

Fault Tree Analysis of Sequential Systems

Joseph A. Shaeiwitz, Steven A. Lapp, and Gary J. Powers*

Department of Chemical Engineering, Carnegie-Mellon University, Pittsburgh, Pennsylvania 15213

Fault tree analysis is a systems safety technique for determining the logical combinations of events which could cause a specific hazard to occur. Digraph models are proposed which describe sequential relationships between events. A computer program which automatically constructs fault trees from digraph models is illustrated for an air-drying process.

Introduction

Fault tree analysis has been used in the aerospace, electronics, nuclear, and chemical industries to aid in (1) the discovery and control of failures before they occur; (2) the analysis of accidents, and (3) the planning of maintenance activities (Fussell, 1974; Powers, 1974). In the use of the fault tree method many safety analysts have expressed concern over the ability of the method to handle sequentially dependent events.

Esary recently illustrated the problem of applying fault tree analysis to sequential systems (Esary and Ziehms, 1975). In his analysis he considered a phased-mission in which the status and function of the components within a system depend on the phase (time sequence) of the mission. Esary presented a fault tree for the phased mission which was composed of sub-trees, one for each phase in the mission. He also presented an excellent discussion of the difficulties involved in calculating the probability of system success given the sequential interdependence of events. In this paper we present a strategy for partially automating the synthesis of fault trees when sequential interdependencies are considered. The key to the

method is the development of cause and effect models which explicitly consider the possible sequential interactions between events. These models are used in an algorithm which automatically generates fault trees.

Digraph Models

In a previous paper (Lapp, 1977), we have developed the concept of a digraph model for the description of both the normal and failed behavior of components in interconnected systems. The models will be briefly reviewed here and extended to sequential situations.

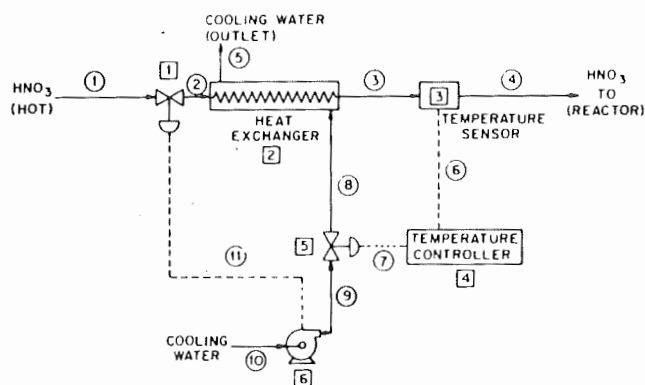


Figure 1. Flow diagram for part of a nitrification process. When low pump speed is sensed at the pump, valve 1 is closed.

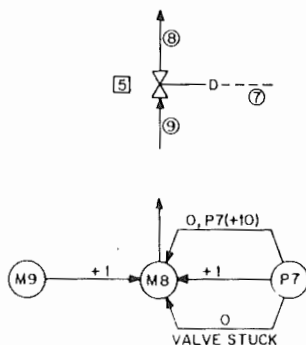


Figure 2. A cause-and-effect model for a control valve.

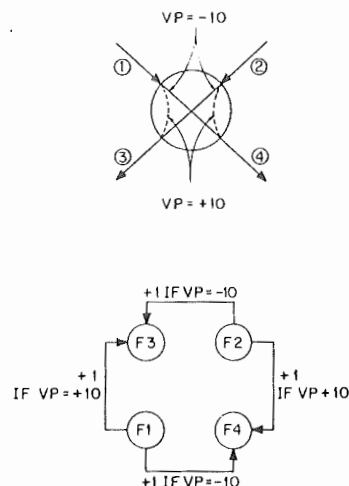


Figure 3. Cause-and-effect model for a four-way valve.

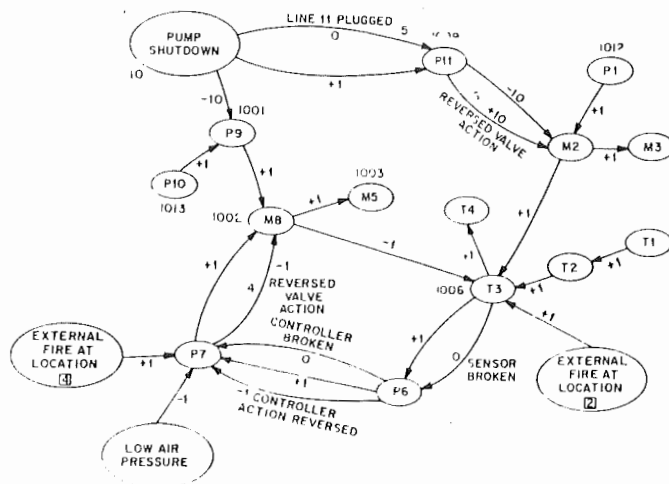


Figure 4. A partial cause-and-effect model for the output variable temperature in stream 4 (T_4) in Figure 1.

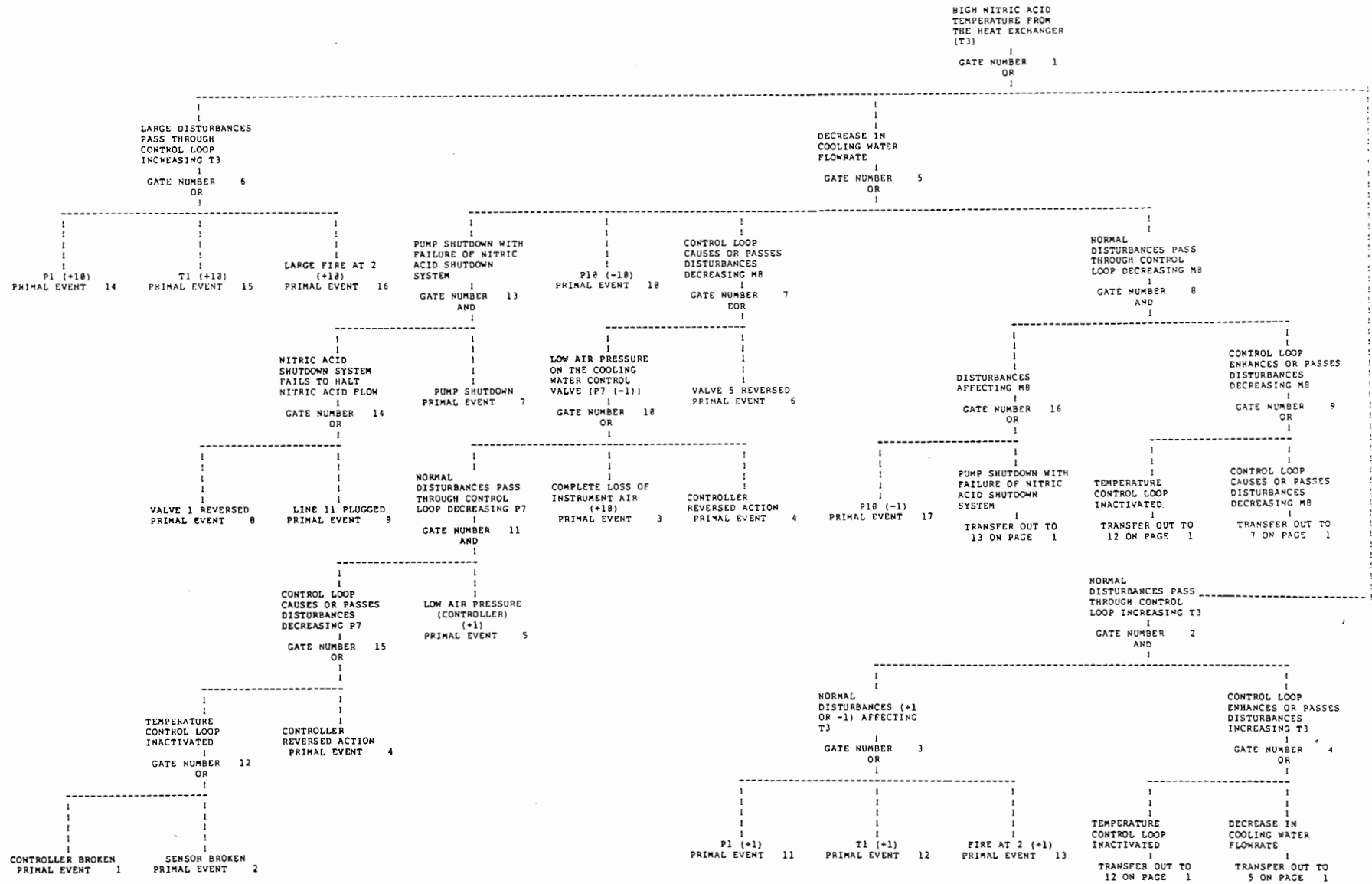


Figure 5. Fault tree for the event T4 too high.

Table I. Operating Procedure for Fixed-Bed Drier System

| Time period | Time since beginning of cycle, h | Value position (steam connections) | | | Bed status | |
|-------------|----------------------------------|------------------------------------|-----------------------|-----------------------|--------------|--------------|
| | | 3W | 4WI | 4WII | Bed I | Bed II |
| 1 | 1 } 2 } | 11→12 | 18→19 AND 22→23 | 20→21 AND 24→25 | Regeneration | In service |
| 2 | 3 | 11→18 | 18→19 AND 22→23 | 20→21 AND 24→25 | Cooling | In service |
| 3 | 4 } 5 } | 11→12 | 18→23 AND 22→19 | 20→25 AND 24→21 | In service | Regeneration |
| 4 | 6 | 11→18 | 18→23 AND 22→19 | 20→25 AND 24→21 | In service | Cooling |

Return to Time Period 1

In developing logic models for physical systems, it is necessary to capture the cause-and-effect nature of interactions which occur between the variables which describe the system

Table II. Sequential Dryer Process Events

| Title event number | Probability | Text |
|--------------------|-----------------------|--|
| 1 | 2.00×10^{-3} | 4-Way valve leaks across |
| 2 | 5.00×10^{-5} | Fire at Bed I |
| 3 | 1.20×10^{-4} | No alumina in Bed I, or channeling |
| 4 | 7.15×10^{-4} | 4-Way valve II motor failure |
| 5 | 3.30×10^{-1} | Time = 1 |
| 6 | 1.67×10^{-1} | Time = 2 |
| 7 | 4.72×10^{-6} | 4-Way valve II timer changes at wrong time |
| 8 | 5.00×10^{-8} | Fire at Bed II |
| 9 | 1.20×10^{-4} | No alumina in Bed II, or channeling |
| 10 | 1.67×10^{-1} | Time = 4 |
| 11 | 4.72×10^{-6} | 4-Way valve II timer fails |
| 12 | 8.63×10^{-5} | 4-Way valve II control line 29 cut |
| 13 | 3.30×10^{-1} | Time = 3 |
| 14 | 5.00×10^{-4} | Inlet air flow up |
| 15 | 5.00×10^{-4} | Proportionating valve pressure up (P10) |
| 16 | 7.15×10^{-4} | 4-Way valve I motor failure |
| 17 | 7.99×10^{-5} | Heater leaks steam into air |
| 18 | 5.00×10^{-4} | Inlet air water concentration up |
| 19 | 7.15×10^{-4} | 3-Way valve motor failure |
| 20 | 4.72×10^{-6} | 4-Way valve I timer changes at wrong time |
| 21 | 4.72×10^{-6} | 4-Way valve I timer fails |
| 22 | 8.63×10^{-5} | 4-Way valve I control line 28 cut |
| 23 | 1.00×10^{-5} | Water separator trap clogged |
| 24 | 2.10×10^{-3} | Valve 6 closed |
| 25 | 5.00×10^{-8} | External fire at separator |
| 26 | 4.72×10^{-6} | 3-Way valve timer changes at wrong time |
| 27 | 4.72×10^{-6} | 3-Way valve timer fails |
| 28 | 8.63×10^{-5} | 3-Way valve control line 27 cut |
| 29 | 5.00×10^{-4} | Cooling water flow down |
| 30 | 5.00×10^{-4} | Cooling water temperature up |
| 31 | 2.99×10^{-3} | Cooler fouled |
| 32 | 5.00×10^{-8} | External fire at cooler |
| 33 | 2.10×10^{-3} | Valve 4 closed |
| 36 | 5.00×10^{-4} | Inlet Air pressure up |

(i.e., temperatures, pressures, flow rates, concentrations, operator action, voltages, valve positions, etc.) and events which occur within the system (i.e., valve failure, fire, explosion, operator error, weather changes, etc.). For example, consider the flow sheet given in Figure 1. The system is composed of valves, pumps, heat exchangers, etc. In order to determine how failures or deviations in input variables propagate through the system, it is possible to construct digraphs whose nodes represent events or variables and whose edges represent the relationships between the nodes. Figure 2 illustrates a cause and effect model for valve 5 in this system. Note that the edges may be event dependent. That is, a relationship between two variables may be dependent on the value of other variables or events in the system. For example, the gain between the pressure on the valve actuator P7 and the mass flow rate leaving the valve M8 is normally +1. An increase in pressure opens the valve and allows a higher flow rate. However, if the pressure on the actuator is very high (P7 = +10) the gain is 0. The valve is wide open and further increases in pressure P7 do not give an increase in the flow rate M8.

If the edges in a digraph are made dependent on other events in the system, it is possible to capture in one digraph the sequential behavior of the complete system. Consider the four-way valve shown in Figure 3. When the valve is in position 1 (valve position = VP = +10) the flow is from stream 1 to stream 3 and from stream 2 to stream 4. In position 2 (valve position = VP = -10) the flow is from stream 2 to stream 3 and from stream 1 to stream 4. A digraph for this valve is given in Figure 3 where VP is the valve position. If, from another

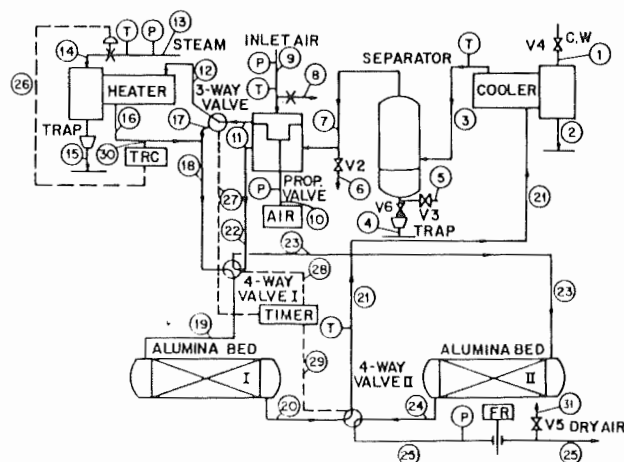
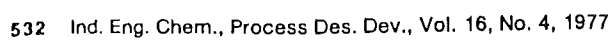


Figure 6. Flow diagram of a utility air drying process. After King (1970).



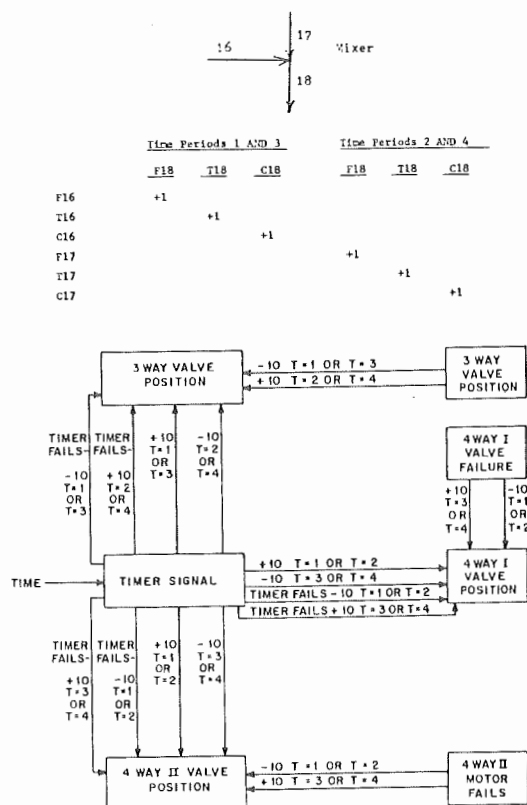
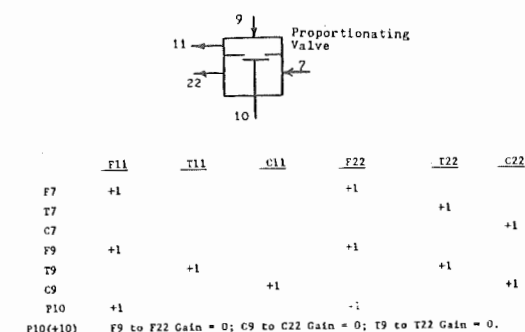
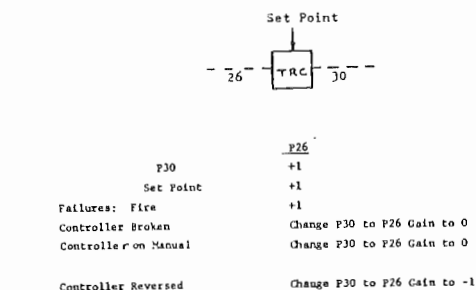
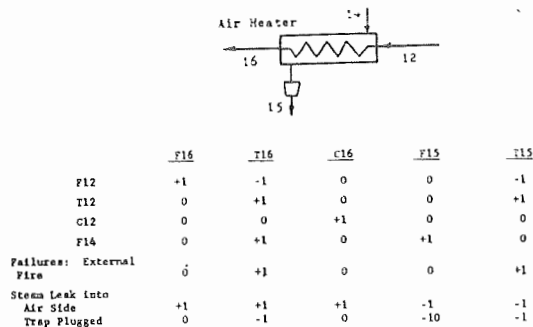
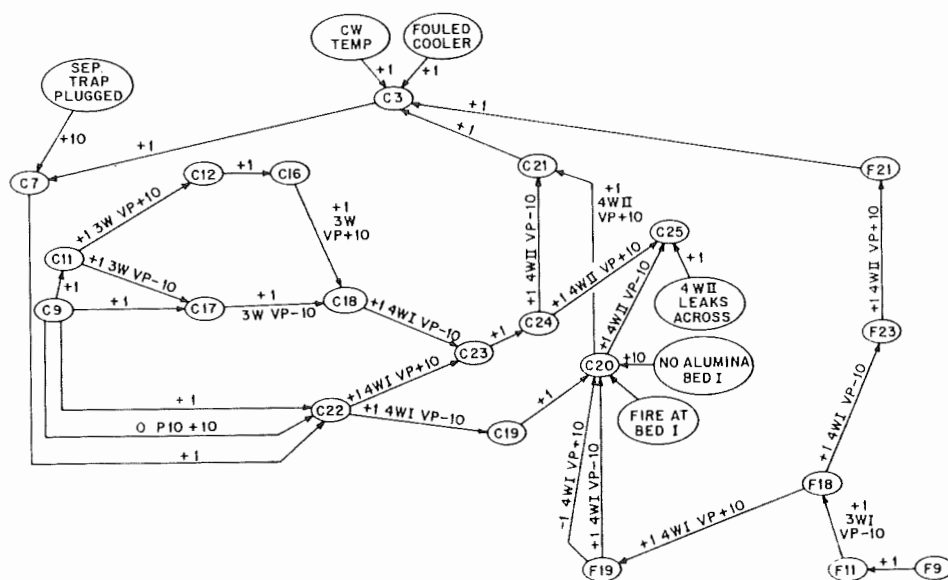
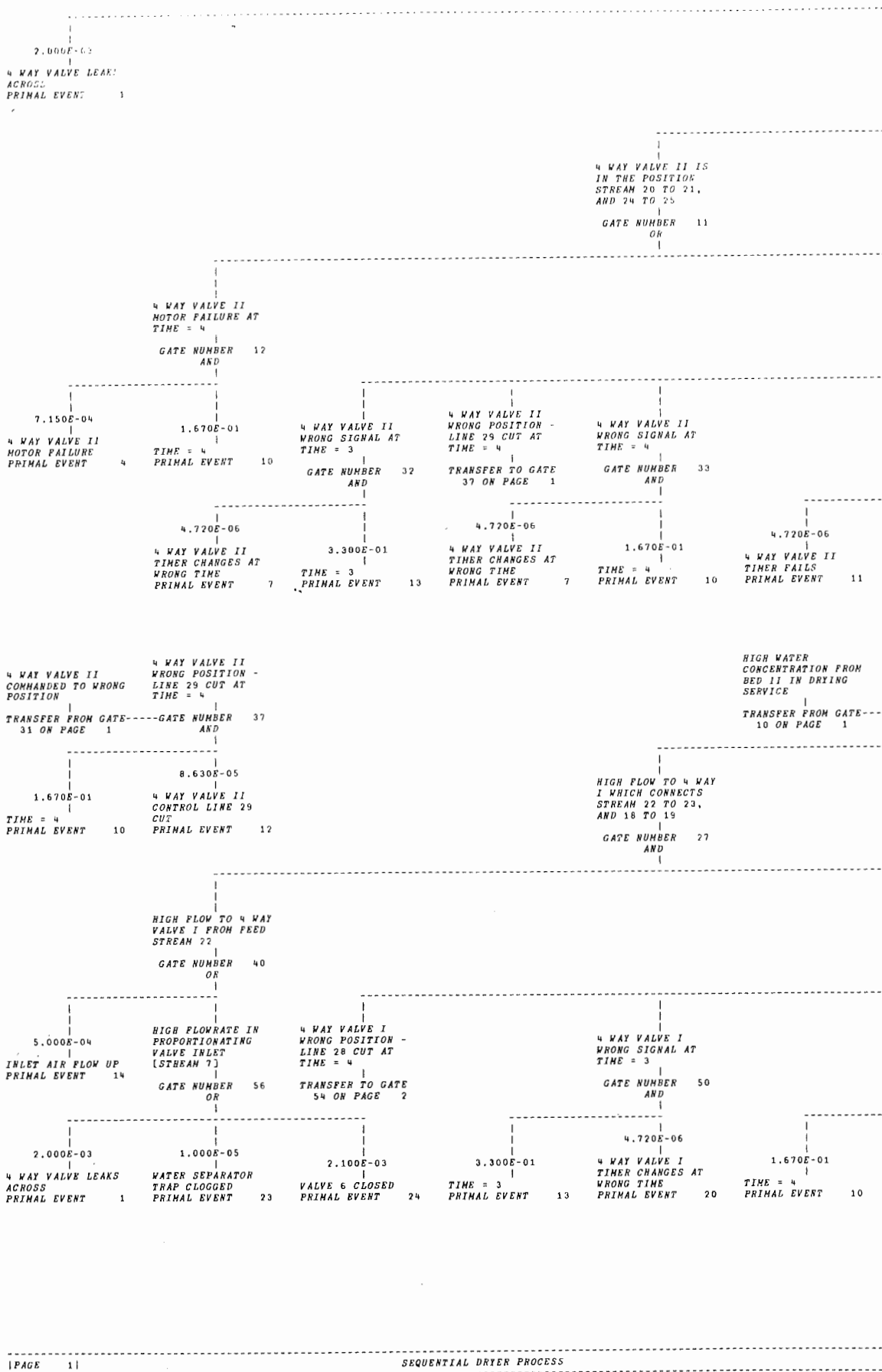


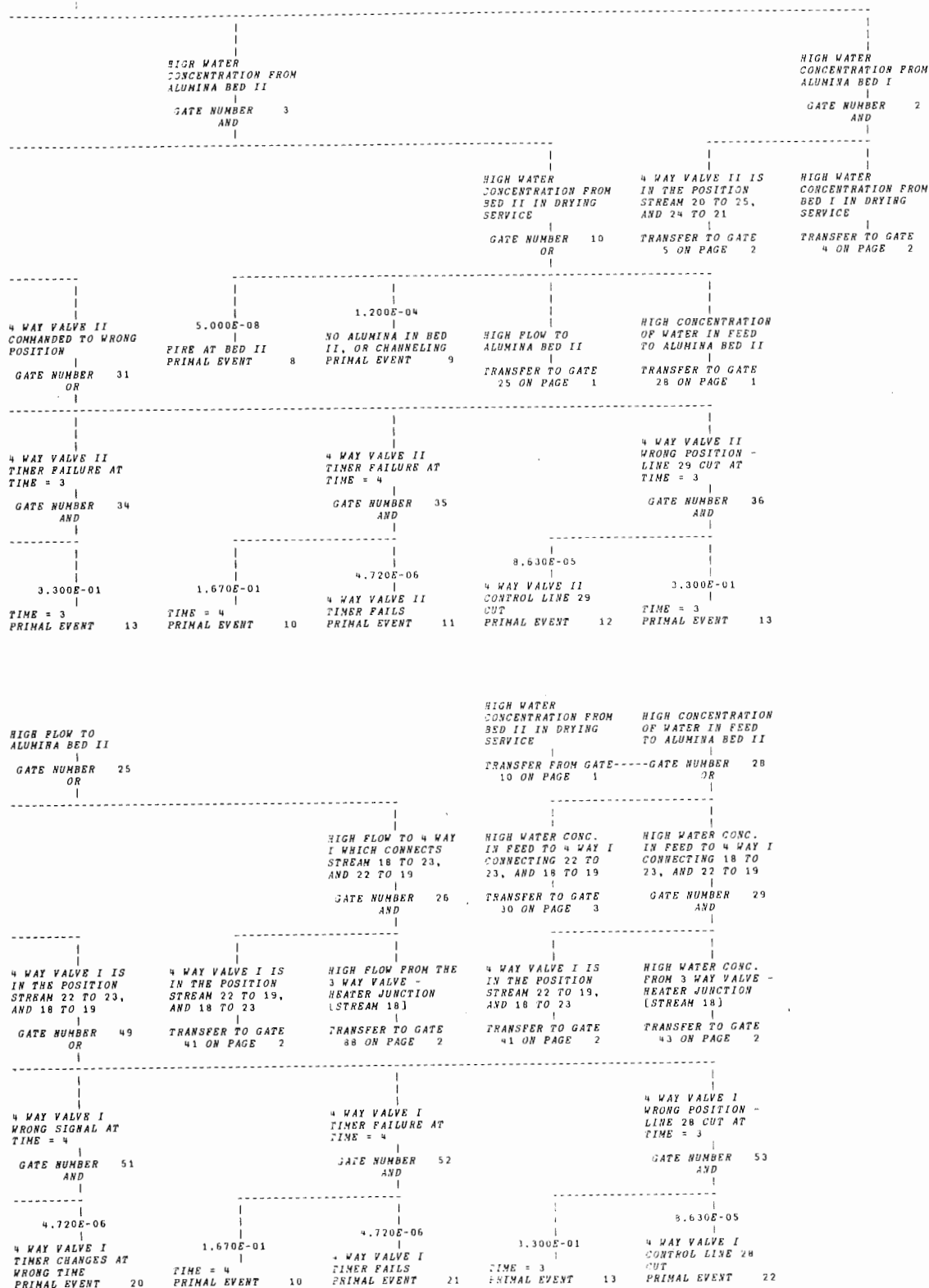
Figure 7. Input-output models for the equipment in the utility air drying process.



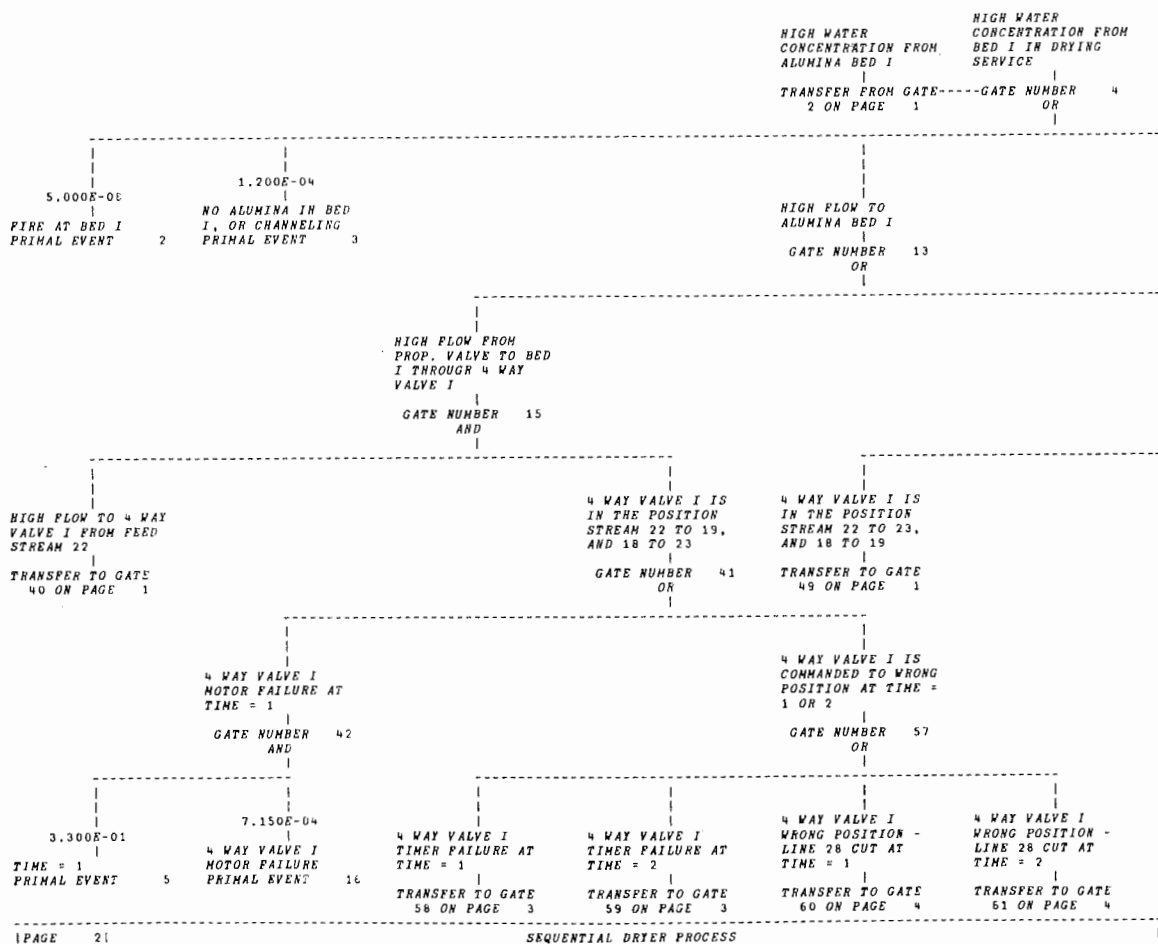
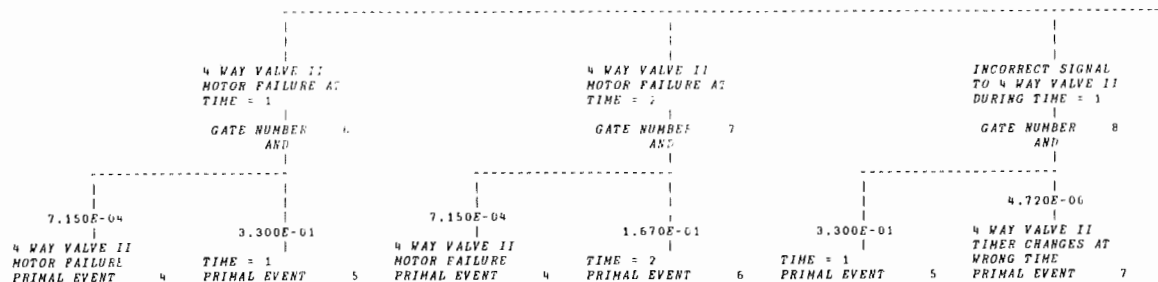


HIGH WATER
CONCENTRATION IN
OUTLET AIR (STREAM
25)

GATE NUMBER 1
OR



HIGH WATER
CONCENTRATION FROM
ALUMINA BED 1
TRANSFER FROM GATE-----
2 ON PAGE 1



1 PAGE 21

SEQUENTIAL DRYER PROCESS

4 WAY VALVE II IS
IN THE POSITION
STREAM 20 TO 25,
AND 24 TO 21

GATE NUMBER 5
OR

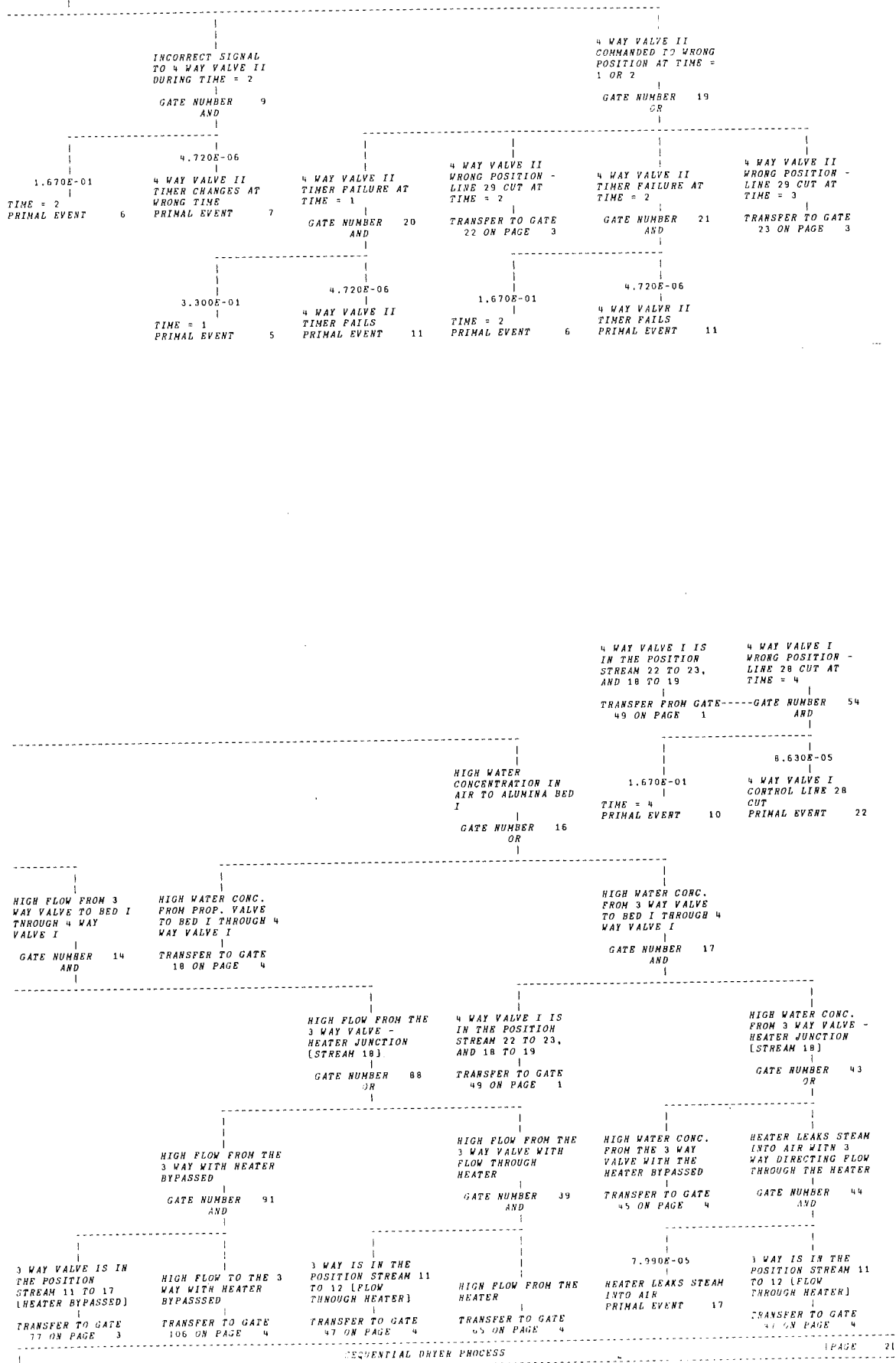


Figure 9 continues

| | | | | |
|--|--|---|--|---|
| 4 WAY VALVE II WRONG POSITION - LINE 29 CUT AT TIME = 3 | 4 WAY VALVE I IS COMMANDED TO WRONG POSITION AT TIME = 1 OR 2 | 4 WAY VALVE I TIMER FAILURE AT TIME = 1 | 4 WAY VALVE I IS COMMANDED TO WRONG POSITION AT TIME = 1 OR 2 | 4 WAY VALVE I TIMER FAILURE AT TIME = 2 |
| -GATE NUMBER 23 AND | TRANSFER FROM GATE-----GATE NUMBER 58 57 ON PAGE 2 | | TRANSFER FROM GATE-----GATE NUMBER 59 57 ON PAGE 2 | |
| 8.630E-05 | | 4.720E-06 | 1.670E-01 | 4.720E-06 |
| 4 WAY VALVE II CONTROL LINE 29 CUT | 3.300E-01 | 4 WAY VALVE I TIMER FAILS | TIME = 2 | 4 WAY VALVE I TIMER FAILS |
| PRIMAL EVENT 12 | TIME = 1 PRIMAL EVENT 5 | PRIMAL EVENT 21 | PRIMAL EVENT 6 | PRIMAL EVENT 21 |

2.100E-03
VALVE 4 CLOSED
PRIMAL EVENT 33

HIGH PRESSURE IN
OUTLET FROM THE 3
WAY VALVE WITH
HEATER BYPASSED
GATE NUMBER 116
AND

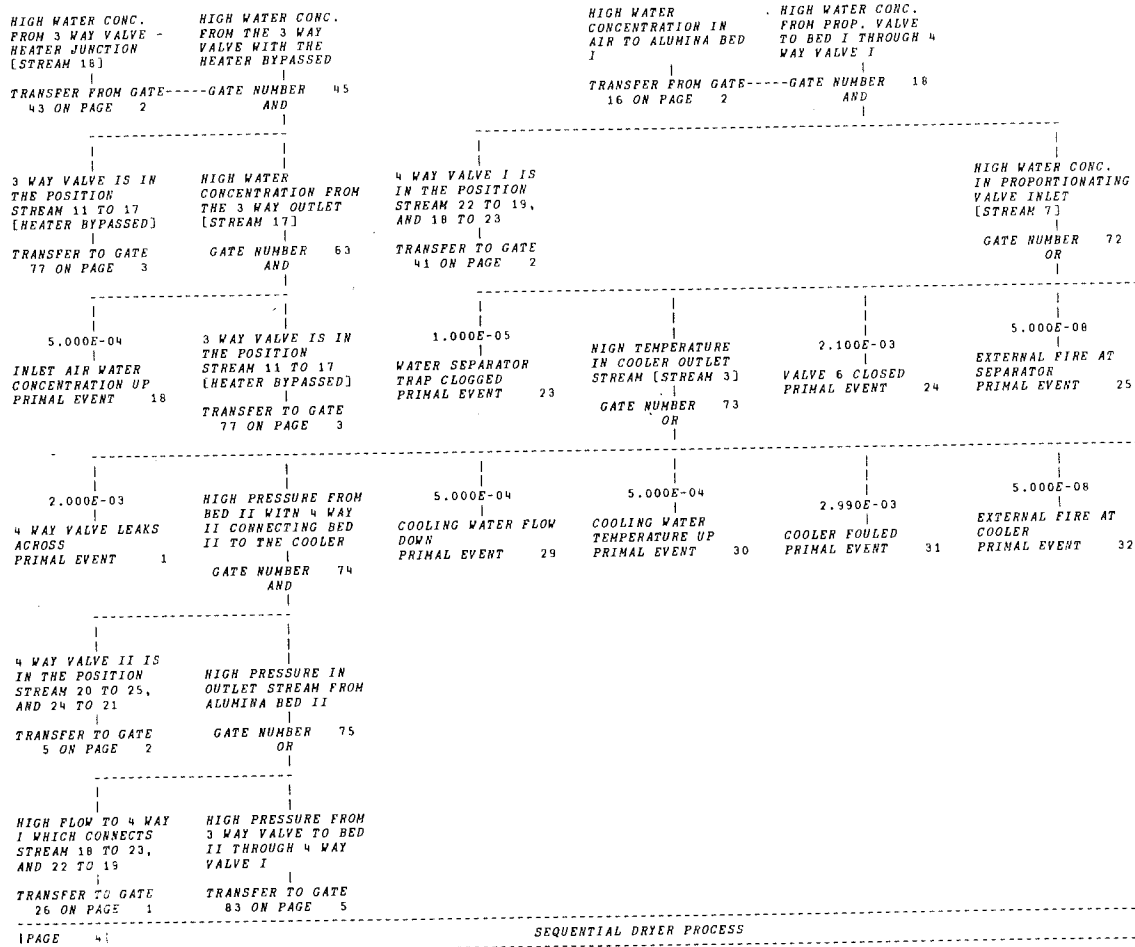
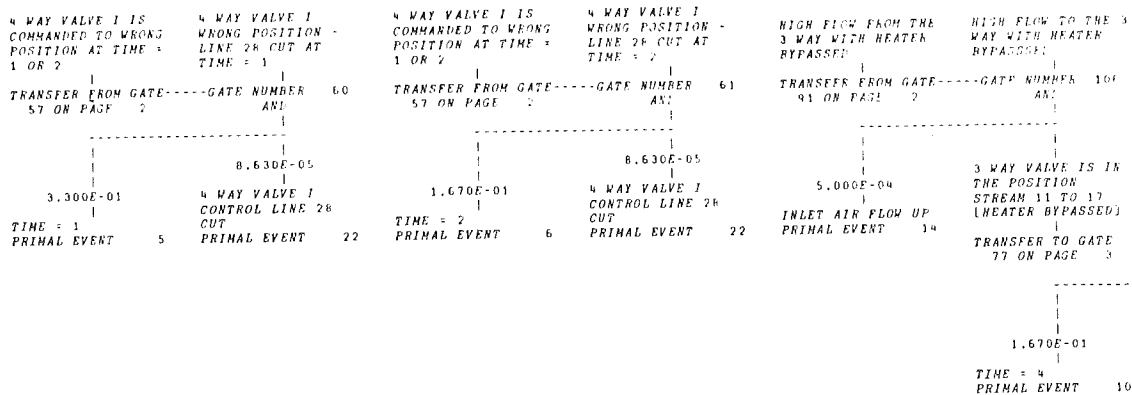
HIGH PRESSURE IN
FEED TO THE 3 WAY
VALVE WITH HEATER
BYPASSED
GATE NUMBER 122
AND

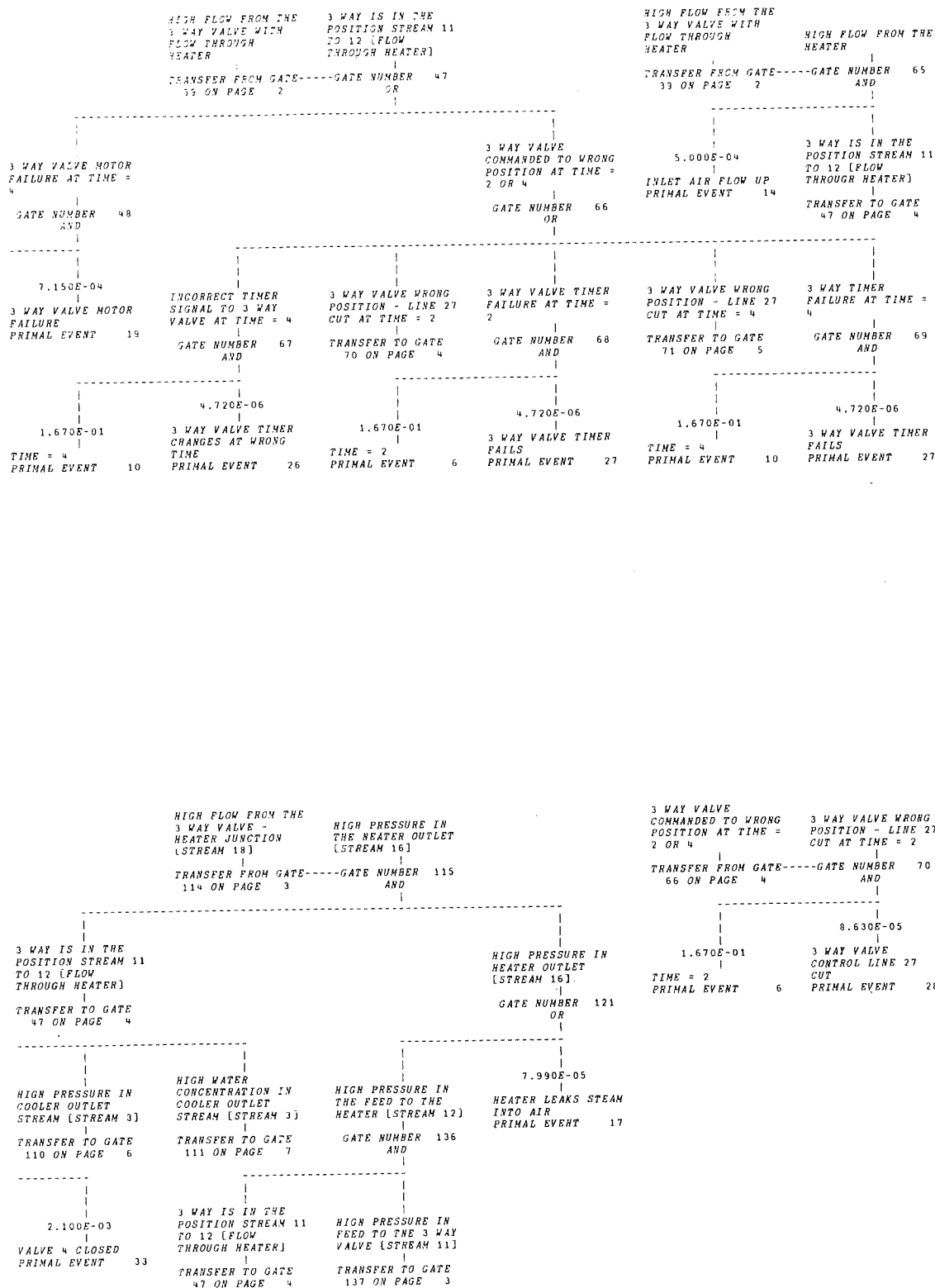
| | | | |
|---|---|---|--|
| 3 WAY VALVE CONTROL LINE (LINE 27) CUT AT TIME = 1 | 3 WAY VALVE CONTROL LINE (LINE 27) CUT AT TIME = 3 | 3 WAY VALVE IS IN THE POSITION STREAM 11 TO 17 (HEATER BYPASSED) | HIGH PRESSURE IN FEED TO THE 3 WAY VALVE (STREAM 11) |
| GATE NUMBER 81 AND | GATE NUMBER 82 AND | TRANSFER TO GATE 77 ON PAGE 3 | GATE NUMBER 137 OR |
| 8.630E-05 | 8.630E-05 | 5.000E-04 | HIGH PRESSURE IN PROPORTIONATING VALVE INLET (STREAM 7) |
| 1.300E-01 | 3.300E-01 | INLET AIR PRESSURE UP | TRANSFER TO GATE 123 ON PAGE 5 |
| TIME = 1 PRIMAL EVENT 5 | TIME = 3 PRIMAL EVENT 13 | PRIMAL EVENT 28 | PRIMAL EVENT 36 |

SEQUENTIAL DRYER PROCESS

1 PAGE 31

Figure 9 continues





POTENTIAL DRYER PROCESS

PAGE 41

Figure 9 continues

HIGH PRESSURE IN
FEED TO 3 WAY
VALVE (STREAM 11)
|
TRANSFER FROM GATE-----GATE NUMBER 173
97 ON PAGE 3

5.000E-03
|
EXTERNAL FIRE AT
SEPARATOR
PRIMAL EVENT 25

HIGH TEMPERATURE
IN THE COOLER
OUTLET (STREAM 3)
|
GATE NUMBER 130
07

2.000E-03
|
4 WAY VALVE LEAKS
ACROSS
PRIMAL EVENT 1

5.000E-04
|
COOLING WATER FLOW
DOWN
PRIMAL EVENT 29

5.000E-04
|
COOLING WATER
TEMPERATURE UP
PRIMAL EVENT 30

2.990E-03
|
COOLER FOULED
PRIMAL EVENT 31

5.000E-06
|
EXTERNAL FIRE AT
COOLER
PRIMAL EVENT 32

2.100E-03
|
VALVE 4 CLOSED
PRIMAL EVENT 33

4 WAY VALVE 11 IS
IN THE POSITION
STREAM 20 TO 21,
AND 24 TO 25
|
TRANSFER TO GATE
11 ON PAGE 1

HIGH WATER CONC.
IN PROPORTIONATING
VALVE INLET
(STREAM 7)
|
TRANSFER FROM GATE-----GATE NUMBER 86
64 ON PAGE 3

HIGH PRESSURE IN
COOLER OUTLET
STREAM (STREAM 3)

5.000E-04
|
COOLING WATER FLOW
DOWN
PRIMAL EVENT 29

5.000E-04
|
COOLING WATER
TEMPERATURE UP
PRIMAL EVENT 30

2.990E-03
|
COOLER FOULED
PRIMAL EVENT 31

5.000E-06
|
EXTERNAL FIRE AT
COOLER
PRIMAL EVENT 32

2.100E-03
|
VALVE 4 CLOSED
PRIMAL EVENT 33

HIGH FLOW FROM BED
I WITH 4 WAY II
CONNECTING BED I
TO THE COOLER
|
TRANSFER TO GATE
92 ON PAGE 5

HIGH PRESSURE IN
FEED TO THE 3 WAY
VALVE WITH HEATER
BYPASSED
|
GATE NUMBER 96
AND

HIGH PRESSURE IN
FEED TO THE 3 WAY
VALVE (STREAM 11)
|
GATE NUMBER 97
08

3 WAY VALVE IS IN
THE POSITION
STREAM 11 TO 17
(HEATER BYPASSED)
|
TRANSFER TO GATE
77 ON PAGE 3

5.000E-04
|
INST AIR PRESSURE
UP
PRIMAL EVENT 36

HIGH PRESSURE IN
PROPORTIONATING
VALVE INLET
(STREAM 7)
|
TRANSFER TO GATE
98 ON PAGE 6

3 WAY IS IN THE
POSITION STREAM 11
TO 12 (FLOW
THROUGH HEATER)
|
TRANSFER TO GATE
47 ON PAGE 4

3 WAY VALVE
COMMANDED TO WRONG
POSITION AT TIME =
2 OR 4

3 WAY VALVE WRONG
POSITION - LINE 27
CUT AT TIME = 4

TRANSFER FROM GATE-----GATE NUMBER 71
66 ON PAGE 4 AND

3.630E-05

HIGH PRESSURE IN
THE COOLER OUTLET
(STREAM 3)

1.670E-01

3 WAY VALVE
CONTROL LINE 27
CUT

TIME = 4

PRIMAL EVENT 10

PRIMAL EVENT 20

GATE NUMBER 139
OR

HIGH FLOW FROM BED
I WITH 4 WAY II
CONNECTING BED I
TO THE COOLER

5.000E-04

COOLING WATER FLOW
DOWN

PRIMAL EVENT 29

GATE NUMBER 92
AND

5.000E-04

COOLING WATER
TEMPERATURE UP

PRIMAL EVENT 30

2.990E-03

COOLER FOULED

PRIMAL EVENT 31

5.000E-08

EXTERNAL FIRE AT
COOLER

PRIMAL EVENT 32

2.100E-03

VALVE 4 CLOSED

PRIMAL EVENT 33

HIGH FLOW FROM 3
WAY VALVE TO BED I
THROUGH 4 WAY
VALVE I

TRANSFER TO GATE
14 ON PAGE 2

HIGH PRESSURE IN
OUTLET STREAM FROM
ALUMINA BED II

TRANSFER FROM GATE-----GATE NUMBER 83
75 ON PAGE 4 AND

HIGH PRESSURE FROM
3 WAY VALVE TO BED
II THROUGH 4 WAY
VALVE I

HIGH PRESSURE FROM
BED I WITH 4 WAY
II CONNECTING BED
I TO THE COOLER

TRANSFER TO GATE
89 ON PAGE 3

HIGH PRESSURE FROM
THE 3 WAY VALVE -
HEATER JUNCTION
(STREAM 18)

GATE NUMBER 84
OR

4 WAY VALVE I IS
IN THE POSITION
STREAM 22 TO 19,
AND 18 TO 23

TRANSFER TO GATE
41 ON PAGE 2

HIGH PRESSURE IN
OUTLET FROM THE 3
WAY VALVE WITH
HEATER BYPASSED

GATE NUMBER 95
AND

HIGH PRESSURE IN
THE HEATER OUTLET
(STREAM 16)

GATE NUMBER 103
AND

3 WAY VALVE IS IN
THE POSITION
STREAM 11 TO 17
(HEATER BYPASSED)

TRANSFER TO GATE
77 ON PAGE 3

HIGH PRESSURE IN
THE HEATER OUTLET
(STREAM 16)

GATE NUMBER 104
OR

3 WAY IS IN THE
POSITION STREAM 11
TO 12 (FLOW
THROUGH HEATER)

TRANSFER TO GATE
47 ON PAGE 4

HIGH PRESSURE IN
THE FEED TO THE
HEATER (STREAM 12)

GATE NUMBER 105
AND

7.990E-05

HEATER LEAKS STEAM
INTO AIR

PRIMAL EVENT 17

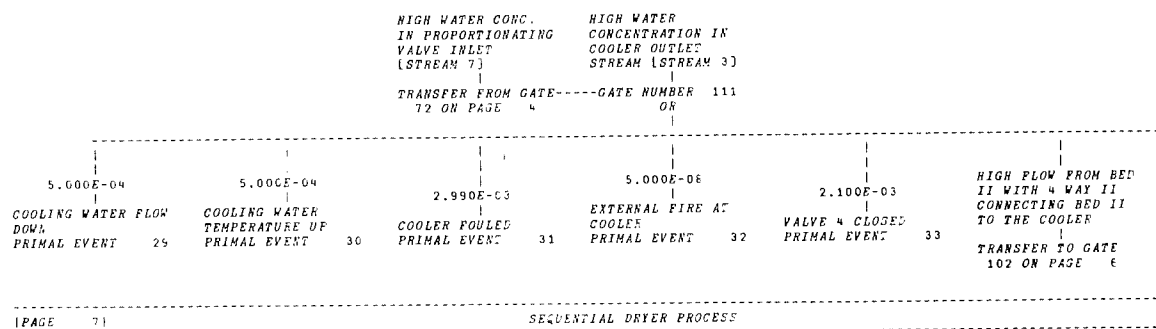
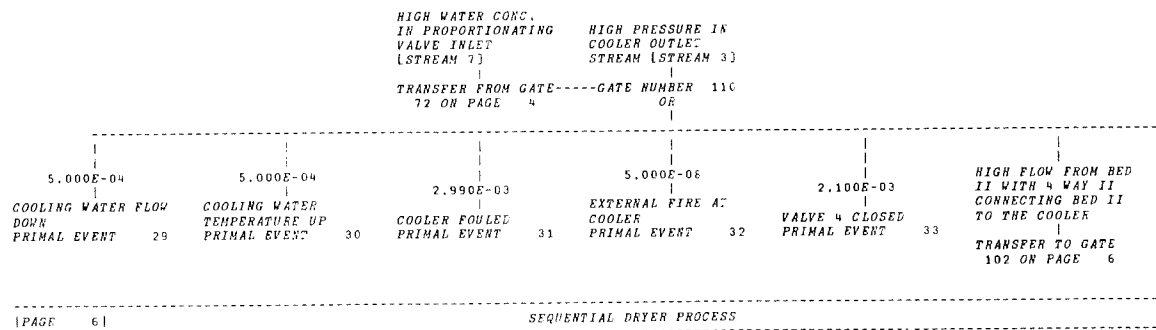
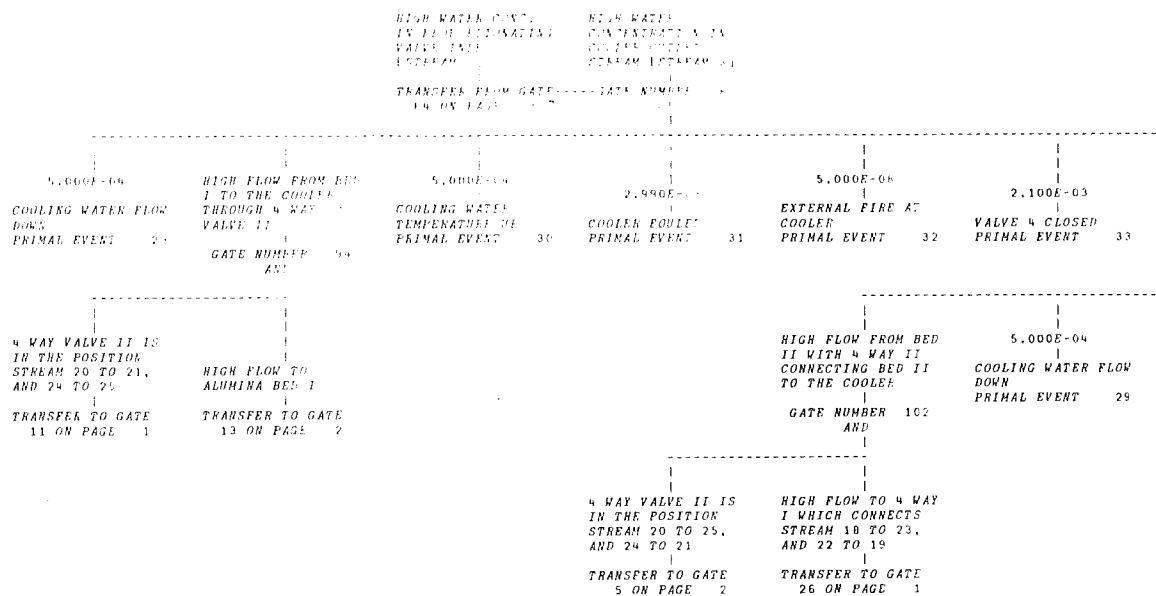
HIGH PRESSURE IN
FEED TO THE 3 WAY
VALVE (STREAM 11)

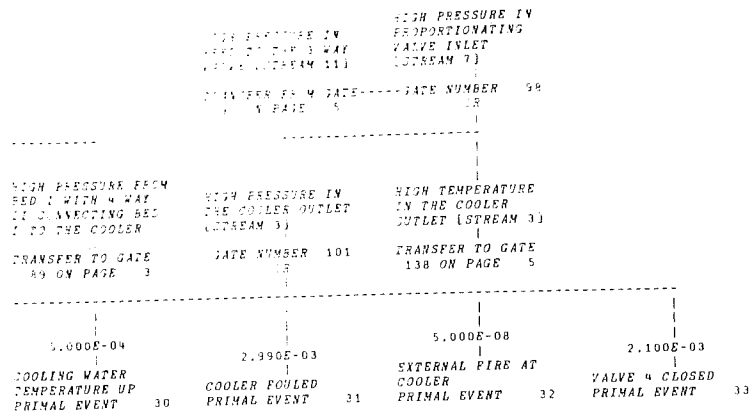
TRANSFER TO GATE
37 ON PAGE 5

INITIAL ORDER PROCESS

(PAGE 51

Figure 9 continues





HIGH PRESSURE FROM
 BED II WITH 4 WAY
 II CONNECTING BED
 II TO THE COOLER
 TRANSFER TO GATE
 74 ON PAGE 4

SEQUENTIAL DRYER PROCESS
 PAGE 61

HIGH PRESSURE FROM
 BED II WITH 4 WAY
 II CONNECTING BED
 II TO THE COOLER
 TRANSFER TO GATE
 74 ON PAGE 4

SEQUENTIAL DRYER PROCESS
 PAGE 71

Figure 9 continues

TITLE:

| GATE NUMBER | GATE TYPE | PROBABILITY | DEVELOP ON P. 13 | TIME |
|----------------|--------------|-------------|--|------|
| 1 | OR | | HIGH WATER CONCENTRATION IN OUTLET AIR (STREAM 25) | |
| 2 | AND | | HIGH WATER CONCENTRATION FROM ALUMINA BED I | |
| 3 | AND | | HIGH WATER CONCENTRATION FROM ALUMINA BED II | |
| 4 | OR | | HIGH WATER CONCENTRATION FROM BED I IN DRYING SERVICE | |
| 5 | OR | | 4 WAY VALVE II IS IN THE POSITION STREAM 20 TO 25, AND 24 TO 21 | |
| 6 | AND | | 4 WAY VALVE II MOTOR FAILURE AT TIME = 1 | |
| 7 | AND | | 4 WAY VALVE II MOTOR FAILURE AT TIME = 2 | |
| 8 | AND | | INCORRECT SIGNAL TO 4 WAY VALVE II DURING TIME = 1 | |
| 9 | AND | | INCORRECT SIGNAL TO 4 WAY VALVE II DURING TIME = 2 | |
| 10 | OR | | HIGH WATER CONCENTRATION FROM BED II IN DRYING SERVICE | |
| 11 | OR | | 4 WAY VALVE II IS IN THE POSITION STREAM 20 TO 21, AND 24 TO 25 | |
| 12 | AND | | 4 WAY VALVE II MOTOR FAILURE AT TIME = 4 | |
| 13 | OR | | HIGH FLOW TO ALUMINA BED I | |
| 14 | AND | | HIGH FLOW FROM 3 WAY VALVE TO BED I THROUGH 4 WAY VALVE I | |
| 15 | AND | | HIGH FLOW FROM PROP. VALVE TO BED I THROUGH 4 WAY VALVE I | |
| 16 | OR | | HIGH WATER CONCENTRATION IN AIR TO ALUMINA BED I | |
| 17 | AND | | HIGH WATER CONC. FROM 3 WAY VALVE TO BED I THROUGH 4 WAY VALVE I | |
| 18 | AND | | HIGH WATER CONC. FROM PROP. VALVE TO BED I THROUGH 4 WAY VALVE I | |
| 19 | OR | | 4 WAY VALVE II COMMANDED TO WRONG POSITION AT TIME = 1 OR 2 | |
| 20 | AND | | 4 WAY VALVE II TIMER FAILURE AT TIME = 1 | |
| 21 | AND | | 4 WAY VALVE II TIMER FAILURE AT TIME = 2 | |
| 22 | AND | | 4 WAY VALVE II WRONG POSITION - LINE 29 CUT AT TIME = 2 | |
| 23 | AND | | 4 WAY VALVE II WRONG POSITION - LINE 29 CUT AT TIME = 3 | |
| 24 | OR | | HIGH FLOW TO ALUMINA BED II | |
| 25 | AND | | HIGH FLOW TO 4 WAY I WHICH CONNECTS STREAM 18 TO 23, AND 22 TO 19 | |
| 26 | AND | | HIGH FLOW TO 4 WAY I WHICH CONNECTS STREAM 22 TO 23, AND 18 TO 19 | |
| 27 | OR | | HIGH CONCENTRATION OF WATER IN FEED TO ALUMINA BED II | |
| 28 | AND | | HIGH WATER CONC. IN FEED TO 4 WAY I CONNECTING 18 TO 23, AND 22 TO 19 | |
| 29 | AND | | HIGH WATER CONC. IN FEED TO 4 WAY I CONNECTING 22 TO 23, AND 18 TO 19 | |
| 30 | OR | | 4 WAY VALVE II COMMANDED TO WRONG POSITION | |
| 31 | AND | | 4 WAY VALVE II WRONG SIGNAL AT TIME = 3 | |
| 32 | AND | | 4 WAY VALVE II WRONG SIGNAL AT TIME = 4 | |
| 33 | AND | | 4 WAY VALVE II TIMER FAILURE AT TIME = 3 | |
| 34 | AND | | 4 WAY VALVE II TIMER FAILURE AT TIME = 4 | |
| 35 | AND | | 4 WAY VALVE II WRONG POSITION - LINE 29 CUT AT TIME = 3 | |
| 36 | AND | | 4 WAY VALVE II WRONG POSITION - LINE 29 CUT AT TIME = 4 | |
| 37 | AND | | HIGH FLOW FROM THE 3 WAY VALVE WITH FLOW THROUGH HEATER | |
| 38 | OR | | HIGH FLOW TO 4 WAY VALVE I FROM FEED STREAM 22 | |
| 39 | OR | | 4 WAY VALVE I IS IN THE POSITION STREAM 22 TO 19, AND 18 TO 23 | |
| 40 | AND | | 4 WAY VALVE I MOTOR FAILURE AT TIME = 1 | |
| 41 | OR | | HIGH WATER CONC. FROM 3 WAY VALVE - HEATER JUNCTION [STREAM 18] | |
| 42 | AND | | HEATER LEAKS STEAM INTO AIR WITH 3 WAY DIRECTING FLOW THROUGH THE HEATER | |
| 43 | AND | | HIGH WATER CONC. FROM THE 3 WAY VALVE WITH THE HEATER BYPASSED | |
| 44 | OR | | HIGH WATER CONC. FROM PROP. VALVE TO BED II THROUGH 4 WAY VALVE I | |
| 45 | OR | | 3 WAY IS IN THE POSITION STREAM 11 TO 12 (FLOW THROUGH HEATER) | |
| 46 | AND | | 3 WAY VALVE MOTOR FAILURE AT TIME = 4 | |
| 47 | OR | | 4 WAY VALVE I IS IN THE POSITION STREAM 22 TO 23, AND 18 TO 19 | |
| 48 | AND | | 4 WAY VALVE I WRONG SIGNAL AT TIME = 3 | |
| 49 | AND | | 4 WAY VALVE I WRONG SIGNAL AT TIME = 4 | |
| 50 | AND | | 4 WAY VALVE I TIMER FAILURE AT TIME = 4 | |
| 51 | AND | | 4 WAY VALVE I WRONG POSITION - LINE 28 CUT AT TIME = 3 | |
| 52 | AND | | 4 WAY VALVE I WRONG POSITION - LINE 28 CUT AT TIME = 4 | |
| 53 | OR | | HIGH FLOWRATE IN PROPORTIONATING VALVE INLET [STREAM 7] | |
| 54 | OR | | 4 WAY VALVE I IS COMMANDED TO WRONG POSITION AT TIME = 1 OR 2 | |
| 55 | AND | | 4 WAY VALVE I TIMER FAILURE AT TIME = 1 | |
| 56 | AND | | 4 WAY VALVE I TIMER FAILURE AT TIME = 2 | |
| 57 | AND | | 4 WAY VALVE I WRONG POSITION - LINE 28 CUT AT TIME = 1 | |
| 58 | AND | | 4 WAY VALVE I WRONG POSITION - LINE 28 CUT AT TIME = 2 | |
| 59 | AND | | HIGH WATER CONCENTRATION FROM THE 3 WAY OUTLET [STREAM 17] | |
| 60 | OR | | HIGH WATER CONC. IN PROPORTIONATING VALVE INLET [STREAM 7] | |
| 61 | AND | | HIGH FLOW FROM THE HEATER | |

GATE TABLE OF CONTENTS

SEQUENTIAL DRYER PROCESS

TITLE:

| GATE NUMBER | GATE TYPE | PROBABILITY | DEVELOPED ON PAGE | TEXT |
|----------------|--------------|-------------|----------------------|---|
| 66 | OR | | 4 | 3 WAY VALVE COMMANDED TO WRONG POSITION AT TIME = 2 OR 4 |
| 67 | AND | | 4 | INCORRECT TIMER SIGNAL TO 3 WAY VALVE AT TIME = 4 |
| 68 | AND | | 4 | 3 WAY VALVE TIMER FAILURE AT TIME = 2 |
| 69 | AND | | 4 | 3 WAY TIMER FAILURE AT TIME = 4 |
| 70 | AND | | 4 | 3 WAY VALVE WRONG POSITION - LINE 27 CUT AT TIME = 2 |
| 71 | AND | | 5 | 3 WAY VALVE WRONG POSITION - LINE 27 CUT AT TIME = 4 |
| 72 | OR | | 4 | HIGH WATER CONC. IN PROPORTIONATING VALVE INLET (STREAM 7) |
| 73 | OR | | 4 | HIGH TEMPERATURE IN COOLER OUTLET STREAM (STREAM 3) |
| 74 | AND | | 4 | HIGH PRESSURE FROM BED II WITH 4 WAY II CONNECTING BED II TO THE COOLER |
| 75 | OR | | 4 | HIGH PRESSURE IN OUTLET STREAM FROM ALUMINA BED II |
| 77 | OR | | 3 | 3 WAY VALVE IS IN THE POSITION STREAM 11 TO 17 (HEATER BYPASSED) |
| 78 | AND | | 3 | INCORRECT TIMER SIGNAL TO THE 3 WAY VALVE AT TIME = 3 |
| 79 | AND | | 3 | 3 WAY VALVE TIMER FAILURE AT TIME = 1 |
| 80 | AND | | 3 | 3 WAY VALVE TIMER FAILURE AT TIME = 3 |
| 81 | AND | | 3 | 3 WAY VALVE CONTROL LINE (LINE 27) CUT AT TIME = 1 |
| 82 | AND | | 3 | 3 WAY VALVE CONTROL LINE (LINE 27) CUT AT TIME = 3 |
| 83 | AND | | 5 | HIGH PRESSURE FROM 3 WAY VALVE TO BED II THROUGH 4 WAY VALVE I |
| 84 | OR | | 5 | HIGH PRESSURE FROM THE 3 WAY VALVE - HEATER JUNCTION (STREAM 18) |
| 85 | OR | | 3 | HIGH TEMPERATURE IN COOLER OUTLET STREAM (STREAM 3) |
| 86 | OR | | 5 | HIGH PRESSURE IN COOLER OUTLET STREAM (STREAM 3) |
| 87 | OR | | 6 | HIGH WATER CONCENTRATION IN COOLER OUTLET STREAM (STREAM 3) |
| 88 | OR | | 2 | HIGH FLOW FROM THE 3 WAY VALVE - HEATER JUNCTION (STREAM 18) |
| 89 | AND | | 3 | HIGH PRESSURE FROM BED I WITH 4 WAY II CONNECTING BED I TO THE COOLER |
| 91 | AND | | 2 | HIGH FLOW FROM THE 3 WAY WITH HEATER BYPASSED |
| 92 | AND | | 5 | HIGH FLOW FROM BED I WITH 4 WAY II CONNECTING BED I TO THE COOLER |
| 94 | AND | | 6 | HIGH FLOW FROM BED I TO THE COOLER THROUGH 4 WAY VALVE II |
| 95 | AND | | 5 | HIGH PRESSURE IN OUTLET FROM THE 3 WAY VALVE WITH HEATER BYPASSED |
| 96 | AND | | 5 | HIGH PRESSURE IN FEED TO THE 3 WAY VALVE WITH HEATER BYPASSED |
| 97 | OR | | 5 | HIGH PRESSURE IN FEED TO THE 3 WAY VALVE (STREAM 11) |
| 98 | OR | | 6 | HIGH PRESSURE IN PROPORTIONATING VALVE INLET (STREAM 7) |
| 99 | OR | | 3 | HIGH PRESSURE IN OUTLET STREAM FROM ALUMINA BED I |
| 101 | OR | | 6 | HIGH PRESSURE IN THE COOLER OUTLET (STREAM 3) |
| 102 | AND | | 6 | HIGH FLOW FROM BED II WITH 4 WAY II CONNECTING BED II TO THE COOLER |
| 103 | AND | | 5 | HIGH PRESSURE IN THE HEATER OUTLET (STREAM 16) |
| 104 | OR | | 5 | HIGH PRESSURE IN THE HEATER OUTLET (STREAM 16) |
| 105 | AND | | 5 | HIGH PRESSURE IN THE FEED TO THE HEATER (STREAM 12) |
| 106 | AND | | 4 | HIGH FLOW TO THE 3 WAY WITH HEATER BYPASSED |
| 107 | AND | | 3 | HIGH PRESSURE FROM 3 WAY VALVE TO BED I THROUGH 4 WAY VALVE I |
| 110 | OR | | 6 | HIGH PRESSURE IN COOLER OUTLET STREAM (STREAM 3) |
| 111 | OR | | 7 | HIGH WATER CONCENTRATION IN COOLER OUTLET STREAM (STREAM 3) |
| 114 | OR | | 3 | HIGH FLOW FROM THE 3 WAY VALVE - HEATER JUNCTION (STREAM 18) |
| 115 | AND | | 4 | HIGH PRESSURE IN THE HEATER OUTLET (STREAM 16) |
| 116 | AND | | 3 | HIGH PRESSURE IN OUTLET FROM THE 3 WAY VALVE WITH HEATER BYPASSED |
| 121 | OR | | 4 | HIGH PRESSURE IN HEATER OUTLET (STREAM 16) |
| 122 | AND | | 3 | HIGH PRESSURE IN FEED TO THE 3 WAY VALVE WITH HEATER BYPASSED |
| 123 | OR | | 5 | HIGH PRESSURE IN PROPORTIONATING VALVE INLET (STREAM 7) |
| 136 | AND | | 4 | HIGH PRESSURE IN THE FEED TO THE HEATER (STREAM 12) |
| 137 | OR | | 3 | HIGH PRESSURE IN FEED TO THE 3 WAY VALVE (STREAM 11) |
| 138 | OR | | 5 | HIGH TEMPERATURE IN THE COOLER OUTLET (STREAM 3) |
| 139 | OR | | 5 | HIGH PRESSURE IN THE COOLER OUTLET (STREAM 3) |

Figure 9 continues

| EVENT NUMBER | PROBABILITY | DEVELOPMENT OR PATH | TEST |
|--------------|-------------|---------------------|--|
| 1 | 7.000E-01 | 1 | 4 WAY VALVE LEAKS |
| 2 | 5.000E-01 | 2 | FIRE AT BED I |
| 3 | 1.700E-04 | 2 | NO ALUMINA IN BED I, OR CHANNELING |
| 4 | 7.150E-04 | 1 | 4 WAY VALVE II MOTOR FAILURE |
| 5 | 3.300E-01 | 1 | TIME = 1 |
| 6 | 1.670E-01 | 1 | TIME = 2 |
| 7 | 4.720E-06 | 1 | 4 WAY VALVE II TIMER CHANGES AT WRONG TIME |
| 8 | 5.000E-06 | 1 | FIRE AT BED II |
| 9 | 1.700E-04 | 1 | NO ALUMINA IN BED II, OR CHANNELING |
| 10 | 1.670E-01 | 1 | TIME = 4 |
| 11 | 4.720E-06 | 1 | 4 WAY VALVE II TIMER FAILS |
| 12 | 8.630E-05 | 1 | 4 WAY VALVE II CONTROL LINE 29 CUT |
| 13 | 3.300E-01 | 1 | TIME = 3 |
| 14 | 5.000E-04 | 1 | INLET AIR FLOW UP |
| 16 | 7.150E-04 | 2 | 4 WAY VALVE I MOTOR FAILURE |
| 17 | 7.990E-05 | 2 | HEATER LEAKS STEAM INTO AIR |
| 18 | 5.000E-04 | 3 | INLET AIR WATER CONCENTRATION UP |
| 19 | 7.150E-04 | 4 | 3 WAY VALVE MOTOR FAILURE |
| 20 | 4.720E-06 | 1 | 4 WAY VALVE I TIMER CHANGES AT WRONG TIME |
| 21 | 4.720E-06 | 1 | 4 WAY VALVE I TIMER FAILS |
| 22 | 8.630E-05 | 1 | 4 WAY VALVE I CONTROL LINE 28 CUT |
| 23 | 1.000E-05 | 1 | WATER SEPARATOR TRAP CLOGGED |
| 24 | 2.100E-03 | 1 | VALVE 6 CLOSED |
| 25 | 5.000E-08 | 3 | EXTERNAL FIRE AT SEPARATOR |
| 26 | 4.720E-06 | 3 | 3 WAY VALVE TIMER CHANGES AT WRONG TIME |
| 27 | 4.720E-06 | 3 | 3 WAY VALVE TIMER FAILS |
| 28 | 8.630E-05 | 3 | 3 WAY VALVE CONTROL LINE 27 CUT |
| 29 | 5.000E-04 | 3 | COOLING WATER FLOW DOWNS |
| 30 | 5.000E-04 | 3 | COOLING WATER TEMPERATURE UP |
| 31 | 2.990E-03 | 3 | COOLER FOULED |
| 32 | 5.000E-08 | 3 | EXTERNAL FIRE AT COOLER |
| 33 | 2.100E-03 | 3 | VALVE 4 CLOSED |
| 36 | 5.000E-04 | 3 | INLET AIR PRESSURE UP |

Figure 9. The fault tree for the event water concentration too high from the utility air dryer process.

the structure of the digraph. It is not necessary for the analyst to preordain the logic (AND, OR, etc.) of the interactions between variables.

With this type of model all foreseeable interactions may be described. What remains is to interconnect the digraph model for each piece of equipment in the system to obtain a model for the complete system. Figure 4 shows a partial digraph for the heat exchanger system shown in Figure 1. From the digraph model, fault trees may be directly deduced. The algorithm for this deduction has been described previously (Lapp, 1977). Briefly, the procedure involves starting at the node in the digraph which denotes the top event. The negative feed-forward and feedback loops through a node determine how it should be logically related to its inputs. The algorithm has over 30 different logical expansions of a node. The input nodes are logically expanded in a similar manner until the complete fault tree is obtained. The consistency of intermediate events and variables is maintained during the generation of the fault tree.

After generation of the fault tree, the tree is listed, "drawn" on a line printer, and put in minimal cut-set form. The minimal cut-sets of a Boolean equation are the sets of events which are sufficient to cause the top event and do not contain any other sufficient sets of events. The fault tree for the event temperature in stream 4 (T4) too high is given in Figure 5.

The following example illustrates the application of this strategy to a sequential process for drying air.

Example: Fixed Bed Alumina Air Dryers. Figure 6 illustrates a process for drying air. Ambient air which contains water vapor enters in stream 9. The air passes through a bed of alumina (Bed I) where the water vapor is adsorbed. The dried air passes out of the process in stream 25. This process has been used by Professor C. J. King of the Department of Chemical Engineering, University of California, Berkeley, Calif., as a case study in process design.

In order to maintain a continuous supply of dry air, two beds of alumina are employed. When one bed is removing water from the inlet air, the other bed is being regenerated. Regeneration involves passing hot air through a bed which has been loaded to capacity with water. The hot air strips the water from the alumina. The hot air leaving the regenerating bed is passed through a condenser where water is removed. The air is reheated and passed through the operating dryer. The regenerated bed is then cooled with inlet air and switched back into service. The same procedure is followed for the other bed. Table I gives the sequence of operations for a complete cycle.

If the outlet air from the process contains too much water a number of pieces of valuable equipment downstream may be destroyed. What could cause the water concentration in stream 25 to be too high? One way to answer this question is to construct a fault tree for the event concentration of water too high in stream 25 (C (+1) Stream 25).

Input-output models for several of the pieces of equipment

Table III. Minimal Cut Sets

PROBLEM ID: SEQUENTIAL DRYER PROCESS

102 MINIMAL CUT SETS GENERATED.

TOP EVENT PROBABILITY= 2.0001E-03

MINIMAL CUT SET NO. 1 ITS PROBABILITY: 2.00E-03
 EVENT 1(2.00E-03) 4 WAY VALVE LEAKS ACROSS

MINIMAL CUT SET NO. 3 ITS PROBABILITY: 1.43E-08
 EVENT 3(1.20E-04) NO ALUMINA IN BED I, OR CHANNELING
 EVENT 4(7.15E-04) 4 WAY VALVE II MOTOR FAILURE
 EVENT 6(1.67E-01) TIME = 2

MINIMAL CUT SET NO. 5 ITS PROBABILITY: 3.42E-09
 EVENT 3(1.20E-04) NO ALUMINA IN BED I, OR CHANNELING
 EVENT 5(3.30E-01) TIME = 1
 EVENT 12(8.63E-05) 4 WAY VALVE II CONTROL LINE 29 CUT

MINIMAL CUT SET NO. 7 ITS PROBABILITY: 1.73E-09
 EVENT 9(1.20E-04) NO ALUMINA IN BED II, OR CHANNELING
 EVENT 10(1.67E-01) TIME = 4
 EVENT 12(8.63E-05) 4 WAY VALVE II CONTROL LINE 29 CUT

MINIMAL CUT SET NO. 9 ITS PROBABILITY: 5.04E-10
 EVENT 4(7.15E-04) 4 WAY VALVE II MOTOR FAILURE
 EVENT 5(3.30E-01) TIME = 1
 EVENT 16(7.15E-04) 4 WAY VALVE I MOTOR FAILURE
 EVENT 31(2.99E-03) COOLER FOULED

MINIMAL CUT SET NO. 11 ITS PROBABILITY: 3.54E-10
 EVENT 4(7.15E-04) 4 WAY VALVE II MOTOR FAILURE
 EVENT 5(3.30E-01) TIME = 1
 EVENT 16(7.15E-04) 4 WAY VALVE I MOTOR FAILURE
 EVENT 33(2.10E-03) VALVE 4 CLOSED

MINIMAL CUT SET NO. 13 ITS PROBABILITY: 1.87E-10
 EVENT 3(1.20E-04) NO ALUMINA IN BED I, OR CHANNELING
 EVENT 5(3.30E-01) TIME = 1
 EVENT 7(4.72E-06) 4WAY VALVE II TIMER CHANGES AT WRONG TIME

MINIMAL CUT SET NO. 15 ITS PROBABILITY: 1.87E-10
 EVENT 7(4.72E-06) 4WAY VALVE II TIMER CHANGES AT WRONG TIME
 EVENT 9(1.20E-04) NO ALUMINA IN BED II, OR CHANNELING
 EVENT 13(3.30E-01) TIME = 3

MINIMAL CUT SET NO. 17 ITS PROBABILITY: 9.46E-11
 EVENT 9(1.20E-04) NO ALUMINA IN BED II, OR CHANNELING
 EVENT 10(1.67E-01) TIME = 4
 EVENT 11(4.72E-06) 4 WAY VALVE II TIMER FAILS

MINIMAL CUT SET NO. 19 ITS PROBABILITY: 9.46E-11
 EVENT 3(1.20E-04) NO ALUMINA IN BED I, OR CHANNELING
 EVENT 6(1.67E-01) TIME = 2
 EVENT 7(4.72E-06) 4WAY VALVE II TIMER CHANGES AT WRONG TIME

MINIMAL CUT SET NO. 2 ITS PROBABILITY: 2.83E-08
 EVENT 3(1.20E-04) NO ALUMINA IN BED I, OR CHANNELING
 EVENT 4(7.15E-04) 4 WAY VALVE II MOTOR FAILURE
 EVENT 5(3.30E-01) TIME = 1

MINIMAL CUT SET NO. 4 ITS PROBABILITY: 1.43E-08
 EVENT 4(7.15E-04) 4 WAY VALVE II MOTOR FAILURE
 EVENT 9(1.20E-04) NO ALUMINA IN BED II, OR CHANNELING
 EVENT 10(1.67E-01) TIME = 4

MINIMAL CUT SET NO. 6 ITS PROBABILITY: 3.42E-09
 EVENT 9(1.20E-04) NO ALUMINA IN BED II, OR CHANNELING
 EVENT 12(8.63E-05) 4 WAY VALVE II CONTROL LINE 29 CUT
 EVENT 13(3.30E-01) TIME = 3

MINIMAL CUT SET NO. 8 ITS PROBABILITY: 1.73E-09
 EVENT 3(1.20E-04) NO ALUMINA IN BED I, OR CHANNELING
 EVENT 6(1.67E-01) TIME = 2
 EVENT 12(8.63E-05) 4 WAY VALVE II CONTROL LINE 29 CUT

MINIMAL CUT SET NO. 10 ITS PROBABILITY: 3.54E-10
 EVENT 4(7.15E-04) 4 WAY VALVE II MOTOR FAILURE
 EVENT 5(3.30E-01) TIME = 1
 EVENT 16(7.15E-04) 4 WAY VALVE I MOTOR FAILURE
 EVENT 24(2.10E-03) VALVE 6 CLOSED

MINIMAL CUT SET NO. 12 ITS PROBABILITY: 1.87E-10
 EVENT 3(1.20E-04) NO ALUMINA IN BED I, OR CHANNELING
 EVENT 5(3.30E-01) TIME = 1
 EVENT 11(4.72E-06) 4 WAY VALVE II TIMER FAILS

MINIMAL CUT SET NO. 14 ITS PROBABILITY: 1.87E-10
 EVENT 9(1.20E-04) NO ALUMINA IN BED II, OR CHANNELING
 EVENT 11(4.72E-06) 4 WAY VALVE II TIMER FAILS
 EVENT 13(3.30E-01) TIME = 3

MINIMAL CUT SET NO. 16 ITS PROBABILITY: 9.46E-11
 EVENT 7(4.72E-06) 4WAY VALVE II TIMER CHANGES AT WRONG TIME
 EVENT 9(1.20E-04) NO ALUMINA IN BED II, OR CHANNELING
 EVENT 10(1.67E-01) TIME = 4

MINIMAL CUT SET NO. 18 ITS PROBABILITY: 9.46E-11
 EVENT 3(1.20E-04) NO ALUMINA IN BED I, OR CHANNELING
 EVENT 6(1.67E-01) TIME = 2
 EVENT 11(4.72E-06) 4 WAY VALVE II TIMER FAILS

MINIMAL CUT SET NO. 20 ITS PROBABILITY: 8.44E-11
 EVENT 4(7.15E-04) 4 WAY VALVE II MOTOR FAILURE
 EVENT 5(3.30E-01) TIME = 1
 EVENT 16(7.15E-04) 4 WAY VALVE I MOTOR FAILURE
 EVENT 30(5.00E-04) COOLING WATER TEMPERATURE UP

in the system are given in Figure 7. Note the time dependent nature of the three-way valve, four-way valves, and the timer. The input-output models were interconnected to give a digraph model for the dryer system. The complete digraph for this system contained 67 nodes and 439 edges. A reduced version of the digraph is shown in Figure 8. Only the main concentration and flow interactions are shown.

The fault tree generation algorithm required 30 s of IBM 360/67 time to generate the fault tree for this system. The tree contains 143 gates and is shown in Figure 9. This tree is different from the usual fault tree in that common events such as time periods are considered.

Probability data were gathered and estimated for the events included in the tree. Table II presents the data. Over 100 cut-sets were computed for the tree. The first twenty are presented in Table III.

An analysis of the cut-sets for this system indicates the importance of leaking of the four-way valve. The results of this fault tree analysis in conjunction with economic considerations of the dryer operation and other possible design or maintenance corrections can be used to decide an appropriate action.

Conclusions

With digraph models that contain edges that depend on other variables and events, it is possible to include common sequential behavior in a system digraph. This allows the generation of a fault tree that contains events (like the sequence of valve operations) that are normally true. The analysis of the minimal cut-sets that result from this fault tree allows the analyst to focus attention on the important parts of the system.

Literature Cited

- Esary, J. D., Ziehms, H., "Reliability Analysis of Phased Missions," SIAM, "Reliability and Fault Tree Analysis," 1975.
 Fussell, J. B., Barlow, R. E., Ed., SIAM, "Reliability and Fault Tree Analysis," 1975.
 Fussell, J. B., Powers, G. J., Bennetts, R. B., *IEEE Trans. Reliab.*, **R-23**, 1 (Apr 1974).
 Lapp, S. A., Powers, G. J., *IEEE Trans. Reliab.*, (Apr 1977).
 Powers, G. J., Tompkins, F. C., *AIChE J.*, **20**, 91 (1974).

Received for review September 20, 1976

Accepted April 29, 1977