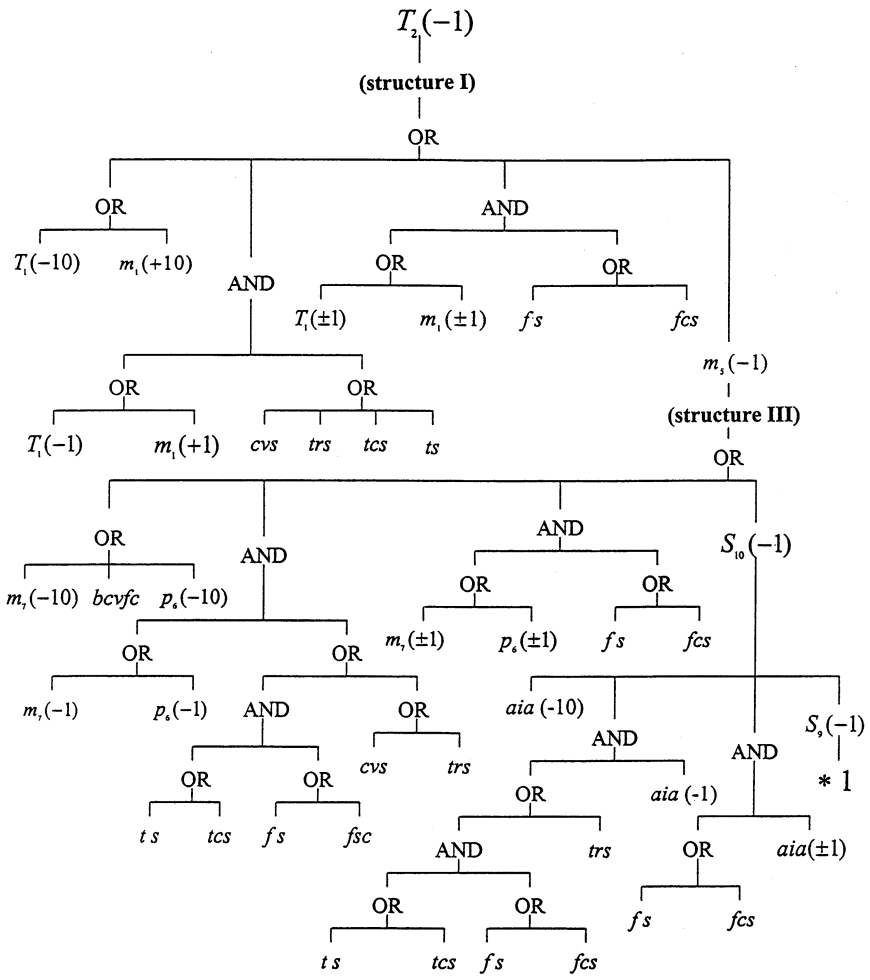

Fig. 10. The fault tree corresponding to the top Event "$T_2(-1)$" in a cascade control system—part 1.

node in the corresponding digraph. To identify the appropriate logic gate (and also its input events) connected to a particular intermediate event, it is necessary to characterize the digraph configuration of the corresponding nodes. Therefore, the simulation results given in Tables I through V must be re-organized according to *node locations* to facilitate implementation of this approach. It can be deduced from the simulation results that the intermediate events associated with the nodes on the same path, i.e., path 1, path 2, or path 3 in Fig. 3, can be actually handled in the same way. On the basis of this finding, a total of six (6) generalized faulttree structures have been developed for the cascade control systems. A detailed description is presented below:

A. Structure I

In developing the fault tree for a given cascade control system, structure I (see Fig. 4) is applicable to a deviation in the *current* output variable associated with an interior node on path 1. The four substructures in structure I, i.e., the 4 inputs of the top-most OR gate, are discussed here in a left-to-right order.

The first substructure is associated with results presented in rows 8, 9, & 14 in Table I, and rows 1, 2, & 7 in Table II. These events are basically originated from *local* input nodes, and further, can be classified into

- the uncontrolled type A faults,
- the type B failures, and
- a set-point change.

Notice that the third event class is included on the ground that the effects generated by altering the set point of master controller are essentially the same as those caused by a type B failure.

In the second substructure, the combined effects of a controllable type A fault at a local input node & a type C failure on the primary loop are described. In this part of the fault tree, a deviation in the current output is attributed to the scenario that a local disturbance cannot be compensated by the feedback mechanism of the outer control loop. Notice that two new terms, *incidence node & feedback path*, are introduced to facilitate concise description of this substructure. Their definitions are presented as follows:

- Incidence Node—The first NFBL node encountered in the digraph-based fault-tree synthesis process.
- Feedback Path—A path on a NFBL which starts at the incidence node and ends at the node representing the current output.

The corresponding simulation results can be found in rows 2, 7 through 9, 14, 16, 21 through 23, & 28 in Table III, and rows 1, 2, 7 through 9, & 14 in Table IV.

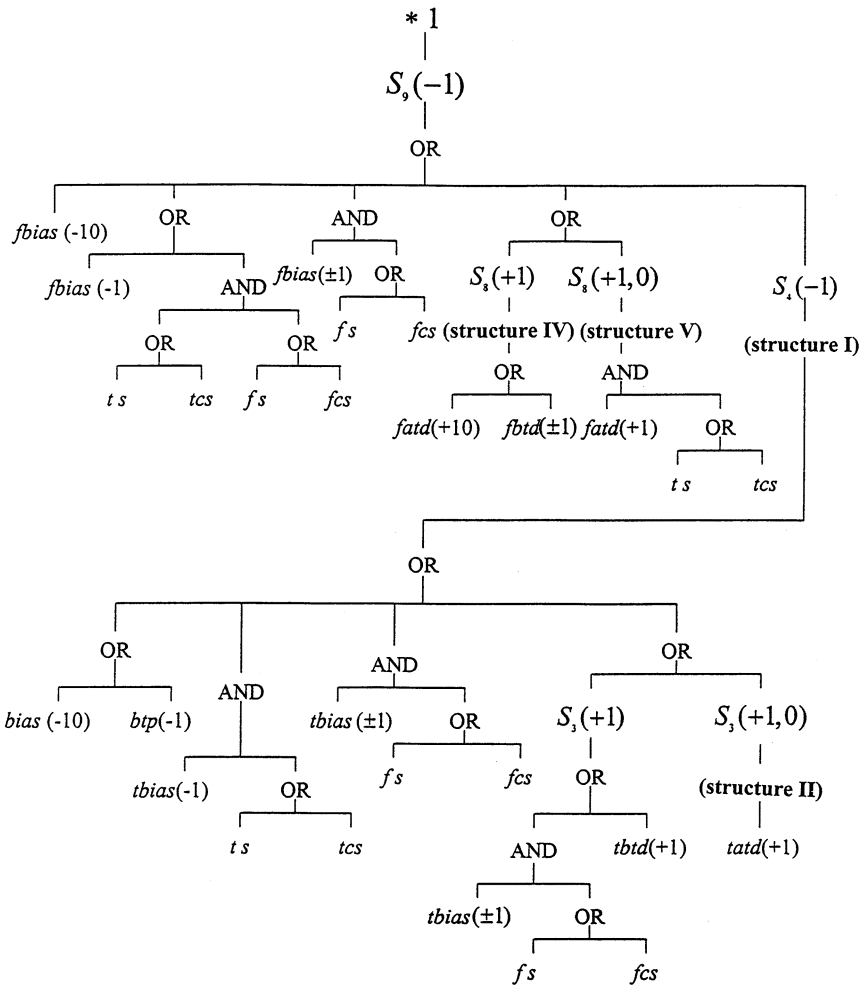

Fig. 11. The fault tree corresponding to the top event "$T_2(-1)$" in a cascade control system—part 2.

Because the oscillatory behavior of current output can be viewed as a special form of abnormal deviation from the normal steady state, its causes are listed under the third substructure. Essentially, this substructure is the conclusion drawn from rows 1, 2, 7 through 9, & 14 in Table V.

The fourth substructure is used to trace the causes of a deviation in the current output along path 1. Under the left branch of this substructure, the value of local input on path 1 can be obtained simply by dividing the output value with gain. The branch on the right hand side is applicable only when the current output is the controller output S_{4o}. Due to the integration action of the master controller, its input value may be expressed in the form $(\pm 1, 0)$.

B. Structure II

There is a need to further develop the right branch under the fourth substructure of structure I. The substructure II in Fig. 5 can be utilized for this purpose. The results in rows 1, 2, & 7 of Table I are basically reflected in the left branch. In other words, the loop variables on path 1 may be affected by the controllable local disturbances initially, but should eventually be brought back to its normal value. The right branch can be used to identify additional upstream causes along path 1.

C. Structure III

Structure III (see Fig. 6) is applicable to the current output associated with a node on path 2. Notice that this 9 structure is organized in a way similar to structure I. The four substructures here are also discussed in the same left-to-right order.

The uncontrollable effects of local inputs, i.e., the type A faults & type B failures, are included in the first substructure. The corresponding results are presented in rows 10 through 12 of Table I, and rows 3 through 5 of Table II, respectively.

Because path 2 is shared by the primary & secondary loops, the effects of a controllable local disturbance can be compensated as long as one of the loops functions normally. In other words, only after these two loops are both inactive, it is possible to create a deviation in the current output with a controllable type A fault. The second substructure is just an alternative statement of this observation. Notice that two possible combinations of type C failures are included in the branch on the right. These two possibilities are:

1) two simultaneous failures:
   - one failure occurring on the intersection of path 1 & the feedback path of primary loop, and
   - another one occurring on the intersection of path 3 & the feedback path of secondary loop;

2) a single failure occurring on the path shared by the feedback paths of both loops.

Here, the definition of feedback path is the same as that given in structure I. The simulation results corresponding to the second case described above are presented in rows 3 through 5 & 10 through 12 of Table IV. Notice that the first scenario above actually violates one of the basic assumptions of this study; the simultaneous occurrence of two or more type C failures should be ignored. Such possibilities are still kept in structure III for the sake of completeness. The user can exclude them in practical applications on a case-by-case basis.

The third substructure is used to represent the results in rows 3 through 5, & 10 through 12 in Table V. These scenarios are basically concerned with the combinations of a type A fault & a type C failure leading to system oscillation.

The fourth substructure here can be used to identify the fault propagation patterns along path 2. Notice first that an external disturbance may enter the system at an *interior* node and then propagate through path 2. The branch on the right is designed to cover such possibilities. Notice also that, because none of the sensor outputs are located on path 2, the input value under this branch should not be $(\pm 1, 0)$. On the other hand, if the current output is corresponding to the starting node of path 2, i.e., S_{4i}, it is obvious that none of its inputs are located on the same path. In this case, the local inputs on the primary & secondary loops must be considered instead. Because the input on the former is the set point of the latter, a change in S_{4o} is guaranteed to cause a deviation in S_{4i}. On the other hand, a deviation in one of the inner-loop variables on path 3 can also generate abnormal perturbations along path 2. These phenomena can be observed in the simulation results corresponding to f_{1i} in Table I to Table IV. In this substructure, the branch on the left can be used to describe the relationships between S_{4i}, and its inputs on paths 1 & 3.

D. Structure IV

Structure IV is intended for the loop variable associated with an interior node on path 3 (see Fig. 7). This structure is most likely needed in developing the left branch under the fourth substructure in structure III. Again, it is organized with the same format as that of structures I & III. Its four substructures are described in the sequel, in a left-to-right order.

The scenario presented in row 13 of Table I is reflected in the first substructure. The root causes are mainly the uncontrollable local faults of type A. It can be observed from row 6 of Table I that, although a deviation in S_{1i} may be caused by the controllable type A faults at f_{1i}, the other loop variables (except S_{4o}) can still be brought back to their normal values by the master controller. These faults cannot be the causes of a commonly-used top event, a deviation in one of the outer-loop variables.

The combined effects of a local fault of type A & type C failure on path 2 are described in the second substructure. Because the disturbance entering path 3 cannot be compensated in this case, the inner loop will be saturated eventually. This type of behavior can be observed in rows 6 & 13 of Table IV.

TABLE VI
THE MINIMAL CUT SETS IN THE CASCADE CONTROL SYSTEM

Set No.	Minimal Cut Set	Set No.	Minimal Cut Set
1	$\{T_1(-10)\}$	32	$\{p_6(\pm 1), fs\}$
2	$\{m_1(+10)\}$	33	$\{p_6(\pm 1), fcs\}$
3	$\{m_7(-10)\}$	34	$\{aia(-1), trs\}$
4	$\{p_6(-10)\}$	35	$\{aia(\pm 1), fs\}$
5	$\{bcvfc\}$	36	$\{aia(\pm 1), fcs\}$
6	$\{aia(-10)\}$	37	$\{fbias(\pm 1), fs\}$
7	$\{fbias(-10)\}$	38	$\{fbias(\pm 1), fcs\}$
8	$\{tbias(-10)\}$	39	$\{fatd(+1), ts\}$
9	$\{btp(-1)\}$	40	$\{fatd(+1), tcs\}$
10	$\{fatd(+10)\}$	41	$\{tbias(-1), ts\}$
11	$\{fbtd(\pm 1)\}$	42	$\{tbias(-1), tcs\}$
12	$\{tatd(+1)\}$	43	$\{tbias(\pm 1), fs\}$
13	$\{tbtd(+1)\}$	44	$\{tbias(\pm 1), fcs\}$
14	$\{T_1(-10), cvs\}$	45	$\{tatd(\pm 1), fs\}$
15	$\{T_1(-10), trs\}$	46	$\{tatd(\pm 1), fcs\}$
16	$\{T_1(-10), tcs\}$	47	$\{m_7(-1), fs, ts\}$
17	$\{T_1(-10), ts\}$	48	$\{m_7(-1), fs, tcs\}$
18	$\{m_1(+10), cvs\}$	49	$\{m_7(-1), fcs, ts\}$
19	$\{m_1(+10), trs\}$	50	$\{m_7(-1), fcs, tcs\}$
20	$\{m_1(+10), tvs\}$	51	$\{p_6(-1), fs, ts\}$
21	$\{m_1(+10), ts\}$	52	$\{p_6(-1), fs, tcs\}$
22	$\{T_1(\pm 1), fs\}$	53	$\{p_6(-1), fcs, ts\}$
23	$\{T_1(\pm 1), fcs\}$	54	$\{p_6(-1), fcs, tcs\}$
24	$\{m_1(\pm 1), fs\}$	55	$\{aia(-1), fs, ts\}$
25	$\{m_1(\pm 1), fcs\}$	56	$\{aia(-1), fs, tcs\}$
26	$\{m_7(-1), cvs\}$	57	$\{aia(-1), fcs, ts\}$
27	$\{m_7(-1), trs\}$	58	$\{aia(-1), fcs, tcs\}$
28	$\{p_6(-1), cvs\}$	59	$\{fbias(-1), fs, ts\}$
29	$\{p_6(-1), trs\}$	60	$\{fbias(-1), fs, tcs\}$
30	$\{m_7(\pm 1), fs\}$	61	$\{fbias(-1), fcs, ts\}$
31	$\{m_7(\pm 1), fcs\}$	62	$\{fbias(-1), fcs, tcs\}$

The failure mechanisms which result in system oscillation are depicted in the third substructure. They can be classified into two groups:

1) a type B failure directly affecting the interior nodes of path 3;
2) a controllable fault of type A entering path 3 after a type C failure occurring on the same path.

An example of the first mechanism can be found in row 6 of Table II. Because there is only one interior node on path 3 of the standard digraph in Fig. 3, examples of the second mechanism are not included in the simulation results. However, it is clear that the effects of these two mechanisms should be the same, because a type B failure can really be viewed as a type A fault & a type C failure acting on the same equipment.

Finally, the fourth substructure can also be used to trace the causes of a deviation in the current output along path 3. Because the controller output S_{4i} is not an interior node of path 3, the possibility of input value $(\pm, 0)$ is excluded from consideration.

E. Structure V

The structure presented in Fig. 8 is also needed in developing the left branch under the fourth substructure in Structure III. The current output in this case must be associated with an interior node on path 3. The substructure on the left hand side is used to represent the fault propagation patterns observed in rows 6, 13, 20 & 27 of Table III. The second substructure can be used to locate the causes along path 3.

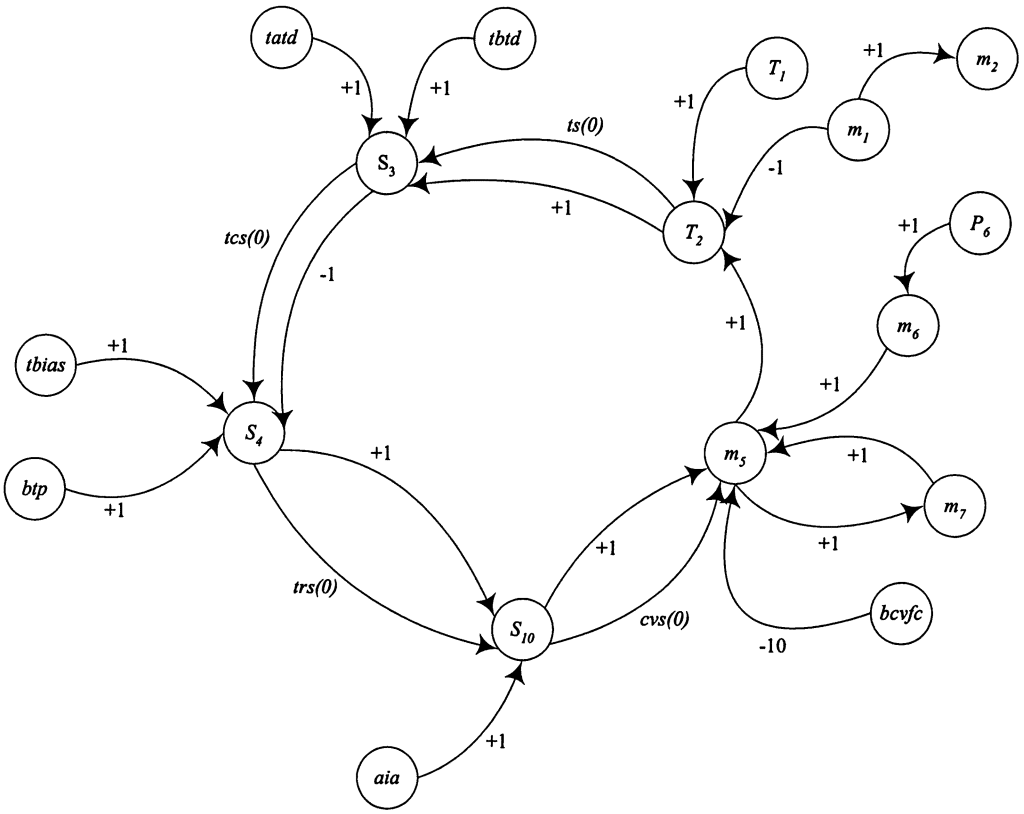

Fig. 12. The digraph model of a heat-exchange process with single-loop feedback control.

F. Structure VI

The structure in Fig. 9 can be applied to a path-2 variable with deviation value $(\pm, 0)$. It is useful only when there is a need to develop the remaining fault tree after applying structure II or structure V in a recursive fashion. This recursive implementation process is continued until the starting node of path 1 or path 3 becomes a local input to the current output of the adopted fault tree structure.

VI. Application

To demonstrate the usefulness of the generalized fault tree structures, they have been applied to the heat exchange system described in Fig. 1. The top event chosen for this example is $T_2(-1)$ (that is, the temperature of stream 2 is too low). The resulting fault tree is presented in Figs. 10 & 11. The minimal cut sets can then be determined accordingly (Table VI).

Notice that a cascade control strategy only complements the standard single-loop feedback control. Because the cascade system requires more control equipment, its reliability is expected to be lower than the equivalent single-loop system. Consequently, there is a need to quantitatively compare the risks of system failures in both cases. If the same heat exchange process is controlled with a single feedback loop, the corresponding system digraph can be obtained by removing the nodes S_8 & S_9 from Fig. 2, and then connecting S_4 to S_{10} (see Fig. 12). In this case, the fault tree can be constructed easily with the conventional techniques (Figs. 13 & 14). Notice that, although both trees are similar, many branches in the tree for the cascade control system do not appear in this new tree. In particular, these missing branches include

- the first four branches under $S_9(-1)$ in Fig. 11 (the failure mechanisms associated with the flow sensor and controller); and
- the branches corresponding to the third substructure in structure I and III (the causes of system oscillation).

The minimal cut sets of the fault tree presented in Figs. 13 and 14 are presented in Table VII. It is clear that, as a result of the missing branches indicated above, the causes of system failure in the single-loop system are much fewer than those in the cascade system. In particular, 25 minimal cut sets of the fault tree in Figs. 10 & 11 are excluded in Table VII. Their set numbers in Table VI are: 7, 10, 11, 22 through 25, 30 through 33, 35 through 40, 43 through 46, & 59 through 62. These results certainly reveal that the cascade control system is less reliable. However, notice that the 47th to 58th sets in Table VI are reduced to the sets numbered as 21, 22, 25, 26, 28 & 29 in Table VII. In these cases, the cascade system should be less vulnerable because the occurrence probability of two simultaneous type C failure can be assumed to be negligible.

Therefore, in terms of reliability and control performance, it is not obvious which one of the two control strategies discussed above is better in general. The issue of trade-off has to be addressed more rigorously on the basis of quantitative risk calculation according to the fault trees presented in Figs. 10, 11, 13, & 14.

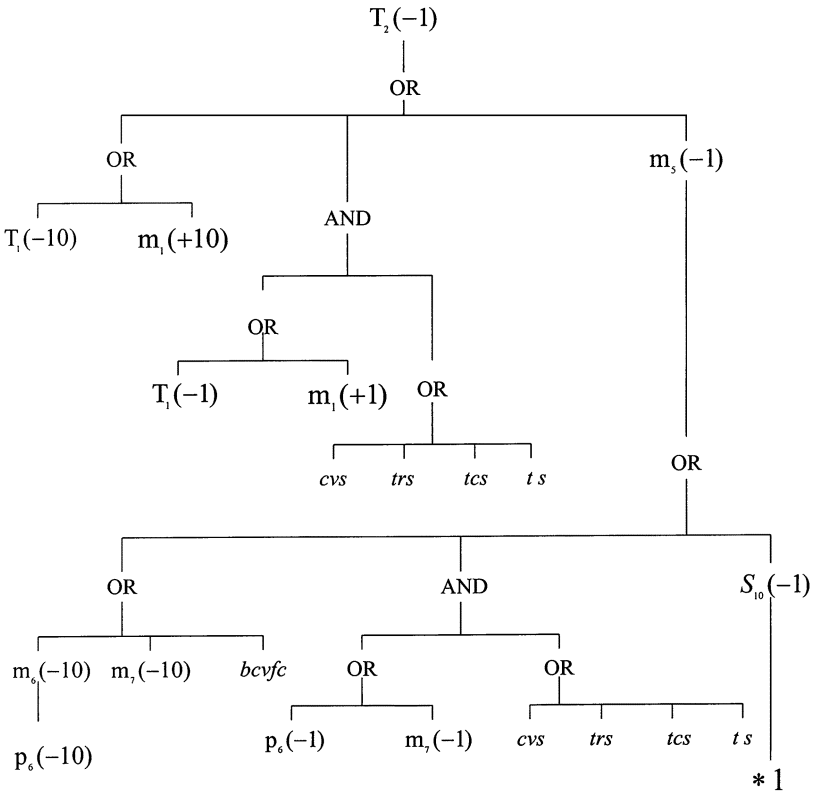

Fig. 13. The fault tree corresponding to the top event "$T_2(-1)$" in a single-loop feedback control system—part 1.

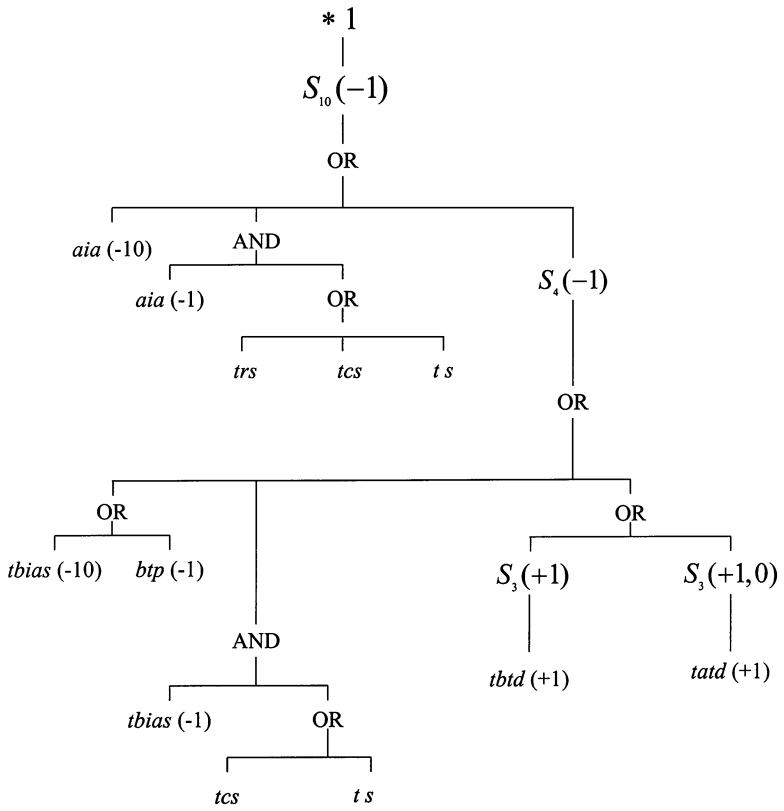

Fig. 14. The fault tree corresponding to the top event "$T_2(-1)$" in a single-loop feedback control system—part 2.

TABLE VII
THE MINIMAL CUT SETS IN THE SINGLE-LOOP FEEDBACK CONTROL SYSTEM

Set No.	Minimal Cut Set	Set No.	Minimal Cut Set
1	$\{T_1(-10)\}$	17	$\{m_1(+1), tcs\}$
2	$\{m_1(+10)\}$	18	$\{m_1(+1), ts\}$
3	$\{m_7(-10)\}$	19	$\{m_7(-1), cvs\}$
4	$\{p_6(-10)\}$	20	$\{m_7(-1), trs\}$
5	$\{bcvfc\}$	21	$\{m_7(-1), tcs\}$
6	$\{aia(-10)\}$	22	$\{m_7(-1), ts\}$
7	$\{tbias(-10)\}$	23	$\{p_6(-1), cvs\}$
8	$\{btp(-1)\}$	24	$\{p_6(-1), trs\}$
9	$\{tatd(+1)\}$	25	$\{p_6(-1), tcs\}$
10	$\{tbtd(+1)\}$	26	$\{p_6(-1), ts\}$
11	$\{T_1(-1), cvs\}$	27	$\{aia(-1), trs\}$
12	$\{T_1(-1), trs\}$	28	$\{aia(-1), tcs\}$
13	$\{T_1(-1), tcs\}$	29	$\{aia(-1), ts\}$
14	$\{T_1(-1), ts\}$	30	$\{tbias(-1), tcs\}$
15	$\{m_1(+1), cvs\}$	31	$\{tbias(-1), ts\}$
16	$\{m_1(+1), trs\}$		

APPENDIX A
CLASSIFICATION OF FAULTS AND FAILURES

The definitions of faults and failures suggested by Himmelblau [11] are followed in this work. The word *fault* is used to designate the departure from an acceptable range of 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. It should be noted that a failure should be viewed as a basic event which may trigger fault propagation in a system. On the other hand, a fault is always the result of an equipment failure or another fault. Because a system boundary must be selected to limit the scope of fault tree analysis, some of the faults in a system could be caused by *external* faults or failures. These faults are also regarded as "initiating" events in the present study.

The initiating faults & equipment failures are classified into four types based on their digraph representations, and also the patterns of their propagation in the system:

Type A: For initiating faults such as abnormal variations 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 Fig. 15, where x_1 & x_2 are process variables, and f is the fault of type A. The effects of this type 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, if *both* x_1 & x_2 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 & 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.

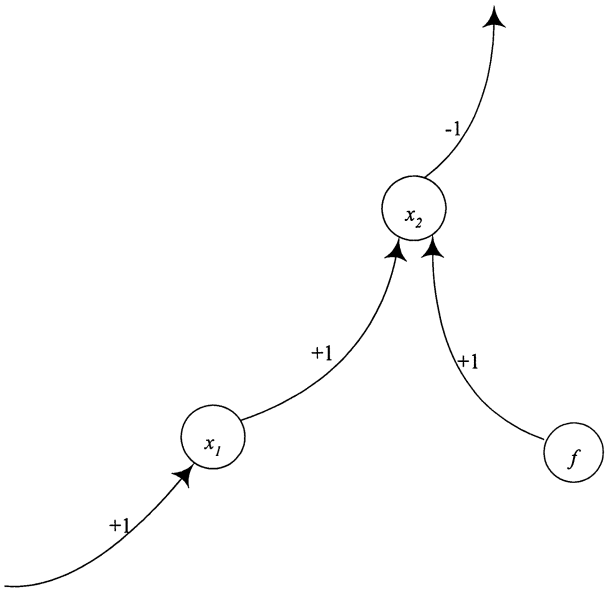

Fig. 15. The digraph model of type A faults.

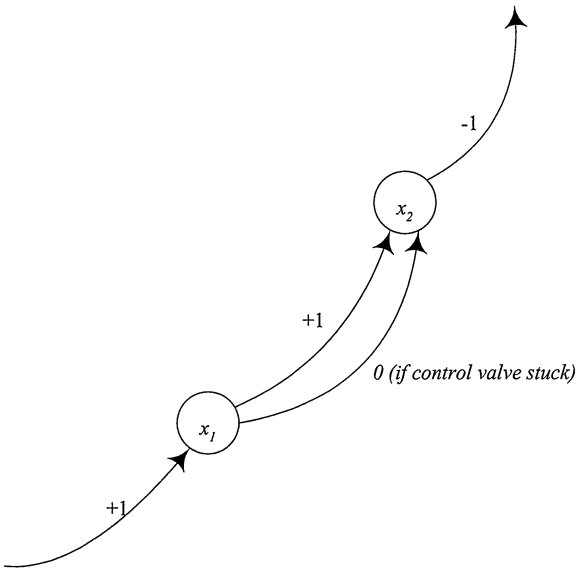

Fig. 16. The digraph model of type C failures.

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 Fig. 16. The occurrence of a failure of this type only changes the configuration of the system digraph; the edge between x_1 & x_2 can be considered as nonexisting. 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 Fig. 17, 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.

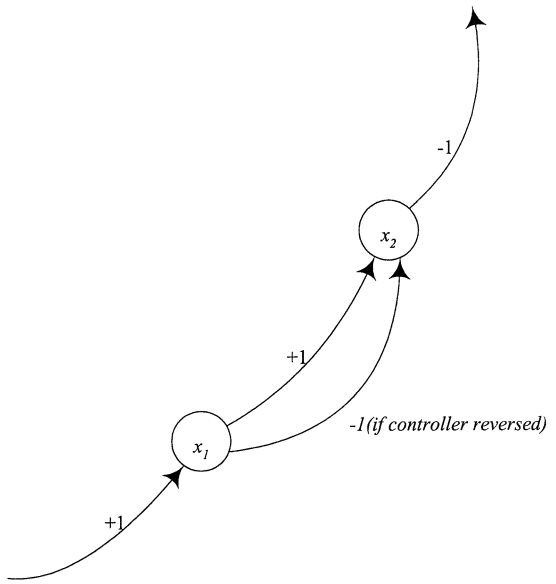

Fig. 17. The digraph model of type D failures.

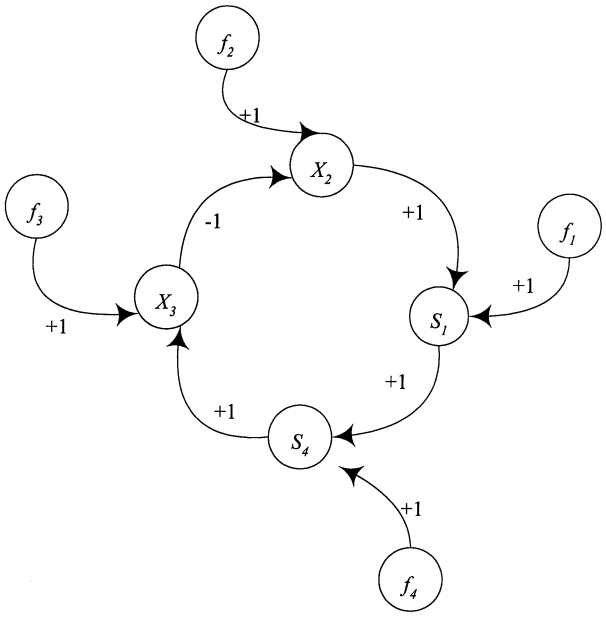

Fig. 18. The digraph configuration of a typical NFBL.

APPENDIX B
THE FAULT PROPAGATION PATTERNS IN A SINGLE NFBL

The fault propagation patterns in a single NFBL can be determined with qualitative simulation techniques. Let us consider the standard NFBL presented in Fig. 18. In this figure, S_1 is the sensor signal, X_2 represents the controlled variable, X_3 is the manipulated variable, S_4 denotes the output signal from the controller, and the nodes $f_1, f_2, f_3, \&\ f_4$ are used to represent type A faults and/or type B failures. In addition, to facilitate illustration of the phenomena caused by an external disturbance and/or an equipment failure, let us define an *event symbol* $N(v)$ to represent the abnormal condition associated with a node on the fault propagation path. Here, N denotes the node label, and v is its qualitative value; this symbol denotes the event "$N = v$".

Three types of scenarios are described next:

The Effects of a Type A Fault: As mentioned previously, any disturbance to a NFBL generates two opposite effects on the incidence loop variable. For example, although the gain of the edge between f_2 & X_2 is positive, the product of the gains on the path $f_2 \rightarrow X_2 \rightarrow S_1 \rightarrow S_4 \rightarrow X_3 \rightarrow X_2$ is negative. The net effect is zero if the control loops function properly. The event $f_2(+1)$ causes $X_2(0), S_1(0), S_4(+1), \&\ X_3(+1)$ at new steady state. This special behavior of NFBL creates a problem in simulating fault propagation, i.e., the cause-effect relations are not consistent with individual edge gains specified in the digraph.

To overcome this problem, Hwang & Chang [6] suggested that the states of loop variables can be represented with symbols of the form (v_0, v_∞). This symbol can be regarded as the state of a loop variable which would have a value v_0 without feedback, but approaches v_∞ at the new steady state due to regulatory action. Thus, due to its integral action, the digraph model of PID controller in NFBL can really be interpreted according to Table VIII. Consequently, the effects of a type A fault corresponding to f_2 can be described with a set of modified event symbols, i.e.,

$$\{X_2(+1,0), S_1(+1,0), S_4(+1,+1), X_3(+1,+1)\} \quad \text{(B1)}$$

Furthermore, the implied fault propagation sequence can be expressed explicitly in terms of a *precedence order*;

$$\begin{aligned} f_2(+1) &\Rightarrow X_2(+1) \Rightarrow S_1(+1) \Rightarrow S_4(+1) \Rightarrow X_3(+1) \\ &\Rightarrow X_2(0) \\ &\Rightarrow S_1(0) \Rightarrow S_4(+1) \Rightarrow X_3(+1) \end{aligned} \quad \text{(B2)}$$

Here, the symbol $\Rightarrow$ is used to represent the *direct* causal relation between two abnormal events.

The patterns of deviations in the loop variables caused by disturbances at various locations are summarized in Table IX. Several interesting features can be observed from this table:

- a sub-path is formed by the loop variables with values $(v_0, 0)$

TABLE VIII
NEW INTERPRETATIONS OF GAINS BETWEEN SENSOR OUTPUTS AND CONTROLLER OUTPUTS

gain	sensor output	controller output
+1	(+1, 0) (-1, 0)	(+1, +1) (-1, -1)
-1	(+1, 0) (-1, 0)	(-1, -1) (+1, +1)

TABLE IX
FAULT PROPAGATION PATTERNS IN A SINGLE NFBL—A TYPE A FAULT OF VALUE +1

fault origin	S_1	X_2	X_3	S_4
$f_1(+1)$	(+1, 0)	(-1, -1)	(+1, +1)	(+1, +1)
$f_2(+1)$	(+1, 0)	(+1, 0)	(+1, +1)	(+1, +1)
$f_3(+1)$	(-1, 0)	(-1, 0)	(+1, 0)	(-1, -1)
$f_4(+1)$	(-1, 0)	(-1, 0)	(+1, 0)	(+1, 0)

TABLE X
FAULT PROPAGATION PATTERNS IN A SINGLE NFBL—A TYPE A FAULT OF VALUE +10

fault origin	S_1	X_2	X_3	S_4
$f_1(+10)$	(+10, +1)	(-10, -10)	(+10, +10)	(+10, +10)
$f_2(+10)$	(+10, +1)	(+10, +1)	(+10, +10)	(+10, +10)
$f_3(+10)$	(-10, -1)	(-10, -1)	(+10, +1)	(-10, -10)
$f_4(+10)$	(-10, -1)	(-10, -1)	(+10, +1)	(+10, +1)

TABLE XI
FAULT PROPAGATION PATTERNS IN A SINGLE NFBL —A TYPE B FAILURE OF VALUE +1

fault origin	S_1	X_2	X_3	S_4
$f_1(+1)$	+1	-10	+10	+10
$f_2(+1)$	+1	+1	+10	+10
$f_3(+1)$	-1	-1	+1	-10
$f_4(+1)$	-1	-1	+1	+1

- the starting node of this sub-path is the incidence node, and
- the terminal node is always the one corresponding to a sensor output.

A similar analysis can be carried out for disturbances of magnitude 10. The value 10 in this study is regarded as a "very large" quantity which would saturate the control loop [13]. A summary of the corresponding fault propagation patterns is presented in Table X. Because the loop is saturated, the effects generated by a disturbance with magnitude 10 cannot be cancelled with regulatory action, and a nonzero deviation always occurs in the sensor output.

The Effects of a Type B Failure: From the definitions presented in Appendix A, it is clear that the digraph representation of a component failure of type B is essentially equivalent to that of simultaneous occurrence of a type C failure & a local disturbance. Because in this case the NFBL is broken, and also the value of incidence loop variable is fixed at $+1$ (or -1), the fault propagation pattern can be determined on the basis of the resulting simple digraph *without* feedback. For example, the simulation result corresponding to a type B failure at f_3 can be expressed as

$$f_3(+1) \Rightarrow X_3(+1) \Rightarrow X_2(-1) \Rightarrow S_1(-1) \Rightarrow S_4(-10) \quad \text{(B3)}$$

Notice that, due to the integral action in controller, the value of S_4 should reach -10 eventually. A summary of XI.

The Combined Effects of a Type a Fault and a Type C Failure: As mentioned previously, a type C failure is represented with a conditional edge with zero gain. If it occurs in the control system, the regulatory action in NFBL is essentially lost. The corresponding feedback loop should be broken due to such a failure. The combined effects of a type A fault & a type C failure can be evaluated by determining the fault propagation behavior in the resulting digraph. For example, the simulation result of a type A fault at f_4 & a type C failure between X_2 & S_1 is

$$f_4(+1) \Rightarrow S_4(+1) \Rightarrow X_3(+1) \Rightarrow X2(-1) \Rightarrow S_1(0) \quad \text{(B4)}$$

Because the effects of other combinations of type A faults & type C failures can be determined easily in a straightforward fashion, the corresponding simulation results are omitted for the sake of brevity.

REFERENCES

[1] D. J. Allen, "Digraphs and fault trees," *I&EC Fundam.*, vol. 23, p. 175, 1984.

[2] D. J. Allen and M. S. M. Rao, "New algorithms for the synthesis and analysis of fault trees," *I&EC Fundam.*, vol. 19, pp. 79–0, 1980.

[3] J. D. Andrews and J. M. Morgan, "Application of digraph method of fault tree construction to process plant," *Reliab. Eng.*, vol. 14, p. 85, 1986.

[4] J. D. Andrews and G. Brennan, "Application of the digraph method of fault tree construction to a complex control configuration," *Reliab. Eng. Syst. Saf.*, vol. 28, p. 357, 1990.

[5] M. F. Chamow, "Directed graph techniques for the analysis of fault trees," *IEEE Trans. Rel.*, vol. R-27, p. 7, 1978.

[6] C. T. Chang and H. C. Hwang, "New developments of the digraph-based techniques for fault-tree synthesis," *Ind. Eng. Chem. Res.*, vol. 31, p. 1490, 1992.

[7] C. T. Chang and K. S. Hwang, "Studies on the digraph-based approach for fault-tree synthesis. 1. The ratio-control systems," *Ind. Eng. Chem. Res.*, vol. 33, p. 1520, 1994.

[8] C. T. Chang, D. S. Hsu, and D. M. Hwang, "Studies on the digraph-based approach for fault-tree synthesis. 2. The trip systems," *Ind. Eng. Chem. Res.*, vol. 33, p. 1700, 1994.

[9] D. L. Cummings, S. A. Lapp, and G. J. Powers, "Fault tree synthesis from a directed graph model for a power distribution network," *IEEE Trans. Rel.*, vol. R-32, pp. 140–0, 1983.

[10] E. J. Henley and H. Kumamoto, *Designing for Reliability and Safety Control*. Englewood Cliffs, New Jersey: Prentice-Hall, 1985, pp. 438–441.

[11] D. M. Himmelblau, *Fault Detection and Diagnosis in Chemical and Petrochemical Processes*. New York, NY: Elsevier, 1978, pp. 2–10.

[12] H. E. Lambert, "Comments on the lapp-powers 'Computer-aided synthesis of fault trees'," *IEEE Trans. Rel.*, vol. R-28, p. 6, 1979.

[13] S. A. Lapp and G. J. Powers, "Computer-aided synthesis of fault trees," *IEEE Trans. Rel.*, vol. R-26, p. 2, 1977.

[14] ——, "Update of Lapp-Powers fault-tree synthesis algorithm," *IEEE Trans. Rel.*, vol. R-28, pp. 12–0, 1979.

[15] O. O. Oyeleye and M. A. Kramer, "Qualitative simulation of chemical process systems: Steady state analysis," *AIChE J*, vol. 34, pp. 1441–0, 1988.

[16] J. A. Shaeiwitz, S. A. Lapp, and G. J. Powers, "Fault tree analysis of sequential systems," in *I&EC Proc. Des. Dev.*, vol. 16, 1977, pp. 529–0.

Shi-Ning Ju received his M.S. degree in Chemical Engineering from National Taiwan University in 2000. In his thesis, a digraph-based procedure has been developed to synthesize fault tress for multi-loop process control systems. He is currently a process engineer at Taiwan Semi-Conductor Manufacturing Co. (TSMC), Hsinchu, Taiwan.

Cheng-Liang Chen received his Ph.D. degree in Chemical Engineering from National Taiwan University in 1987. He is currently a Professor in the Department of Chemical Engineering at National Taiwan University. His research interests include control systems design, optimization of chemical processes, and fuzzy modeling/control in chemical engineering.

Chuei-Tin Chang is a Professor in the Department of Chemical Engineering at National Cheng Kung University, Tainan, Taiwan. He was an Assistant Professor in the Department of Chemical Engineering at University of Nebraska, Lincoln, NE, and also worked as a Process Engineer for FMC Corporation, Princeton, NJ. He received his Ph.D. in 1982 in Chemical Engineering from Columbia University (New York City) and his B.S. in 1976 from National Taiwan University (Taipei). His research interests are mainly concerned with process systems engineering, especially in areas such as process synthesis and design, process safety assessment, fault detection and diagnosis, and metabolic network modeling.