NUREG/CR-1965
SAND81-7068
RS

THE USE OF THE COMPUTER CODE IMPORTANCE WITH SETS INPUT

by:

H. E. Lambert
B. J. Davis

Submitted by
TERA Advanced Services Corporation
Berkeley, California
Under Contract No. 49-5945
to
Sandia National Laboratories
Albuquerque, New Mexico 87185

Work Sponsored by
Division of Safeguards, Fuel Cycle and Environmental Research
Office of Nuclear Regulatory Research
U. S. Nuclear Regulatory Commission
Washington, DC 20555

Under Memorandum of Understanding DOE 40-550-75
NRC FIN No. A1060

Submitted: September 1980
Printed: March 1981

ABSTRACT

This report is a user's manual for the fault tree computer code IMPORTANCE. These codes accept as input (1) the min cut sets generated from the computer code SETS and (2) the basic event data, failure rates and fault duration times. IMPORTANCE computes and produces as output the following Top Event Characteristics:

- System unavailability
- Expected number of system failures
- Top Event rate (rate of system failure)
- Mean time to occurrence of the Top Event
- Mean Duration time of the Top Event

In addition, IMPORTANCE computes various measures of deterministic and probabilistic importance (i.e., sensitivity) for basic events and min cut sets. These measures can aid an analyst in determining weaknesses in a system and suggest the optimal course of system upgrade for improvement of system safety or reliability. Simple examples as well as an actual analysis conducted in industry are used to interpret the meaning and demonstrate the possible uses of the computer output.

The report also describes concepts which are important in computing interval reliability for control systems and for analysis of catastropic Top Events. These concepts include:

- Critical System States
- Initiating Events
- Enabling Events

The differences in meaning between system unavailability, system unreliability, the expected number of system failures and the importance measures computed in terms of these expressions are explained.

TABLE OF CONTENTS

Section		Page
1.0	INTRODUCTION	1-1
2.0	PROBABILISTIC CALCULATIONS OF IMPORTANCE	2-1
2.1	Reliability Concepts	2-1
2.2	Assumptions for the Calculations	2-3
2.3	Flowsheet Depicting Calculations	2-4
2.4	Reliability Network Diagrams	2-5
2.5	System Unavailability	2-5
2.6	Expected Number of System Failures	2-13
2.7	Asymptotic Top Event Characteristics	2-27
2.8	Bound to System Unreliability	2-28
2.9	Use of System Performance Measures	2-33
2.10	Importance Measures	2-34
3.0	PROBABILISTIC IMPORTANCE	3-1
3.1	General Summary	3-1
3.2	Options to the Code	3-2
3.3	IMPORTANCE Input	3-5
3.4	Pressure Tank Example	3-10
3.5	Program Implementation	3-29
4.0	COMMERCIAL APPLICATION OF IMPORTANCE	4-1
4.1	Chlorine Vaporizer System	4-1
4.2	System Digraphs	4-5
4.3	Component Failure Mode Analysis	4-5
4.4	Fault Tree Generation and Qualitative Analysis	4-5
4.5	Reliability Analysis	4-9
4.6	Comments	4-11
5.0	FUTURE DEVELOPMENTS	5-1
6.0	REFERENCES	6-1
APPENDICES		
A	IMPORTANCE OUTPUT FOR PROPORTIONAL HAZARDS	A-1
B	IMPORTANCE OUTPUT FOR INTERVAL RELIABILITY ANALYSIS	B-1
C	IMPORTANCE OUTPUT FOR CHLORINE VAPORIZER	C-1

LIST OF TABLES

Table No.		Page
1-1	Event Types for Control System Analysis	1-5
2-1	IMPORTANCE Measures of System Unavailability	2-38
2-2	IMPORTANCE Measures of Interval Reliability	2-40
3-1	IMPORTANCE Measures Computed in IMPORTANCE Computer Code	3-3
3-2	Variables in PARVC Vector	3-31
3-3	Error Messages that cause IMPORTANCE to be terminated	3-32

LIST OF FIGURES

Figure No.		Page
2-1	Calculational Flow Sheet for IMPORTANCE	2-5
2-2	Four Sample Systems	2-7
2-2B	Accuracy of Min Cut Upper Bound 2-out-of-3-System	2-14
2-3	Component Unavailability, Constant λ and τ	2-22
2-4	Failure Frequency, Constant λ and τ	2-23
2-5	Sample System to Illustrate Bounds	2-30
2-6	Transitional State Diagram for Sample System	2-31
2-7	System Performance Measures Versus Time	2-32
3-1	SETS-IMPORTANCE Interface	3-6
3-2	Pressure Tank System	3-11
3-3	Digraph for Pressure Tank Rupture	3-13
3-4	Fault Tree for Pressure Tank Rupture	3-14
3-5	SETS Input	3-16
3-6	SETS Output	3-17
3-7	IMPORTANCE Input - Proportional Hazards	3-21
3-8	IMPORTANCE Input - Interval Reliability Analysis	3-25
3-9	Simplified Example	3-33
4-1	Original System	4-2
4-2	System A	4-3
4-3	System B	4-4
4-4	System Digraph for System A	4-6
4-5	Failure Modes	4-7
4-6	Failure Modes	4-8
4-7	Effect of System Design Changes	4-10

1.0 INTRODUCTION

The first version of the fault tree computer code, IMPORTANCE, was developed in 1975 at Lawrence Livermore Laboratory. The code was written as part of a Ph.D. thesis entitled "Fault Trees for Decision Making in Systems Analysis."[1] Several examples of the use of the code are presented in the thesis.

IMPORTANCE computes various measures of system performance for systems which have been modeled in terms of a fault tree with a Top Event. Some of these measures are:

- System unavailability
- Expected number of system failures
- Top Event rate (rate of system failure)
- Mean time to occurrence of the Top Event
- Mean duration time of the Top Event

The code computes various measures of probabilistic importance (sensitivity) for basic events and for system modes of failure called the min cut sets.* These measures can aid an analyst in determining weaknesses in a system and suggest the optimal course of system upgrade. Analysis of most non-trivial systems produces an enormous number of min cut sets. A sensitivity analysis is necessary in identifying important contributors because it is virtually impossible for an analyst to visually inspect all the min cut sets and make an assessment of the relative contribution of a component to system failure. This is particularly true if (1) basic events appear in many cut sets (i.e., components are replicated) and (2) basic events have varying failure rates and fault duration times.

---

* Basic events represent the limit of resolution in fault tree analysis and are events such as human error, hardware failure and environmental conditions for which probabilistic data exist.

IMPORTANCE has been revised so that its calculations can be used for interval reliability analysis and for probabilistic analysis of control systems. Also emphasized is that the engineering analysis necessary to construct the fault tree must also be applied in the reliability calculations.

This report describes a new version of IMPORTANCE which accepts as input the min cut sets generated from the computer code, Set Evaluation Transformation System, SETS. SETS has been developed at Sandia National Laboratories. The code symbolically and directly manipulates Boolean equations. SETS can be used for qualitative evaluations of fault trees (2). Some of the many uses of SETS are listed below:

- Finding prime implicants to fault trees
- Conducting a common cause analysis (3)
- Modeling of safeguards effectiveness (4), (5) and (6)

To make the analysis of complicated fault trees more efficient, SETS allows the user to locate independent subtrees (called modules) and/or conduct the Boolean reduction in stages (2). A newer version of the code has been generated which requires less user interaction by use of a special command called GENFTEQN, "generate fault tree equation." (7).

The computer code IMPORTANCE has been revised so that its calculations can be used for reliability analysis of control systems. These calculations are based on the concept of interval reliability which is relevant when the system is required to operate over an interval of time without failure. System unavailability, which is a measure of performance at one point in time, is meaningless for analysis of catastrophic system events. Examples of Top Events which require interval reliability analysis are:

- "Explosion of butadiene chemical reactor"
- "Inadvertant launch of ballistic missile"

- "Auxiliary feedwater system fails to operate for 24 hours following loss of main feedwater"
- "Device fires upon inadvertant arming"
- "Security system vulnerable to theft of Special Nuclear Material"

As suggested by the listing of the Top Events above, interval reliability analysis is applicable to a wide range of systems, e.g.,

- Chemical processing systems
- Aerospace systems
- Nuclear systems
- Weapon systems

One measure of sensitivity computed by the code is expressed in terms of system unavailability. For this measure, we are interested in events that quantitatively contribute to the downtime of the system. Other measures are computed in terms of the expected number of system failures (the integral of Top Event rate over the mission time) which is a measure of system performance over an interval of time. For this measure, we are interested in events which contribute to or cause the system to make a transition from the unfailed to the failed state. System unreliability, the probability of one or more failures, is another measure of system performance over an interval of time. When system failure is rare over the mission time (which is true for many systems analyzed by fault tree analysis), then the expected number of system failures is an accurate approximation to system unreliability.

Concepts of availability and interval reliability can be explained in terms of an example involving an airplane flight. Whether the plane checks out okay before takeoff is a question of availability. Given successful takeoff, whether the plane can fly to the destination is a question of reliability. The same analogy applies to engineered safeguard systems designed to mitigate the effects of a loss of coolant accident at a nuclear power plant.

Interval reliability analysis requires that two types of basic events be identified:

- Initiating Events cause a perturbation of system variables from their normal value. *
- Enabling Events permit initiating events to cause the Top Event (also known as "demand" failures)

For example in weapon systems, enabling events could be events that inadvertantly arm a device. Initiating events are events that fire the device given inadvertant arming. As another example, an enabling event could represent loss of redundancy in a system—loss of the other redundant component then represents the initiating event which causes the Top Event to occur.

In the context of control systems, initiating events perturb system variables and place a demand on the control system to respond.

Enabling events inactivate control loops and include events such as:

- Control device inactive
- Relay contacts fail to respond
- Operator fails to respond

The time required for the initiating event to cause the Top Event is generally small, hence the probability of another component failing during this time is small. However, the time in many cases is long enough to consider mitigative action from the operator. Following this reasoning, enabling events representing component failures generally occur before the occurrence of the initiating event whereas events involving the operator failing to respond occur after the occurrence of the initiating event. The occurrence of the enabling event is

---

* The basic starting point for the construction of event trees and cause consequence diagrams is the identification of initiating events.

conditional (in a statistical sense) on the occurrence of the initiating event. This implies that the order in which events occur is important in interval reliability analysis. Table I-1 categorizes initiating and enabling events for simple negative feedback and feedforward loops. Note that reversal of a control device on a negative feedforward loop (NFFL) causes the loop to be positive. Another system disturbance is required to perturb system variables since positive feedforward loops do not amplify noise like positive feedback loops do. For this reason, a reversal of a control device on a NFFL is an enabling event.

It is important to note that the engineer who constructed the fault tree need not be separated from the quantitative analysis. For example, in the Reactor Safety Study, fault tree analysts supplied information on failure rates and fault duration times. Fault tree analysts must also identify enabling events and initiating events. Failure of some components can be either enabling, or initiating -- zero gain or "stuck" failures are enablers, initiators are the fail high or low modes.

It is important to note that in some cases an event can be either an initiating or enabling event. For example, consider a redundant system of two components whose failure will cause system failure. The component that fails first is an enabling event -- the component that fails last is the initiating event. A similar example with this property is a fire caused by the two events listed below which can occur in either order:

- Spill of flammable material
- Ignition source present

A useful feature of IMPORTANCE is the ease with which the code can handle enabling gate events in the fault tree. No separate analysis of this gate event is required. In the IMPORTANCE input the analyst simply indicates that all basic events below the gate event are enabling events.

In the next section we explain, in terms of examples, the probabilistic calculations computed in IMPORTANCE. The importance of identifying initiating and enabling events for interval reliability analysis is shown.

TABLE I-1

EVENT TYPES FOR CONTROL SYSTEM ANALYSIS

Event	Negative Feedback Loop	Negative Feedforward Loop
Control Device Inactive	Enabler	Enabler
Control Device Fails High or Low	Initiator	Initiator
Control Device Reversed	Initiator	Enabler
External Disturbance	Initator	Initiator

In Section 3.0 we explain the input specifications for the computer codes IMPORTANCE and describe the interface with SETS. We use the simple example of a Pressure Tank System to interpret the meaning of the computer output. As illustrated in Section 4.0, many of the concepts and ideas presented in the reliability analysis of the Pressure Tank system can be directly extended to the design of chemical processing systems and more generally to control systems. In this section we describe how duPont Co. has used IMPORTANCE to improve the safety of a chlorine vaporizer system. In Section 5.0, we describe potential future developments of IMPORTANCE.

The reader who is interested only in the input specifications to IMPORTANCE should go directly to Section 3.3.

2.0 PROBABILISTIC CALCULATIONS OF IMPORTANCE

To explain the probabilistic calculations of IMPORTANCE, we discuss the following topics:

- Reliability concepts
- The assumptions in the probabilistic calculations
- Flowsheet representing the reliability calculations of IMPORTANCE
- Reliability network diagrams
- System unavailability
- Expected number of system failures
- Asymptotic Top Event characteristics
- Bound to system (un)reliability
- Probabilistic importance

2.1 RELIABILITY CONCEPTS

Availability

The term "availability" will be used in two distinct senses:

(1) Availability = Probability that a system works upon demand

(2) Availability at time t = Probability that a system is working at time t

(a component can be considered to be a system)

Definition (1) is applicable to standby safety systems which change state upon demand.

Definition (2) is applicable to systems containing repairable components with non-catastrophic Top Events. It is not applicable to systems containing repairable components with catastrophic Top Events since repairing components in this case does not rectify the occurrence of the Top Event.

Definition (2) is also applicable to systems consisting of non-repairable components. In this case working at time t implies that the system has worked continuously in the time interval $\left[t_0, t\right]$ where t_0 equals the start of the mission time.

Reliability

The reliability of a system over an interval of time is the probability that the system works continuously over that interval of time. If we let $S_i(0,t)$ be the event that there are exactly i system failures in $(0,t)$, then we can define reliability by:

$$F_s(t) = P(S_0(0,t))$$

$$= 1 - \sum_{i=1}^{\infty} P(S_i(0,t))$$

As described in the introduction, reliability is especially relevant to systems for which system failure is catastrophic or for non-repairable systems.

Expected Number of System Failures

If we let $N_s(t)$ be the number of system failures in $(0,t)$, then the expected number of system failures in $(0,t)$ is given by:

$$E\left[N_s(t)\right] = \sum_{i=1}^{\infty} i\, P(S_i(0,t))$$

For Top Events which represent a non-catastrophic shutdown of a (repairable) system, availability, reliability and the expected number of system failures are

all distinct and useful measures of system performance. For non-repairable systems, such as satellite and aerospace systems, availability, reliability, and 1 minus the expected number of system failures are identical in value. This is because for non-repairable systems: (1) the system works at time t if and only if it has worked during $(0,t)$—thus availability equals reliability, and (2) the probability of two or more failures equals 0, so the expected number of system failures equals the probability of one failure (in (0,t)) and reliability equals 1 minus the expected number of system failures.

As described in the introduction, basic events can be divided into two categories: initiating events and enabling events. Enabling events represent demand failures, conditional on the occurrence of the initiating event in causing the Top Event to occur. Each minimal cut set will contain at least one initiating event. A single event minimal cut set represents the situation where there are no protective features to prevent the initiating event from causing the Top Event to occur. Minimal cut set probabilities and hence Top Event probabilities will be computed using the following conditional probability expression:

$$P(A)\,P(B/A)$$

where A represents the event "initiating event occurs" and B/A represents the event "enabling event occurs given that the initiating event occurs."

2.2 ASSUMPTIONS

The assumptions used for the calculation in IMPORTANCE are listed below:

- Component failures cannot improve system performance (and component success cannot degrade system performance)*

---

* This implies that we do not allow complemented events in the min cut sets for IMPORTANCE. Fault trees for reliable systems generally generate complemented events which have a probability of occurrence near unity. Setting these events to TRUE to eliminate complemented events in the min cut sets will result in a slightly conservative overprediction in the probability of the Top Event for reliable systems. This step must be conducted in SETS before running IMPORTANCE if the fault tree contains complemented events.

- Occurrences of basic events are statistically independent
- Repair processes are statistically independent (this assumes a separate repairman for each component in the system)
- The probability of occurrence of two or more initiating events in a differential time interval is zero (i.e., of order $(dt)^2$ where dt is a differential time interval)

2.3 FLOWSHEET DEPICTING CALCULATIONS

Figure 2-1 depicts a flowsheet that is helpful in understanding the calculations of IMPORTANCE. It is helpful to refer to Figure 2-1 for the discussions in the following sections. As indicated by the dashed line, the calculations of IMPORTANCE are both deterministic (i.e., qualitative) and probabilistic. Both computations require a Boolean structural representation of the Top Event which in IMPORTANCE is given by the Boolean union of all the min cut sets. The deterministic calculations compute the structural importance of a basic event. For example, when considering the event "failure to operate," a component placed in series with a system is structurally more important than that component placed in parallel with a system. Computing structural importance requires that the criticality function as described in Section 2.6 be computed. This function allows us to determine the number of system states in which the failure of a component will cause the system to fail. (There are a total of 2^n system states where n equals the number of system components.) Probabilistic calculations in IMPORTANCE compute both time dependent and steady state values for system unavailability, Top Event Rate and expected number of system failures.

Computing system unavailability and importance measures based on system unavailability requires that component (basic event) unavailability be computed. This in turn requires that the basic event parameters be known, i.e., failure rates and fault duration times. (These parameters are also used to compute the failure frequency.) Computing the Top Event rate and the expected number of system failures requires that the following quantities be calculated for each system component:

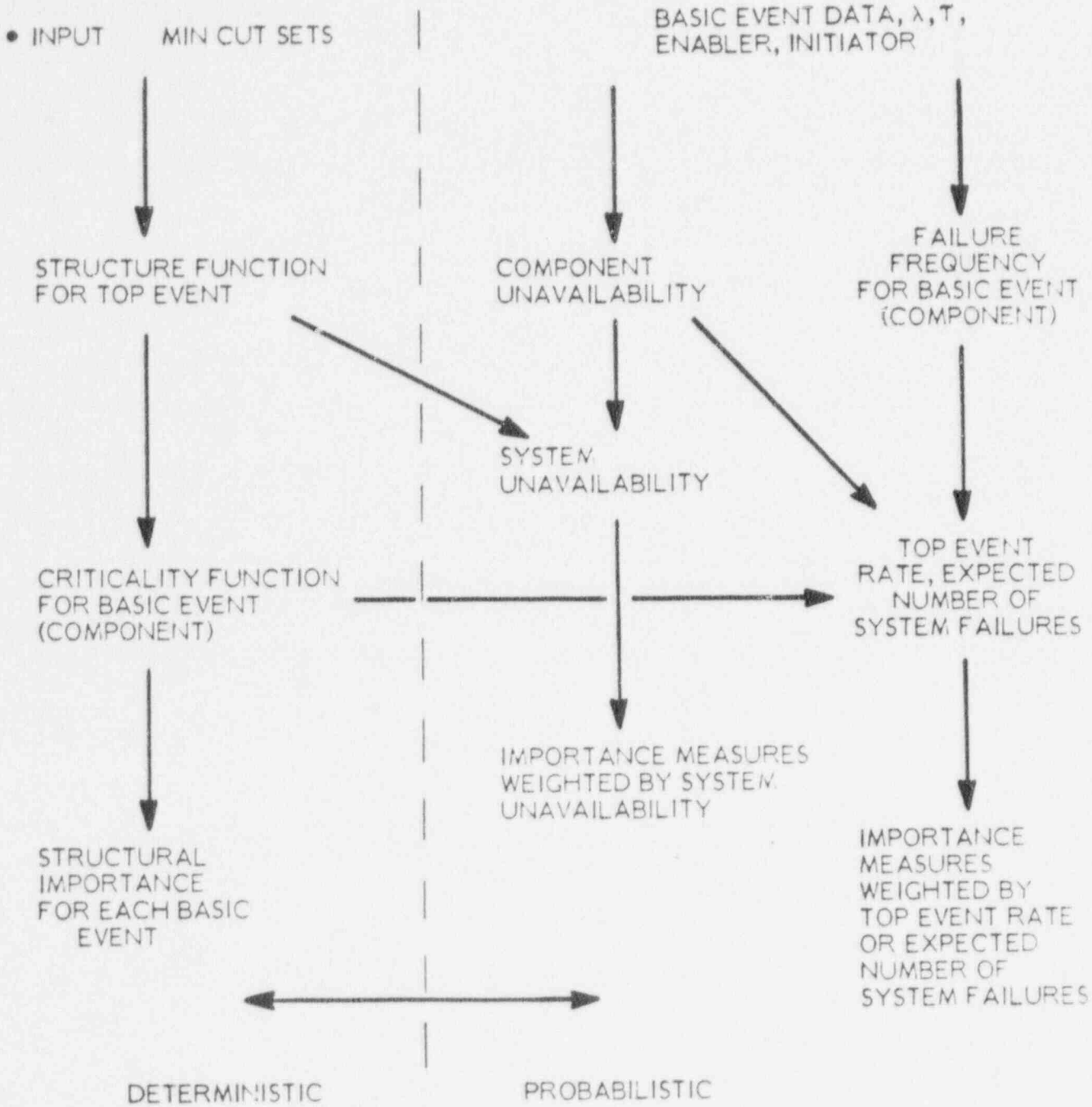


FIGURE 2-1

CALCULATIONAL FLOW SHEET FOR IMPORTANCE

- Criticality Function
- Unavailability
- Failure Frequency

In addition, the basic event type, i.e., whether the basic event is an initiating or enabling event must be specified.

2.4 RELIABILITY NETWORK DIAGRAMS

Reliability network diagrams, fault trees and min cut sets are introduced by way of four examples in Figure 2-2.

A cut set is a set of components such that failure of these components guarantees system failure. A cut set can be thought of as a "cut" through the reliability network diagram which divides it into two separate pieces. A min cut set is a cut set with the additional property that no proper subset of it is also a cut set.

2.5 SYSTEM UNAVAILABILITY

If we take the Boolean union of all of a system's min cut sets, we have one representation of that system's "structure function"—a mapping from the set of 2^n (mutually exclusive) system states (n = the number of components in the system) to 0 and 1 ; 0 if the system works in that system state and 1 if it does not.

Let i denote the event "component i is in a failed state," and $\bar{i}$ the event "component i works".* Let

$$P(i) = q_i$$

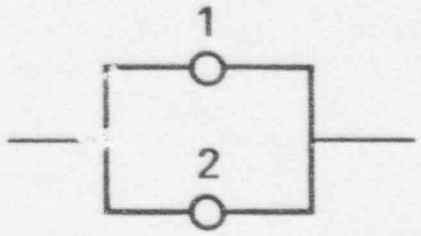
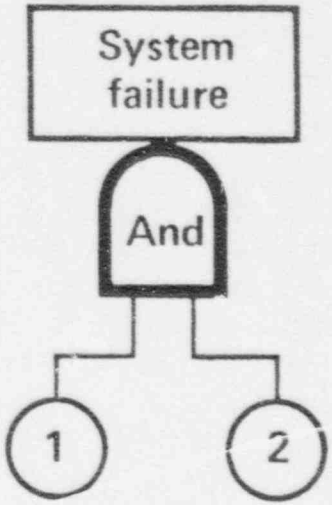
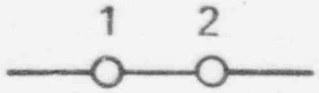
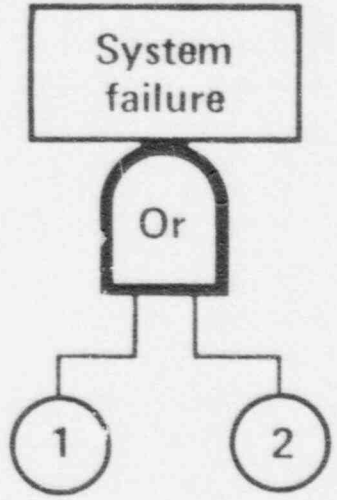
and

$$P(\bar{i}) = 1 - q_i$$

---

* With this notation, $(\bar{1},2)$ is an example of a system state for a two component system (corresponding to component 1 working and component 2 not working).

FOUR SAMPLE SYSTEMS

System	Reliability network diagram	Fault tree	Min cut sets
Parallel			Component 1 fails and component 2 fails $\{1,2\}$
Series			$\{1\}, \{2\}$

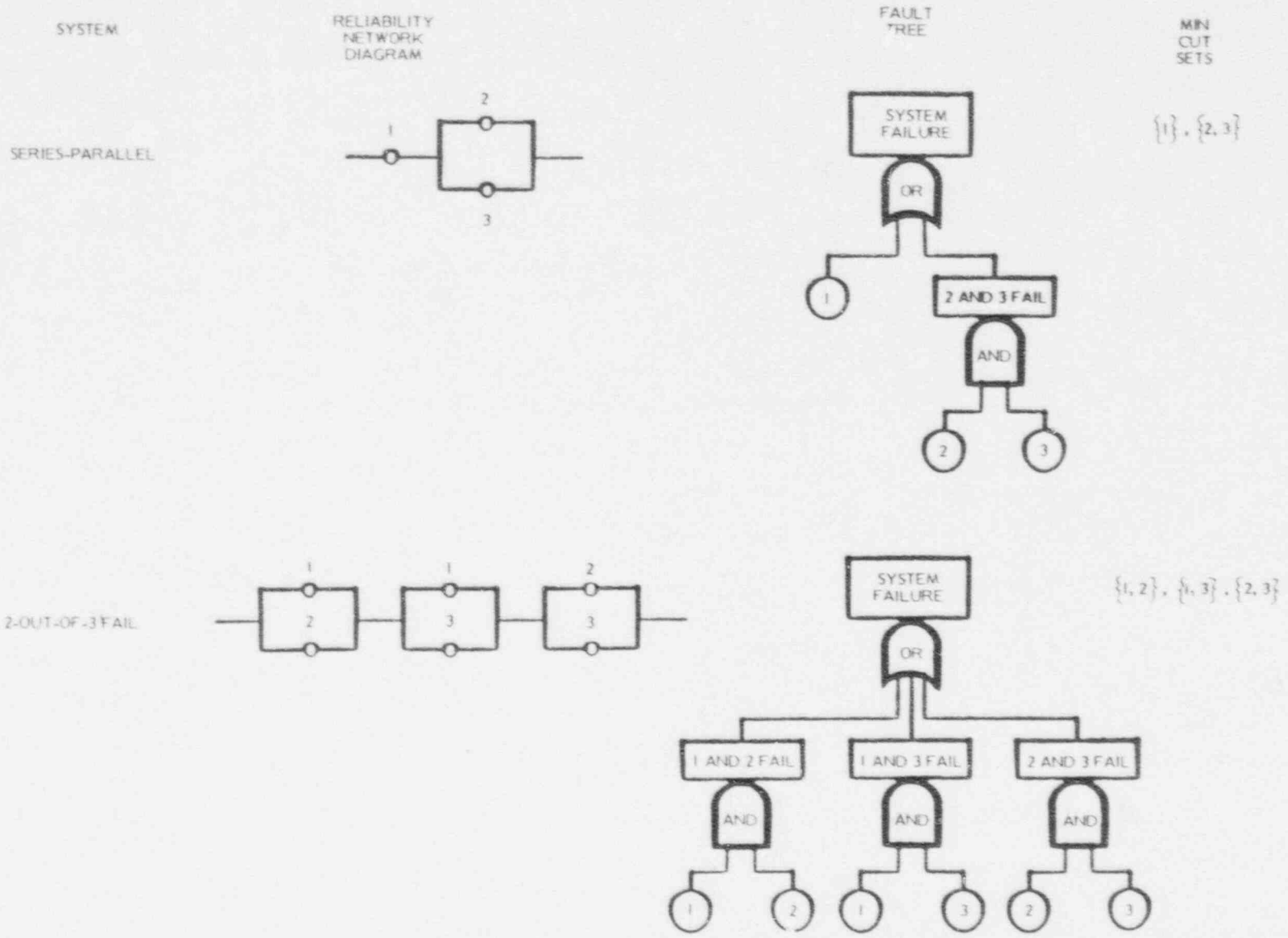


FIGURE 2-2

FOUR SAMPLE SYSTEMS
(CONT.)

The following table shows the four system states of a two component system, their probability of occurrence and the corresponding series and parallel structure function values.

System State	Probability of Occurrence	Series Structure Function Value	Parallel Structure Function Value
$(1,2)$	$q_1 q_2$	1	1
$(\bar{1},2)$	$(1 - q_1) q_2$	1	0
$(1,\bar{2})$	$q_1 (1 - q_2)$	1	0
$(\bar{1},\bar{2})$	$(1 - q_1)(1 - q_2)$	0	0

System unavailability ($g(\underline{q})$) is the probability that the system is in a failed state (i.e., that the system's structure function equals 1). Thus it equals the sum of the probabilities of occurrence of the system states whose structure functions equal 1 as is illustrated below (since system states are mutually exclusive).

System	System Unavailability ($g(\underline{q})$)
2 component series	$q_1 q_2 + (1 - q_1) q_2 + q_1 (1 - q_2)$ $= q_1 + q_2 - q_1 q_2$ $= 1 - (1 - q_1)(1 - q_2)$
2 component parallel	$q_1 q_2$
n component series	$1 - \prod_{i=1}^{n} (1 - q_i)$
n component parallel	$\prod_{i=1}^{n} q_i$

The results for the 2-out-of-3 case are given below:

System State	Probability of Occurrence	2-out-of-3 Struc. Funct. Value
$(1,2,3)$	$q_1 q_2 q_3$	1
$(\bar{1},2,3)$	$(1 - q_1) q_2 q_3$	1
$(1,\bar{2},3)$	$q_1 (1 - q_2) q_3$	1
$(1,2,\bar{3})$	$q_1 q_2 (1 - q_3)$	1
$(\bar{1},\bar{2},3)$	$(1 - q_1)(1 - q_2) q_3$	0
$(\bar{1},2,\bar{3})$	$(1 - q_1) q_2 (1 - q_3)$	0
$(1,\bar{2},\bar{3})$	$q_1 (1 - q_2)(1 - q_3)$	0
$(\bar{1},\bar{2},\bar{3})$	$(1 - q_1)(1 - q_2)(1 - q_3)$	0

$$g = q_1q_2q_3 + (1 - q_1) q_2q_3 + q_1 (1 - q_2) q_3 + q_1q_2 (1-q_3)$$

$$= q_1q_2 + q_1q_3 + q_2q_3 - 2q_1q_2q_3$$

An upper bound to system unavailability is given by the sum of the probabilities of occurrence of all min cut sets (this is called the "rare event approximation").

To see that this is an upper bound, let E_i = the event that min cut set i occurs. ($i = 1, \ldots, K$ where K = number of min cut sets)

$$P \text{ (system failure)} = P\left(\sum_{i=1}^{K} E_i \right) \leq$$

$$P(E_1) + P(E_2) + \ldots + P(E_K)$$

by probability theory since the E_i's are not mutually exclusive events (i.e., we are not subtracting off the probabilities associated with the occurrence of two or more overlapping min cut sets).

The following table illustrates this idea:

	2-Component Series	2-out-of-3
Unavailability	$q_1 + q_2 - q_1q_2$	$q_1q_2 + q_1q_3 + q_2q_3 - 2q_1q_2q_3$
Min Cut Sets	$\{1\}$, $\{2\}$	$\{1,2\}$, $\{1,3\}$, $\{2,3\}$
Rare Event Approximation	$q_1 + q_2$	$q_1q_2 + q_1q_3 + q_2q_3$

If component failures are "rare events," then the probability of two or more cut sets failing is small and so the rare event approximation is accurate. The rare event approximation is useful in describing the calculations of IMPORTANCE. However, IMPORTANCE uses a more accurate bound for reliable systems called the min cut set upper bound which is described below.

We can express the probability of system failure as follows:

$$\begin{aligned} P(\text{system failure}) &= P(\text{at least 1 min cut set occurs}) \\ &= 1 - P(\text{no min cut set occurs}) \end{aligned}$$

It can be shown that

$$P(\text{no min cut set occurs}) \geq \prod_{i=1}^{K} P(\text{min cut set } i \text{ does not occur})$$

Thus we have that

$$P(\text{system failure}) \leq 1 - \prod_{i=1}^{K} P(\text{min cut set } i \text{ does not occur})$$

$$= 1 - \prod_{i=1}^{K} (1 - P(E_i))$$

This approximation is called the "min cut set upper bound" to system unavailability.

Esary and Proschan proved that the following relation holds:

$$g(\underline{q}) \leq 1 - \prod_{i=1}^{K} (1 - P(E_i)) \leq \sum_{i=1}^{K} P(E_i) \qquad (1)$$

Exact — Min Cut Set Upper Bound — Rare Event Approximation

The table below illustrates this inequality for the 2-out-of-3 system:

	2-out-of-3 System
System Unavailability	$q_1q_2 + q_1q_3 + q_2q_3 - 2\,q_1q_2q_3$
Min Cut Set Upper Bound	$1 - (1 - q_1q_2)(1 - q_1q_3)(1 - q_2q_3)$
	$= q_1q_2 + q_1q_3 + q_2q_3$
	$- (q_1 + q_2 + q_3 - q_1q_2q_3)\,q_1q_2q_3$
Rare Event Approximation	$q_1q_2 + q_1q_3 + q_2q_3$

Now,

$$0 \leq q_1 + q_2 + q_3 - q_1q_2q_3 \leq 2$$

for $q_i \in [0,1]$

so we see that inequality (1) holds.

If component failures are rare events (i.e., if the q_i's are small) we see that the min cut set upper bound and the rare event approximation are both close to the true value since the three expressions only differ in terms involving three or more q_i's, and these terms are small compared to the terms only involving two q_i's.

Figure 2-3 plots all three expressions versus a shared basic event probability (i.e., $q_1 = q_2 = q_3 = q$) for the three components and shows the accuracy of the approximations for small q.

2.6 EXPECTED NUMBER OF SYSTEM FAILURES

To compute the expected number of system failures, we need to explain the following basic event characteristics:

- Critical System States
- Time Dependent Component Unavailability
- Failure Frequency

CRITICAL SYSTEM STATES

A critical system state for component i is a state for the remaining n-1 components such that failure of component i causes the system to go from a working to a failed state. See the table below for some examples.

ACCURACY OF MIN CUT UPPER BOUND 2-OUT-OF-3 SYSTEM

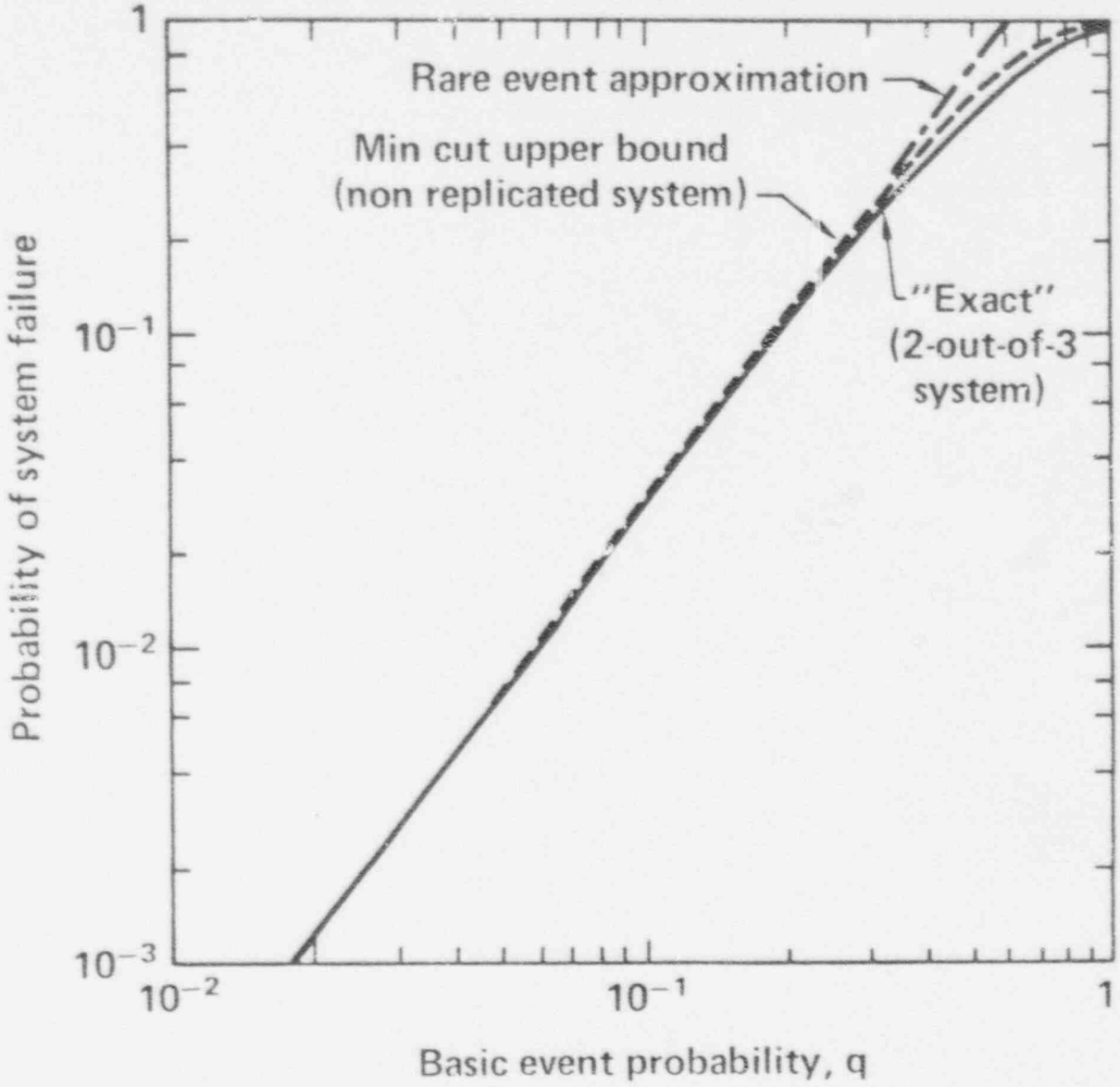


FIGURE 2.2 B

System	State	Probability of Occurrence	Critical System State for Component 1?
Series	$(\cdot,2)$	q_2	No
	$(\cdot,\bar{2})$	$1 - q_2$	Yes
Parallel	$(\cdot,2)$	q_2	Yes
	$(\cdot,\bar{2})$	$1 - q_2$	No
2-out-of-3	$(\cdot,2,3)$	$q_2 q_3$	No
	$(\cdot,\bar{2},3)$	$(1 - q_2) q_3$	Yes
	$(\cdot,2,\bar{3})$	$q_2 (1 - q_3)$	Yes
	$(\cdot,\bar{2},\bar{3})$	$(1 - q_2)(1 - q_3)$	No

For a series system $(\cdot,2)$ is not a critical system state for component 1 since if component 2 has already failed then the system is already in a failed state and so failure of component 1 does not cause the system to go from a working to a failed state.

The criticality function for component i, $\Delta g_i(q)$, is the probability that the system is in a critical system state for component i. Thus it is the sum of the probabilities of occurrence of the critical system states for component i. Thus the criticality function for component 1 for a series system is $1 - q_2$, for a parallel system q_2 and for a 2-out-of-3 system $(1 - q_2) q_3 + q_2 (1 - q_3)$. The criticality function is also called Birnbaum's measure of importance.

Two expressions for the criticality function $\Delta g_i(\underline{q})$ are

(1) $g(1_i, \underline{q}) - g(0_i, \underline{q})$

where $(1_i, \underline{q}) = (q_1, \ldots, q_{i-1}, 1, q_{i+1}, \ldots, q_n)$

$(0_i, \underline{q}) = (q_1, \ldots, q_{i-1}, 0, q_{i+1}, \ldots, q_n)$

and (2) $\dfrac{\partial g(\underline{q})}{\partial q_i}$

(1) is the probability the system works with component i working minus the probability the system works with component i not working and is thus the probability that the system works only if component i works, i.e., it is the criticality function.

g (q) is a linear function of each q_i and so

$$\frac{\partial g(\underline{q})}{\partial q_i} = \frac{g(1_i, \underline{q}) - g(0_i, \underline{q})}{1 - 0}$$

Thus (1) and (2) are equivalent.

IMPORTANCE uses the min cut set upper bound to compute both $g(1_i, \underline{q})$ and $g(0_i, \underline{q})$. Strictly speaking, one should substract a lower bound for $g(0_i, \underline{q})$. However, for reliable systems, we have not found a case for basic events in cut sets of order 2 or higher in which IMPORTANCE does not give a conservative overprediction for $\Delta g_i(\underline{q})$. This is due to the fact that for reliable systems the overprediction by the minimal cut set upper bound increases as the system becomes less reliable, as is illustrated in Figure 2-2.

For a system to be in a critical system state for component i, all the components in a min cut set containing i, other than i, clearly must have failed (so that the failure of i can cause system failure). On the other hand, even if all the components in a min cut set containing i, other than i, have failed, a min cut set not containing i may have already caused system failure (making that system state "non-critical" for component i). Thus we see that the set of system states for which all the components in a min cut set containing i, other than i, have failed is larger than (contains) the set of critical system states for i. Thus, if we

let E_k^i be the event "$\{\{$min cut set k (containing i)$\}$ - $\{i\}\}$ occurs," we see that

$$\Delta g_i(q) \leq \sum_{k \mid i \in k} P(E_k^i) \qquad (2\text{-}1)$$

This upper bound will be used later in an example to explain the calculations of IMPORTANCE.

To illustrate the above inequality, consider component 1 in a 2-out-of-3 system. There are two min cut sets containing component 1: $\{1,2\}$, $\{1,3\}$. Thus,

$$\sum_{k \mid i \in k} P(E_k^1) = q_2 + q_3$$

As stated earlier for a 2-out-of-3 system

$$\begin{aligned} \Delta g_1(q) &= q_2(1 - q_3) + q_3(1 - q_2) \\ &= q_2 + q_3 - q_2 q_3 \end{aligned}$$

and so we see that the above inequality holds.

The calculations thus far have considered the system at one point in time, i.e., we have not considered time dependent component unavailability, q(t). The following section discusses maintenance policies and reliability parameters necessary for computing q(t).

MAINTENANCE POLICIES

There are three basic types of maintenance policies considered in IMPORTANCE:

(1) No Repair

(2) Repair - Announced Failure (unscheduled maintenance)

(3) Repair - Unannounced Failure (scheduled maintenance or inspections every θ time units)

Maintenance Type (1) is typical of satellites and other remotely controlled systems. Type (2) is common when some kind of continuous process is being monitored (such as a chemical processing plant). Type (3) is common to standby safety systems such as fire protection systems).

FAILURE RATE

If we let

$$F(t) = P \text{ (a given non-repairable component fails in } (0,t))$$

and $f(t)$ be the corresponding density (if it exists), then we can define the failure rate at time t by

$$\lambda(t) = \frac{f(t)}{1 - F(t)} \qquad (2\text{-}2)$$

$\lambda(t)$ has the significance that

$$\lambda(t)\,\Delta t \approx P \left(\text{the component fails in } (t, t + \Delta t) \;\middle|\; \text{it has not failed in } (0,t) \right)$$

for small Δt. This is because

$$\frac{f(t)}{1 - F(t)}\,\Delta t \approx \frac{\frac{F(t + \Delta t) - F(t)}{\Delta t}}{1 - F(t)}\,\Delta t$$

$$= \frac{F(t + \Delta t) - F(t)}{1 - F(t)}$$

$$= \frac{P(\text{component fails in } (t, t + \Delta t))}{P(\text{component has not failed in } (0,t))}$$

$$= P(\text{component fails in } (t, t + \Delta t) \mid \text{component has not failed in } (0,t))$$

If we integrate both sides of equation (2-2), we obtain

$$\int_0^t \lambda(t')\, dt' = -\log(1 - F(t))$$

This implies that

$$F(t) = 1 - e^{-\int_0^t \lambda(t')\, dt'}$$

REPAIR RATE

Following exactly the analysis for failure rate, if we let

$$R(t) = P(\text{a given, failed, component is repaired in } (0,t))$$

(where time "0" is the time at which the component fails)

and $r(t)$ be the corresponding density (if it exists), then we can define the repair rate at time t by

$$\nu(t) = \frac{r(t)}{1 - R(t)}$$

where

$$\nu(t)\Delta t \approx P \text{ (component is repaired in } (t, t + \Delta t) \mid \text{it has not been repaired in } (0,t))$$

Analogously to before, we obtain

$$R(t) = 1 - e^{-\int_0^t \nu(t')\, dt'}$$

In IMPORTANCE, both failure rates and the repair rates are assumed to be constants, thus

$$F(t) = 1 - e^{-\int_0^t \lambda\, dt'}$$

$$= 1 - e^{-\lambda t}$$

and

$$R(t) = 1 - e^{-\int_0^t \nu\, dt'}$$

$$= 1 - e^{-\nu t}$$

(i.e., we assume that the time to failure and repair are exponentially distributed)

It is easy to show that for the exponential case, the mean time to failure (μ) = $1/\lambda$, and the mean repair time (τ_r) = $1/\upsilon$.

FAILURE FREQUENCY

For both repairable and non-repairable components, the failure frequency ($w_f(t)$) is defined as:

$$w_f(t) = \lim_{\Delta t \to 0} \frac{P\,(\text{a given component fails in } (t, t+\Delta t))}{\Delta t}$$

$w_f(t)\,\Delta t$ is the unconditional probability of failure in $(t, t + \Delta t)$, as opposed to $\lambda(t)\,\Delta t$ which is the conditional probability of failure in $(t, t + \Delta t)$ (given no failures in $(0,t)$).

It can be shown that

$$\int_0^t w_f(t)\,dt = \text{the expected number of component failures in } \left[0,t\right]$$

Component unavailability and failure frequency are given in Figures 2-3 and 2-4 for the three types of maintenance policies. The results for the two repair cases are asymptotic and obtained from renewal theory.

CALCULATIONS OF EXPECTED NUMBER OF SYSTEM FAILURES

A system failure occurs when the system makes a transition from the unfailed to the failed state. From the discussions in the introduction, it is an initiating event which causes system failure when the system is in a critical system state for that event. The probability that the system is in a critical system state for initiating event i ($i = 1, \ldots n$) is (by definition) the criticality function $\Delta g_i(q)$ and the probability that an initiating event i occurs at t' in a differential time element dt' is $w_{f,i}(t')\,dt'$. Thus the probability of a system failure at t' in a differential time element dt' equals

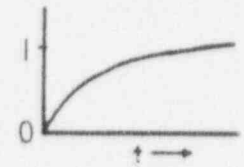
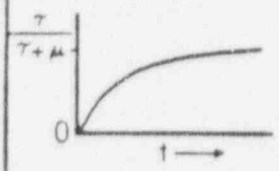
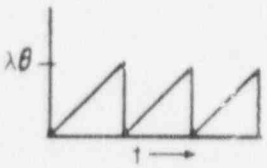
MAINTENANCE POLICY	COMPONENT UNAVAILABILITY	ASYMPTOTIC VALUE	GRAPH
NO REPAIR	$1 - e^{-\lambda t} \leq \lambda t$	1	
REPAIR ANNOUNCED FAILURE	$\frac{\tau}{\mu+\tau}\left(1 - e^{-\left(\frac{\mu+\tau}{\mu\tau}\right)t}\right)$	$\frac{\tau}{\mu+\tau} \leq \lambda\tau$	
REPAIR UNANNOUNCED FAILURE	$\sim 1 - e^{-\lambda(n\theta - t)}$ $(n-1)\ \theta \leq t \leq n\theta$ $n=1, 2, \ldots$	$\frac{\lambda\theta}{2} + \lambda\tau$ (AVERAGE UNAVAILABILITY)	

FIGURE 2-3

COMPONENT UNAVAILABILITY
CONSTANT λ AND τ

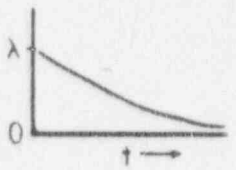
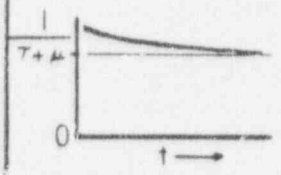
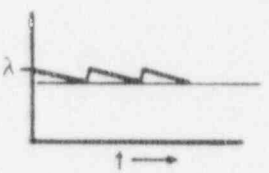
MAINTENANCE POLICY	FAILURE FREQUENCY	ASYMPTOTIC VALUE	GRAPH
NO REPAIR	$\lambda e^{-\lambda t}$	0	
REPAIR ANNOUNCED FAILURE	$\frac{1}{\mu+\tau} + \frac{\tau}{(\mu+\tau)} e^{-(\frac{\mu+\tau}{\mu\tau})t}$	$\frac{1}{\mu+\tau} < \lambda$	
REPAIR UNANNOUNCED FAILURE	$\sim\lambda e^{-\lambda(n\theta - t)}$ $(n-1)\ \theta \le t \le n\theta$ $n=1, 2, \ldots$	$\sim \lambda e^{-\frac{\lambda\theta}{2}} < \lambda$	

FIGURE 2-4

FAILURE FREQUENCY
CONSTANT λ AND γ

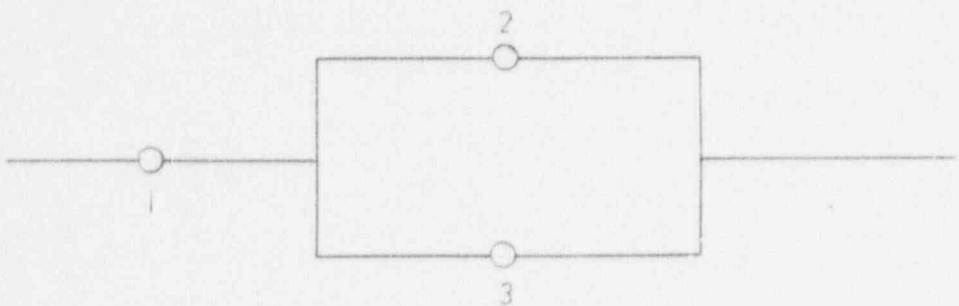
$$\left[\sum_{i=1}^{n} \Delta g_i \left(\underline{g}\,(t')\right)\ w_{f,i}\,(t')\right] dt' \qquad (2\text{-}3)$$

(the term in brackets is known as the "Top Event Rate" - R(t'))

Since the probability of two or more initiating events occurring in dt' is zero, the expected number of system failures in $\left[0,t\right]$ equals the integral of expression (2-3) over the interval $\left[0,t\right]$, i.e.,

$$E\left[N_s(t)\right] = \int_0^t \left[\sum_{i=1}^{n} \Delta g_i \left(\underline{g}\,(t')\right)\ w_{f,i}\,(t')\right] dt' \qquad (2\text{-}4)$$

As an example of the calculation of $E\left[N_s(t)\right]$, consider the series-parallel system given in the reliability network diagram below:



$$\text{If } Y_i = \begin{cases} 1 & \text{if component i is failed} \\ 0 & \text{if component i is working} \end{cases}$$

then the structure function for this system is given by

$$Y_1 + Y_2Y_3 - Y_1Y_2Y_3$$

Thus $g(\underline{q}(t)) = E(Y_1 + Y_2Y_3 - Y_1Y_2Y_3)$

$= q_1(t) + q_2(t)\,q_3(t) - q_1(t)\,q_2(t)\,q_3(t)$

since the components are assumed to be statistically independent.

This implies that

$$\Delta g_1(\underline{q}(t)) = 1 - q_2(t)\,q_3(t)$$

$$\Delta g_2(\underline{q}(t)) = q_3(t) - q_1(t)\,q_3(t)$$
$$= (1 - q_1(t))\,q_3(t)$$

$$\Delta g_3(\underline{q}(t)) = q_2(t) - q_1(t)\,q_2(t)$$
$$= (1 - q_1(t))\,q_2(t)$$

Assume that the system is at steady state, failures are announced, and τ is small compared to μ. In this case we can use the approximations

$$q_i(t) = \frac{\tau_i}{\mu_i + \tau_i} \leq \frac{\tau_i}{\mu_i} = \lambda_i\,\tau_i \qquad (2\text{-}5)$$

and

$$w_{f,i}(t) = \frac{1}{\mu + \tau} \leq \frac{1}{\mu} = \lambda_i \qquad (2\text{-}6)$$

Thus, using equation (2-4), we get

$$E\left[N_s(t)\right] = \int_0^t R\,dt'$$

$$= R \cdot t$$

where $R = \sum_{i=1}^{3} \Delta g_i(\underline{q}(t))\, w_{f,i}(t)$

$$= (1 - \lambda_2 \tau_2\ \lambda_3 \tau_3)\ \lambda_1$$

$$+ (1 - \lambda_1 \tau_1)\lambda_3 \tau_3\ \lambda_2$$

$$+ (1 - \lambda_1 \tau_1)\lambda_2 \tau_2\ \lambda_3$$

Another example is the 2-out-of-3 system which has structure function

$$Y_1Y_2 + Y_1Y_3 + Y_2Y_3 - 2Y_2Y_2Y_3$$

and

$$g(\underline{q}(t)) = q_1q_2 + q_1q_3 + q_2q_3 - 2q_1q_2q_3$$

If we assume that

$$q_i(t) = \lambda\ \tau$$

and

$$w_{f,i}(t) = \lambda$$

for each i

we obtain

$$g(q(t)) = 3(\lambda\ \tau)^2 - 2(\lambda\ \tau)^3$$

$$3(\lambda\ \tau)^2$$

$$\Delta g_i(q(t)) = 2(\lambda\ \tau - (\lambda\ \tau)^2)$$

$$2\ \lambda\ \tau \qquad i = 1,2,3$$

So
$$E\left[N_s(t)\right] = \int_0^t (2 \cdot \lambda\tau \cdot \lambda + 2\,\lambda\tau \cdot \lambda + 2\,\lambda\tau \cdot \lambda)\, dt'$$
$$= 6\,\lambda^2 \tau \cdot t$$

If we let $\lambda =$ 10^{-4}/hr

$\tau =$ 10 hr

and $t =$ 30 years (e.g., the plant life)

we obtain

$$E\left[N_s(30 \text{ yrs})\right] = 0.16 \ \frac{\text{failures}}{\text{plant life}}$$

$$g(\underline{q}\,(30 \text{ yrs})) = 3.0 \times 10^{-6}$$

These two results show the large difference between these two measures of system performance.

2.7 ASYMPTOTIC TOP EVENT CHARACTERISTICS

$\frac{1}{R(\infty)}$ is the steady state (asymptotic) mean time between system failures. This mean time is clearly equal to the sum of the mean time to system failure ("mean uptime") and the mean time to system repair (mean downtime). Since $g(q(\infty))$ is the (steady state) proportion of time the system is in a failed state (and $1-g(\underline{g}(\infty))$ the proportion in a working state), the mean time to system failure (for $R(\infty) \neq 0$) is

$$(1 - g(\underline{q}(\infty)) \cdot \frac{1}{R(\infty)}$$

and the mean repair time is

$$g(\underline{q}(\infty)) \cdot \frac{1}{R(\infty)}$$

2.8 BOUNDS TO SYSTEM UNRELIABILITY

System unavailability, $g(\underline{q}(t))$, system unreliability, $(\bar{F}_s(t))$, and the expected number of system failures, $E\left[N_s(t)\right]$, have the following relationship:

$$g(\underline{q}(t)) \leq \bar{F}_s(t) \leq E[N_s(t)]$$

To see that $\bar{F}_s(t) \leq E\left[N_s(t)\right]$, let $P_i(t) = P$ (exactly i system failures in $[0,t]$). It then follows that

$$\bar{F}_s(t) = \sum_{i=1}^{\infty} P_i(t) \leq \sum_{i=1}^{\infty} i \cdot P_i(t) = E\left[N_s(t)\right]$$

with equality holding if and only if the probability of two or more system failures is 0, i.e., if we have an unrepairable system.

To see that $g(\underline{q}(t)) \leq \bar{F}_s(t)$ we need only realize that

$$\bar{F}_s(t) = g(\underline{q}(t)) + P \text{ (the system is working at time t but was failed at a time prior to t)}$$

since if the system is failed at t, then it has failed in $[0,t]$. Equality holds if and only if the second term on the right equals 0, i.e., if and only if the system is unrepairable (so that the event "working at t, but failed at a time prior to t" has probability 0).

Finding the exact system unreliability can be accomplished using a Markov approach where transitions can only take place between "neighboring" system states. (Here "neighboring" means "differing in only one component".) These are the only transitions which are possible since for the system to change states, at least one component must go from a failed to an unfailed state (or the reverse), and we are assuming that the probability of two or more components changing state simultaneously is 0.

For moderately large systems, implementation of the Markov approach becomes intractable because of the large number of system states (recall that there are 2^n where n = the number of components in the system). For reliable systems, however, $E[N_s(t)]$ is a very good approximation to system unreliability since, for these systems, the probability of two or more system failures is very small.

To illustrate this idea consider the sample system in Figure 2-5. This system is a 2-out-of-3 system in parallel with component 4. Each component is identical with $\tau = .1\ \mu$ (mean time to repair = .1 x mean time to failure). The transitional state diagram is shown in Figure 2-6 where the co-ordinates (x,y) have the following meaning:

$$x = \begin{cases} 1 & \text{component 4 has failed} \\ 0 & \text{component 4 has not failed} \end{cases}$$

$$y = \begin{cases} 3 & \text{components in 2-out-of-3 system} \\ 2 & \text{components in 2-out-of-3 system failed} \\ 1 & \text{component in 2-out-of-3 system failed} \\ 0 & \text{components in 2-out-of-3 system failed} \end{cases}$$

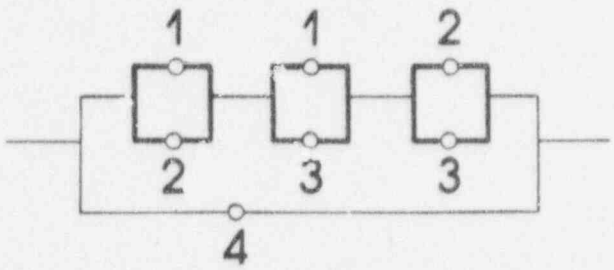
States 6 and 7 are absorbing which means that once the system enters either of these states, it cannot leave.

The plot of the expected number of system failures (obtained from IMPORTANCE) and system unreliability versus time (in units of μ) is shown in Figure 2-7.

For this system, $E\left[N_s(t)\right]$ is a good approximation to system unreliability for t less than about μ. Thus, if μ is large, this approximation is good for a long time into the future.

One advantage of the Markov approach is that it can handle cases in which repair is not statistically independent (e.g., repair cues). However, it may be

SAMPLE SYSTEM TO ILLUSTRATE BOUNDS



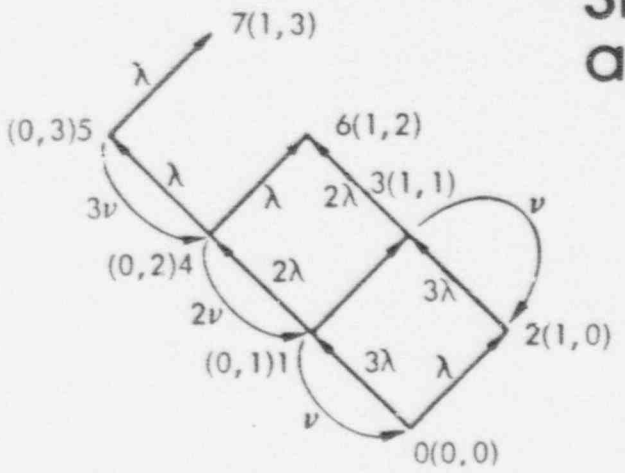
SAMPLE SYSTEM

τ_i = mean time to repair
μ_i = mean time to failure
$\gamma_i = 1/\tau_i$ = repair rate
$\lambda_i = 1/\mu_i$ = failure rate
let $\tau_i = .1\mu_i$ for i = 1, 2, 3

FIGURE 2-5

TRANSITIONAL STATE DIAGRAM FOR SAMPLE SYSTEM

States 6 and 7 are absorbing



EXPRESSION FOR SYSTEM UNRELIABILITY

$$\bar{F}_s(t) = P_6(t) + P_7(t)$$

FIGURE 2-6

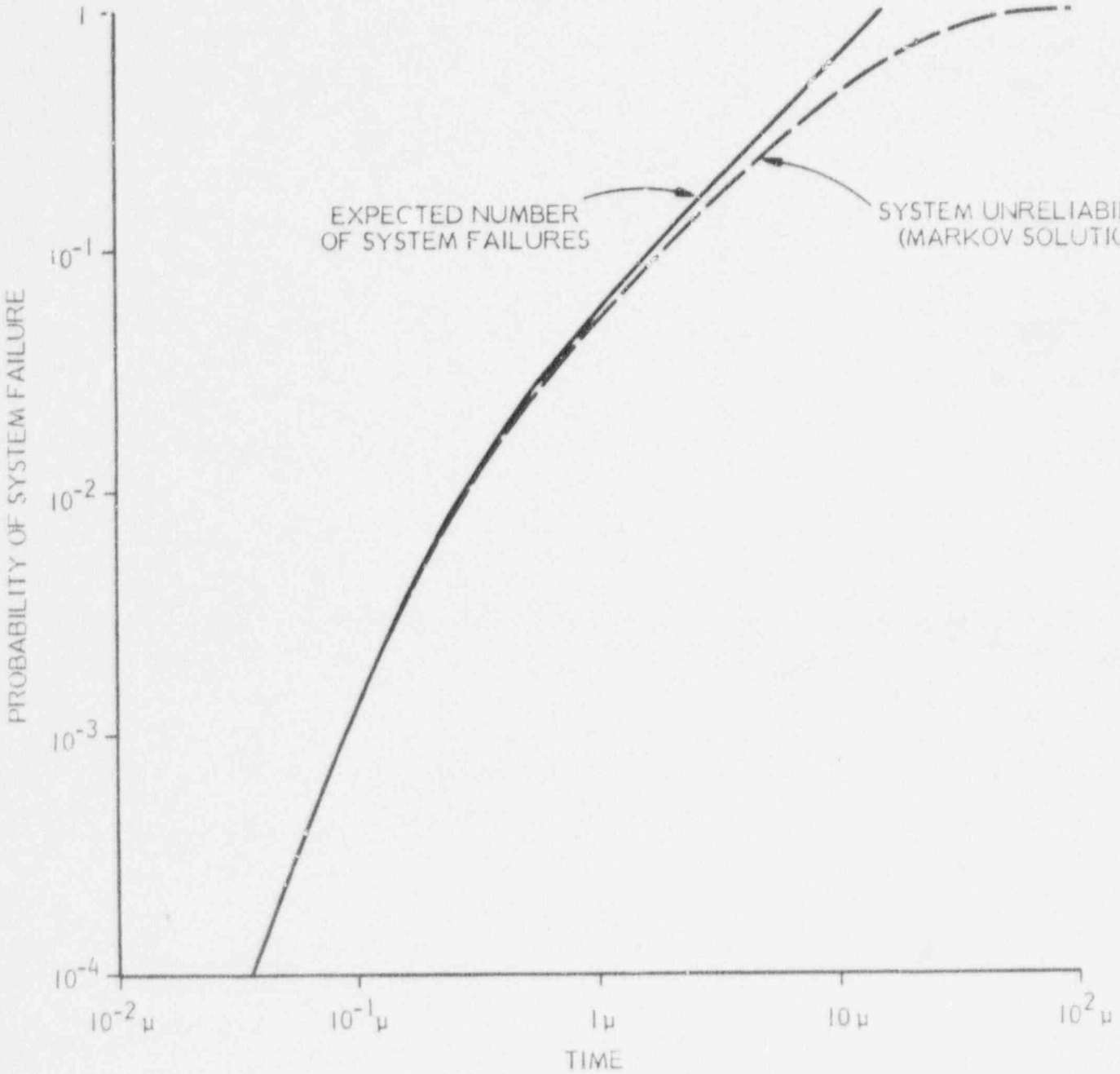


FIGURE 2-7

SYSTEM PERFORMANCE MEASURES
VERSUS TIME

argued that expensive land based facilities generally have several repairmen so that the assumption that repair is statistically independent (as is assumed in IMPORTANCE) is valid.

The disadvantage of the Markov approach is the exponentially increasing number of system states to be considered. The number of calculations to compute $E\left[N_s(t)\right]$ in IMPORTANCE, on the other hand, is of the order

$$2 \cdot NIE \cdot NCS$$

where

NIE = number of initiating events

NCS = number of cut sets

IMPORTANCE has performed with relative ease calculations involving 20,000 min cut sets and 80 components. These calculations took less than 0.2 CPU minutes on an IBM 370 computer.

2.9 USE OF SYSTEM PERFORMANCE MEASURES

1. For continuously operating systems for which failure cannot be tolerated (e.g., top events such as "fire," "explosion" or "inadvertant nuclear release") $E\left[N_s(t)\right]$ is the relevant measure of system performance.

2. When system failure can be tolerated, $g(\underline{q}(t))$, $\bar{F}_s(t)$, and $E\left[N_s(t)\right]$ all have relevance. For moderately large systems $\bar{F}_s(t)$ is difficult to calculate exactly, but if the system is reliable, $\bar{F}_s(t) \approx E\left[N_s(t)\right]$.

3. For standby systems, $g(\underline{q}(t))$, the probability that the system will fail upon demand is the relevant measure.

4. $E\left[N_s(t)\right]$ can be used in a financial measure of system performance. If C_i equals the cost of top event i*, and $E\left[N_{s,i}(t)\right]$ equals the expected number of occurrences of top event i, then maximizing system performance could be viewed as being equivalent to minimizing

$$\sum_i C_i \cdot E\left[N_{s,i}(t)\right] + C_{SYSTEM\ MOD}$$

where $C_{SYSTEM\ MOD}$ is the annualized cost of system modifications.

2.10 IMPORTANCE MEASURES

We now discuss the importance measures computed by IMPORTANCE. Importance measures assess the role that basic events or min cut sets play in either causing or contributing to the occurrence of the top event. They in general assign a probability value to each basic event or min cut set which allows these events to be ranked according to the extent of their contribution to the occurrence of the top event.

Importance measures can be categorized in two ways:

- Deterministically
- Probabilistically

Probabilistic measures in turn can be categorized in three ways:

- Birbaum's Measure (a partial derivative)
- Measures Weighted by Unavailability
- Measures Weighted by the Expected Number of System Failures (or event rate)

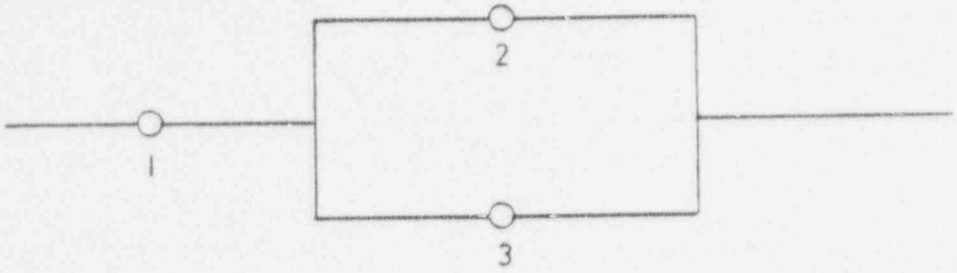
* Where top events include events such as "fire," "explosion," or "system shutdown."

DETERMINISTIC MEASURES

Deterministic measures assess the importance of a component to system operation without consideration to probability. One such measure is the structural measure of importance for component i which is defined as the number of critical system states for component i divided by 2^{n-1} (the total number of states for the n-1 remaining components). It is thus the fractional number of system states (for the n-1 remaining components) which are critical for component i.

The figure below gives an example of the calculation of structural importance.

SERIES-PARALLEL SYSTEM



FOR COMPONENT 1, STATES FOR THE OTHER 2 COMPONENTS	CRITICAL SYSTEM STATE FOR COMPONENT 1?
$(\cdot,2,3)$	NO
$(\cdot,\bar{2},3)$	YES
$(\cdot,2,\bar{3})$	YES
$(\cdot,\bar{2},\bar{3})$	YES

STRUCTURAL IMPORTANCE OF COMPONENT 1 = 3/4

FOR COMPONENT 2, STATES FOR THE OTHER 2 COMPONENTS	CRITICAL SYSTEM STATE FOR COMPONENT 2?
$(1,\cdot,3)$	NO
$(\bar{1},\cdot,3)$	YES
$(1,\cdot,\bar{3})$	NO
$(\bar{1},\cdot,\bar{3})$	NO

STRUCTURAL IMPORTANCE OF COMPONENT 2 AND 3 = 1/4

It can be shown that the structural measure of importance of component i equals

$$\Delta g_i(\underline{1/2}) = g(1_i, \underline{1/2}) - g(0_i, \underline{1/2}))$$

which is the expression used by IMPORTANCE to compute stuctural importance. For the series-parallel system above,

$$\Delta g_1(\underline{q}) = 1 - q_2 \; q_3$$

So $$\Delta g_1(\underline{1/2}) = 1 - 1/2 \cdot 1/2 = 3/4$$

and $$\Delta g_2(\underline{q}) = q_1(1 - q_3)$$

so $$\Delta g_2(\underline{1/2}) = 1/2(1 - 1/2) = 1/4$$

as obtained before.

We see that the above results substantiates what we intuitively know, i.e., that component 1 is more important than components 2 or 3. Structural importance can direct an analyst to areas where better basic event data should be obtained.

PROBABILISTIC MEASURES

We now discuss probabilistic measures of importance. One measure of importance is the criticality function (also called Birnbaums measure of importance) which is given by:

$$\Delta g_i(\underline{q}(t)) = g(1_i, \underline{q}(t)) - g(0_i, \underline{q}(t))$$

$$= \partial g(\underline{q}(t))/\partial q_i$$

as was discussed in Section 2.6.

This measure is not a function of the component's availability and by itself is not an extremely useful measure of importance. However, many of the remaining importance measures to be described can be defined in terms of Birnbaum's measure.

The next four measures, three of basic event importance and one of min cut set importance, are computed in terms of system unavailability. These measures are meaningful for systems whose components are:

(1) Non-repairable (in which case system unavailability equals system unreliability)

and (2) Repairable and whose top event is not catastrophic

(If the top event is catastrophic, repairing the failed components may not repair the system. For example, if the top event is "inadvertant detonation of a nuclear warhead," fixing the spark-gap switch which caused this event will not repair the system—there may not be a system left.) We will say that for systems satisfying (1) or (2), "system downtime" has meaning.

The measures, listed in Table 2-1, are weighted according to system unavailability, $g(\underline{q}(t))$. All three measures of basic importance yield the same ranking for reliable systems. These measures will be called importance measures of system unavailability. The upgrading function is applicable only to non-repairable systems. For this measure the proportional hazard, α, is defined by

$$F(t) = 1 - e^{-\alpha R(t)}$$

where $R(t)$ is the common hazard assumed to be shared by all system components. α can be thought of as simply a failure rate. As illustrated in Section 3.4, the upgrading function is a useful measure during the design stages of a system where data regarding repair times may not be available and only the relative failure rates are known.

TABLE 2-I

IMPORTANCE MEASURES OF SYSTEM UNAVAILABILITY

Measure	Probabilistic Expression	Interpretation
Criticality measure of basic event importance	$\frac{\Delta g_i(\underline{q}(t))\ q_i(t)}{g(\underline{q}(t))}$	Probability that the system is in a critical state for component i and i has failed *
Upgrading function of basic event importance	$\frac{\alpha i}{g(\underline{q}(t))} \cdot \frac{\partial g(\underline{q}(t))}{\partial \alpha i}$	Fractional reduction in the probability of the Top Event when α_i is reduced fractionally *
Fussell Vesely measure of basic event importance	$\frac{P\left(\bigcup_{i \in K_j} E_k\right)_j}{g(\underline{q}(t))}$	Probability of the union of the min cut sets containing basic event i *
Fussell Vesely measure of min cut set importance	$\frac{P(E_k)}{g(\underline{q}(t))}$	Probability of occurrence of min cut set E_k *

* Given system is in a failed state at time t.

The Fussell-Vesely measure of basic event importance is simply the probability of the union of all min cut sets containing the basic event given that the system has failed (i.e., the Top Event has occurred). The Fussell-Vesely measure of cut set importance is simply the probability of occurrence of the cut set weighted according to system unavailability.

The remaining three measures, two of basic event importance and one of cut set importance are given in Table 2-2. They are computed in terms of the criticality function and the failure frequency function and are weighted according to the expected number of system failures. They assess the contribution of a basic event or a min cut set to the occurrence of system failure over an interval of time and are called measures of interval reliability. The first measure, called the Barlow-Proschan measure, is the probability that an initiating event causes the Top Event to occur. This measure follows directly from the way the expected number of system failures was calculated in Section 2.6. The second measure, called sequential contributory, is the probability that an enabling event permits an initiating event to cause the Top Event. The index j in Table 2-2 runs over the initiating events which are contained in the same min cut set as enabling event i. This measure has meaning for basic events contained in min cut sets of order two or higher. The third measure of importance is called the Barlow-Proschan measure of cut set importance which is the probability that a min cut set causes system failure (given that failure has occurred). For a given min cut set to cause system failure, a basic event (which must be an initiating event) must have occurred and all other basic events in the min cut set must have failed at the time the initiating event occurs. The number of initiating events in a min cut set determine the number of ways a min cut set can fail.

For repairable systems, sequential measures of importance reach a steady state value.

To illustrate these measures, assume that a system has the three min cut sets of order two listed below:

$$\{A, B\}\ ,\ \{A, C\}\ ,\ \{B, C\}$$

TABLE 2-2

IMPORTANCE MEASURES OF INTERVAL RELIABILITY

Measure	Probabilistic Expression	Interpretation
Barlow-Proschan measure of basic event importance (initiator)	$\dfrac{\int_0^t \lvert g(1_i, \underline{g}(t')) - g(0_i, \underline{g}(t'))\rvert \; w_{f,i}(t')\,dt}{E[N_s(t)]}$	Probability that initiating event i causes system failure in $[0,t]$ *
Sequential contributory measure of basic event importance (enabler)	$\sum_{\substack{j \\ i \neq j \\ i \,\&\, j \in K_\ell \\ \text{for some } \ell}} \dfrac{\int_0^t \lvert g(1_i, 1_j, \underline{g}(t')) - g(1_i, 0_j, \underline{g}(t'))\rvert q_j(t') \, w_{f,i}(t')\,dt}{E[N_s(t)]}$	Probability that enabling event i permits an initiating event to cause system failure in $[0,t]$ *
Barlow-Proschan measure of min cut set importance	$\dfrac{\sum_{i \in K_\ell} \int_0^t [1 - g(0_i, \underline{1}_{K_\ell - \{i\}}, \underline{g}(t))] \prod_{\substack{j \neq i \\ j \in K_\ell}} q_j(t) \cdot w_{f,i}(t)\,dt}{E[N_s(t)]}$	Probability that a min cut set causes system failure in $[0,t]$ *

* Given that system failure has occurred in $[0,t]$

Assume that event C is an enabling event. Assume that q_i and λ_i are accurate steady state approximations to component unavailability and failure frequency. Furthermore, assume that the system is reliable.

The Top Event Rate, R, is (using the expressions given in (2-3), (2-5) and (2-6)):

$$R = \lambda_A q_B + \lambda_B q_A + \lambda_A q_C + \lambda_B q_C$$

Note that there are two ways that the first cut set can fail but only one way that the remaining two min cut sets can fail.

The expected number of system failures over an interval of time $[0,t]$ is simply $R \cdot t$. The probability that basic event A causes system failure (i.e., the Barlow-Proschan measure) is simply the expected number of times event A causes system failure divided by the expected number of system failures as given below:

$$\frac{(\lambda_A q_B + \lambda_A q_C)\, t}{(\lambda_A q_B + \lambda_B q_A + \lambda_A q_C + \lambda_B q_C)\, t}$$

Note that the above measure is an increasing function of λ_A, the failure frequency of event A. Thus to decrease a component's Barlow-Proschan measure of importance, its failure rate should be decreased. Increasing its repair rate (ν) does not decrease its Barlow-Proschan measure of importance. This is a general property in the ranking of initiators.

The sequential contributory importance of event C which is an enabling event is given by

$$\frac{(\lambda_A q_C + \lambda_B q_C)\, t}{(\lambda_A q_B + \lambda_B q_A + \lambda_A q_C + \lambda_B q_C)\, t}$$

Note that the above measure is an increasing function of q_C, the unavailability of the enabling event. Thus to decrease an enablers' ranking, its unavailability

should be decreased. This can be accomplished by decreasing its failure rate or by increasing its repair rate. This is a general property for the ranking of enablers.

The Barlow-Proschan, B-P, measure of cut set importance for min cut set $\{A,B\}$ is

$$\frac{(\lambda_A q_B + \lambda_B q_A)\, t}{(\lambda_A q_B + \lambda_B q_A + \lambda_A q_C + \lambda_B q_C)\, t}$$

For min cut set $\{B,C\}$, the B-P measure of cut set importance is

$$\frac{\lambda_B q_C\, t}{(\lambda_A q_B + \lambda_B q_A + \lambda_A q_C + \lambda_B q_C)\, t}$$

The above calculations assume that when a min cut set ocurs, it causes system failure. This assumption is not true for redundant systems in which several min cut sets can fail when an initiating event occurs. In this case, one would use the expressions in Table 2-2 which uses the criticality function which takes this possibility into account.

Because the criticality function is used to compute (1) event rate and (2) importance rankings for min cut sets, the following statements are true:

- Sum of basic event initiating rankings equals unity.
- Sum of B-P measure of min cut set importance is equal to or exceeds unity.
- Sum of enabler rankings may exceed unity.

The above statements are obvious when we consider the following system with two min cut sets

$$\{1,2\} \qquad \{1,3\}$$

where basic events 2 and 3 are enabling events only. If we fix the state of basic event 1, there are four remaining system states:

System State	Component State 2	Component State 3	Critical System State for 1
1	Work	Work	no
2	Fail	Work	yes
3	Work	Fail	yes
4	Fail	Fail	yes

System state 4 has the characteristic that when component 1 fails, both min cut sets cause the system to fail, and both basic events 2 and 3 enable component 1 to cause system failure. In the min cut set rankings and enabler rankings, system state 4 is counted in both rankings. For this reason, the sum of these rankings exceed unity.

3.0 INSTRUCTIONS ON THE USE OF IMPORTANCE

We now summarize from Section 2.0 the calculations of IMPORTANCE. By use of an illustrative example, we describe the computer code input, the options available and interpret the output and give some useful engineering guidelines on the use of IMPORTANCE. In the last section we describe information necessary in using SETS with IMPORTANCE.

3.1 GENERAL SUMMARY

The computer code, IMPORTANCE, computes various Top Event characteristics and measures of probabilistic importance of basic events and cut sets of a fault tree. The code requires as input the minimal cut sets (obtained from SETS), the failure rates and the fault duration times (i.e., the repair times) of all basic events contained in the min cut sets. The failure and repair distributions are assumed to be exponential. The code can compute seven measures of basic event importance and two measures of cut set importance. All measures are computed assuming statistical independence of basic events.

The Top Event time dependent characteristics generated by the code include:

- System Unavailability g (q(t))
- Expected Number of System Failures $E[N_S(t)]$

In addition, for repairable systems with asymptotic Top Event rate greater than zero, the code computes the following Top Event Characteristics:

- Limiting System Unavailability
- Top Event Rate
- Mean Time to System Failure
- Mean Duration Time for the Top Event

These characteristics are computed when the Barlow-Proschan (initiator) measure of basic event importance is computed.

The measures of importance which the code computes are shown in Table 3.1. The notation used is that of Section 2. Each measure can be calculated for both time dependent and asymptotic component unavailability. The only exception is the upgrading function which must be calculated in terms of the time dependent unavailability of non-repairable components.

As shown in the list of expressions in Table 3-1, the measures that depend upon one point in time are conditioned on the system unavailability, $g(\underline{q}(t))$. These measures should be used only when system downtime has meaning. The measures which are time integrated quantities depend upon the sequences of events leading to system failure and are conditioned on the expected number of system failures, $E\left[N_s(t)\right]$. Initiating and enabling events must be identified in the analysis. When repair is not allowed, $g(\underline{q}(t))$ equals $E\left[N_s(t)\right]$. When repair is allowed, $g(\underline{q}(t))$ does not depend upon any previous sytem state as does $E\left[N_s(t)\right]$. The time integrated measures of importance when divided by $E\left[N_s(t)\right]$ approach an asymptotic value for large time when asymptotic Top Event Rate is greater than zero.

Two options in the code allow calculations to be performed using asymptotic (steady state) probabilities. In this case the expected number of system failures is equal to the top event rate (a constant) times mission time. Importance measures in this case assess the contribution of the occurrence of the basic events or min cut sets to the Top Event rate.

3.2 OPTIONS TO THE CODE

Four options are allowed when using the code. The first option, Option 1, computes measures of importance as a function of time. The input data required are the points in time for which the measures are to be computed. The basic event data, i.e., the failure rates and repair times, are expressed in time units (e.g., per hour or hours). The second and third options, Options 2 and 3, compute the measures of importance as a function of the probability of the top event. These options do not permit repair. The second option requires the failure rates to be given in time units. The third option allows failure rates to be expressed proportionally (i.e., when proportional hazards are assumed). These options also require as input the probabilities of the top event for which the measures are

TABLE 3-1

IMPORTANCE MEASURES COMPUTED IN IMPORTANCE COMPUTER CODE

	Basic Event Measure	Expression
1.	Structural	$g(1_i, \underline{1/2}) - g(0_i, \underline{1/2})$
2.	Birnbaum	$\frac{\partial g(\underline{q}(t))}{\partial q_i(t)} = g(1_i, \underline{q}(t)) - g(0_i, \underline{q}(t))$
3.	Criticality	$\frac{(g(1_i, \underline{q}(t)) - g(0_i, \underline{q}(t)) \quad q_i(t)}{g(\underline{q}(t))}$
4.	Upgrading Function	$\frac{\alpha_i}{g(t, \underline{\alpha})} \cdot \frac{\partial g(t, \underline{\alpha})}{\partial \alpha_i}$
5.	Fussell-Vesely	$\frac{P\left(\bigcup_{j \; i \in K_j} E_{k_j}\right)}{g(\underline{q}(t))}$
6.	Barlow-Proschan (Initiator)	$\frac{\int_0^t \{ g(1_i, \underline{q}(t')) - g(0_i, \underline{q}(t')) \} \cdot w_{f,i}(t') \, dt'}{E[N_s(t)]}$

TABLE 3-1

(CONT.)

Basic Event Measure	Expression
7. Sequential Contributory (Enabler)	$\sum_{\substack{j \\ i \neq j \\ i \,\&\, j \in K_\ell \\ \text{for some } \ell}} \frac{\int_0^t \left\{ g(1_i, 1_j, \underline{q}(t')) - g(1_i, 0_j, \underline{q}(t')) \right\} q_i(t') \, w_{f,j}(t') \, dt}{E\left[N_S(t)\right]}$

Cut Set Measure	Expression
1. Barlow-Proschan	$\sum_{i \in K_\ell} \frac{\int_0^t \left[1 - g(0_i, \underline{1}^{K_\ell - \{i\}}, \underline{q}(t))\right] \prod_{\substack{j \neq i \\ j \in K_\ell}} q_j(t) \; w_{f,i}(t) \, dt}{E\left[N_S(t)\right]}$
2. Fussell-Vesely	$\frac{\prod_{i \in K_\ell} q_i(t)}{g(\underline{q}(t))}$

computed. Option 4 is like Option 1 except that the basic event data is inputted in terms of the mean time to failure instead of the failure rate.

The computer output consists of a series of tables listing the measures of importance in descending order as a function of the data input (i.e., time or the probability of the top event).

Figure 3-1 shows the SETS-IMPORTANCE interface. The SETS input consists of (1) THE SETS user program which describes the commands necessary to generate the min cut sets and (2) the fault tree description. [2] SETS generates the output on file no. 2. In addition, SETS generates file no. 9 which contains the min cut sets in "packed" form and other information necessary to run IMPORTANCE.

IMPORTANCE reads two input files:

- File 9 generated from SETS
- File 5 supplied by the user which contains (1) options employed in IMPORTANCE and (2) the basic event data.

As described in Section 3.5, the information contained on file 9 will indicate if the min cut sets can be stored within the array bounds set by IMPORTANCE. Also, a check is performed to see if complemented events are contained within the min cut sets. (These events must be eliminated in SETS before IMPORTANCE is run.)

On file 5, the user supplies the input regarding options employed and the basic event data. Section 3.3 describes how to generate this input data.

3.3 IMPORTANCE INPUT

The following describes the IMPORTANCE input card sequence.

1. Title card - The title can be up to 80 alphanumeric characters and should begin somewhere in columns 1-8 (column 5 is best in terms of centering the title on the output).

2. Option card - A 1, 2, 3 or 4 in column 10 assigns a value to IDATA, and a 0 or 1 in column 20 assigns a value to ITDEP. The meaning of these values is given below.

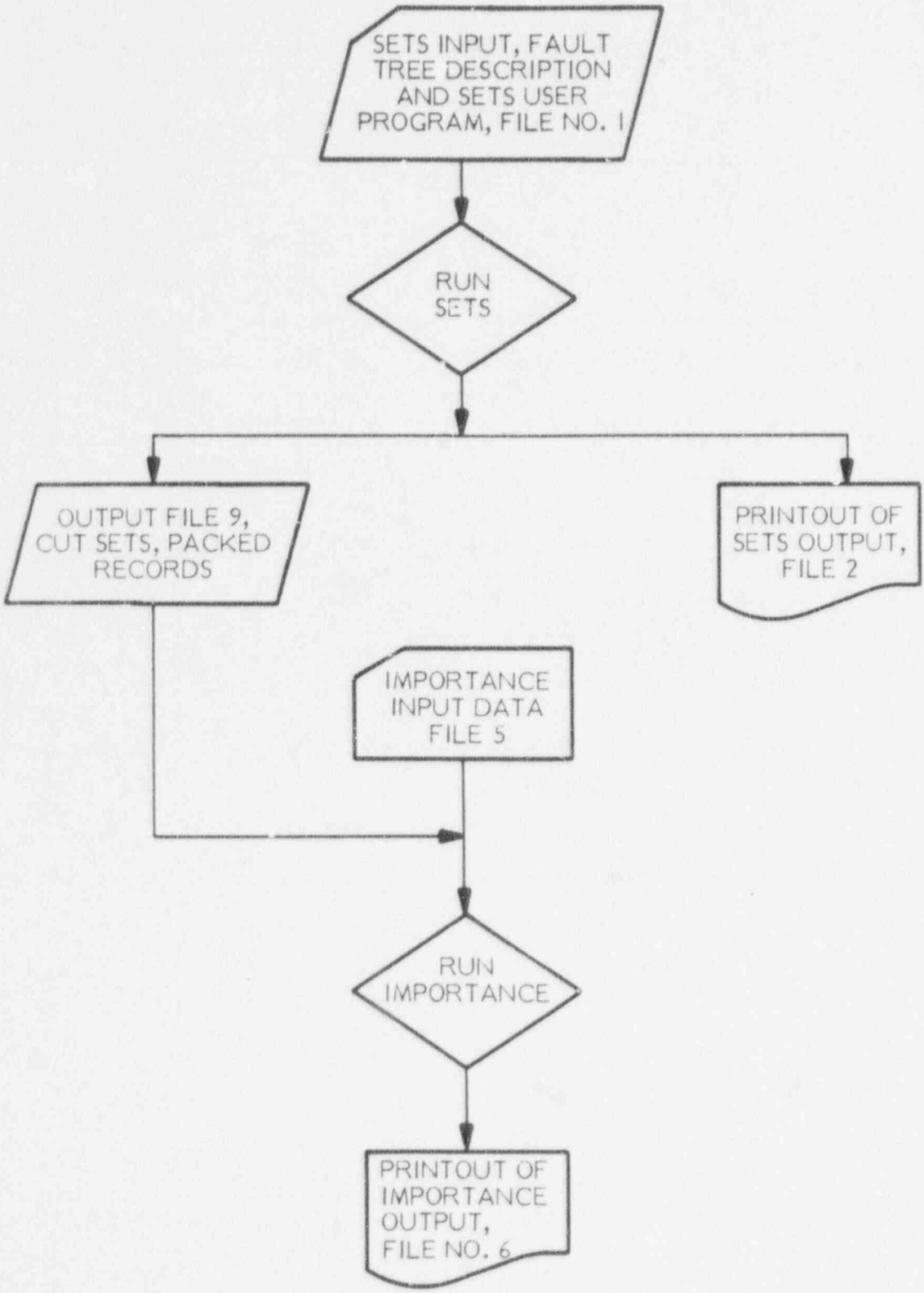


FIGURE 3-1

SETS-IMPORTANCE INTERFACE

(PTOP = Probability of the top event)

IDATA	Inputted Component Data	Importance Measures Outputted as a function of:
1	Failure rate, Mean fault duration	Time
2	Failure rate (No repair allowed)	PTOP
3	Proportional Hazard (No repair allowed)	PTOP
4	Mean time to failure, Mean fault duration	Time

ITDEP	Interpretation
0	Asymptotic (steady-state) values for component unavailability will be used in all calculations. One importance value will be calculated for each component for each importance measure invoked.
1	Time dependent expressions for component unavailability will be used in all calculations. Importance values will be calculated at each inputted point.

ITDEP has relevance only for Options 1 and 4.

3. Number of data points card - A 1, 2, 3, . . ., or 8 in column 10 assigns a value to NTPT which stands for the number of time points or probabilities of the top event at which importance measures will be calculated (depending on whether IDATA = 1 or 4, or, 2 or 3). (If ITDEP = 0, NTPT gives the number of time points at which the expected number of system failures will be calculated.)

4. Data points card - The data points (NTPT of them) should be typed in according to format 8 (E9.3, 1X), if IDATA = 2 or 3, or according to format 8 (E9.3, A1), if IDATA = 1 or 4. In the latter, the A1 position in columns 10, 20, etc., should contain an H, D, M or Y, depending on whether the corresponding time point is in terms of hours, days, months or years (respectively). This format allows between 1 and 8 data points.

5. Importance measure selection cards - Any subset (in any order) of the following list of cards may be included.

Card		Importance measure selected
col. 1 ↓		Measures of component importance
BE	BRNBM	Birnbaum
BE	CRTCL	Criticality
BE	FV	Fussell-Vesely
BE	INIT	Initiator (Barlow-Proschan)
ENABLER		Enabler (Sequential Contributory)
BE	STRUC	Structural
BE	UPGRF	Upgrading function

		Col. 20 ↓	Measures of cut set importance
CS	FV	xx	Fussell-Vesely
CS	INIT	xx	Initiator (Barlow-Proschan)

For the two cut set measures, if it is desired that a maximum cut set order be imposed on the calculations, the maximum cut set order should be typed in, ending in column 20.

A card typed ENDIM (starting in col. 1) must immediately follow the importance measure selection cards.

6. Multiple option cards - Two cards, called the DETAILCS and TABLE determine the number of min cut sets which will be printed. An example of these three cards plus a NOPTION card (which must follow these cards) is given below:

column	1	2Ø	3Ø
	DETAILCS	5	.1
	TABLE		
	NOPTION		

On the first card three variables are read, DETAILCS, NM and FACTOR with format (A8, 2X, I1Ø, F1Ø.5). In the example NM = 5 and FACTOR = .1. NM and FACTOR have the following interpretation. If MAX equals the largest importance value of all the cut sets, the number of cut sets which the code will (in the output) describe in detail (by printing the full description of the basic events in them) equals the minimum of NM and the number of cut sets whose importance values lie between MAX and FACTOR * MAX. If the DETAILCS card is deleted, then the code will assign to NM and FACTOR the default values of

- NM = 1ØØ
- FACTOR = .ØI

The DETAILCS card should be omitted if cut set measures are not invoked.

The second card with the name TABLE starting in column 1 indicates that min cut sets will be printed with 8-character basic event names at the end of the IMPORTANCE output. If the TABLE card is omitted, then the maximum number of cut sets which will be printed is 500. The TABLE card should not be included if cut set measures are not invoked.

The last card with the name NOPTION starting in column 1 indicates the end of the group of these cards. The NOPTION card must be included.

7. Basic event data cards - The format of these cards is as follows.

Columns 1-16 contain the name of the basic event (or the component).

Columns 21-29 contain the failure rate, proportional hazard or mean time to failure (with format E9.3) depending on the value of IDATA. Column 30 contains the symbol for the corresponding units (either H, D, M or Y) unless columns 21-29 contain a proportional hazard in which case column 20 is left blank.

Columns 31-39 contain the mean fault duration (with format E9.3) if IDATA = 1 or 4 and are left blank if IDATA = 2 or 3. Column 40 contains the units for the mean fault duration (H, D, M or Y) if IDATA = 1 or 4 (blank otherwise). Columns 31-40 should be left blank if the component is non-repairable.

Column 41 contains an asterisk if the basic event is an enabler event (blank otherwise). The probability of the enabling event is constant and is given by the product of LAMBDA and TAU.

Columns 43-80 contain a description of the basic event.

Another way of inputting a constant probability event is to type 0.0 somewhere in columns 21-29 and to type the probability (i.e., a number between 0 and 1) in columns 31-39 (according to a E9.3 format). (Columns 30 and 40 should be left blank.)

A constant probability event is always treated as an enabling event.

An NDATA card must immediately follow the Basic Event Data Cards.

Following the NDATA card must be a SETS card which indicates to IMPORTANCE that the min cut sets will be read from file no. 9. (If the SETS card is deleted, then IMPORTANCE will read a file generated by the computer code "Fault Tree Analysis Program" (FTAP) (12) which contains the min cut sets. A description of the use of IMPORTANCE with FTAP is contained in the user's manual entitled "The Fault Tree Computer Codes IMPORTANCE and GATE."

8. Before running IMPORTANCE, the user should check his input to verify that four lines exist in the input with the following characters:

Column 1

ENDIM
NOPTION
NDATA
SETS

9. The restrictions on the data input for each of the options are described below.

Restrictions on Data Input

Option	LAMDA	TAU
1	Failure rate expressed in time units	Repair time expressed in time units
2	Failure rate expressed in time units	Repair time must be 0 or left blank (convention indicating repair not allowed)
3	Proportional hazard rate	Repair time must be 0 or left blank
4	Lamda in this case is not a failure rate but is the reciprocal, mean time to failure.	Repair time expressed in time units

A useful feature of IMPORTANCE is that the number of basic event names in the input can exceed the number of basic events in the min cut sets. Hence a universal library of basic event data can be used.

3.4 PRESSURE TANK EXAMPLE

We use the system described below to generate a fault tree by the digraph (directed graph) fault tree technique. We run SETS to perform the qualitative analysis, identify the enabling and initiating events, and run IMPORTANCE to perform the quantitative analysis. The concepts presented in this example can be directly extended to analysis of control systems and generally to concepts of interval reliability.

System Description

The system given in Figure 3-2 discharges gas from a reservoir into a pressure tank. The pumping cycle is initiated by an operator who manually resets a timer which causes the timer contacts to close and the pump to start. The switch is

PRESSURE TANK SYSTEM

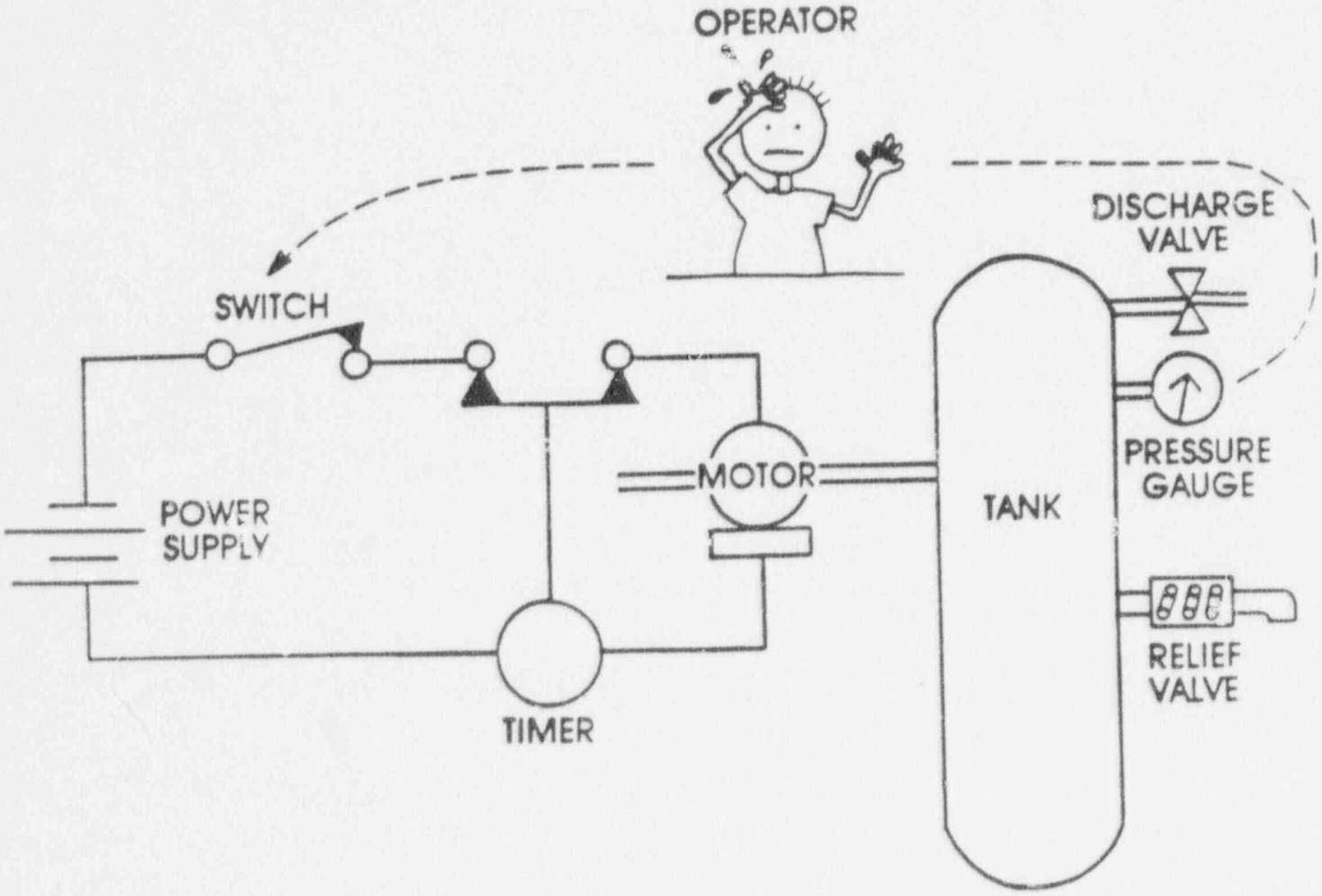


FIGURE 3-2

PRESSURE TANK SYSTEM

normally closed. At a prescribed time later (well before any overpressure condition can exist), the timer times out and the timer contacts open. Current is denied to the pump and pumping ceases. If the timer contacts do not open, the operator will notice the tank pressure by the pressure gauge becoming too high and he will open the switch. Again current is denied to the pump and pumping should cease. It is assumed that after each cycle, the compressed gas is discharged by opening the valve. It is also assumed that the valve is closed before the next cycle begins.

System Digraph

The system digraph is an intermediate step in the construction of the fault tree. It is a multivalued logic model that depicts the interrelationship of system variables. The system digraph with Top Event variable, tank pressure is shown in Figure 3-3. The Top Event of concern is pressure tank rupture. There are two feedback loops indicated by bold cyclic lines in the digraph. The function of these loops is to counteract the effect of the disturbance "timer contacts fail to open" which causes the pump motor to continue operating which results in overpressure. There are two loops:

- The operator sensing indicated pressure and opening the switch if pressure is too high
- Pressure relief valve opening in the event of excess pressure

Events which inactivate the loops are called zero gain events and appear as basic events in the fault tree.

Fault Tree

A fault tree with Top Event "Pressure Tank Rupture" is presented in Figure 3-4. The events are coded in the tree according to an alphanumeric scheme useful for input into SETS. There are two initiating events that can cause the Top Event to occur:

DIGRAPH FOR PRESSURE TANK RUPTURE

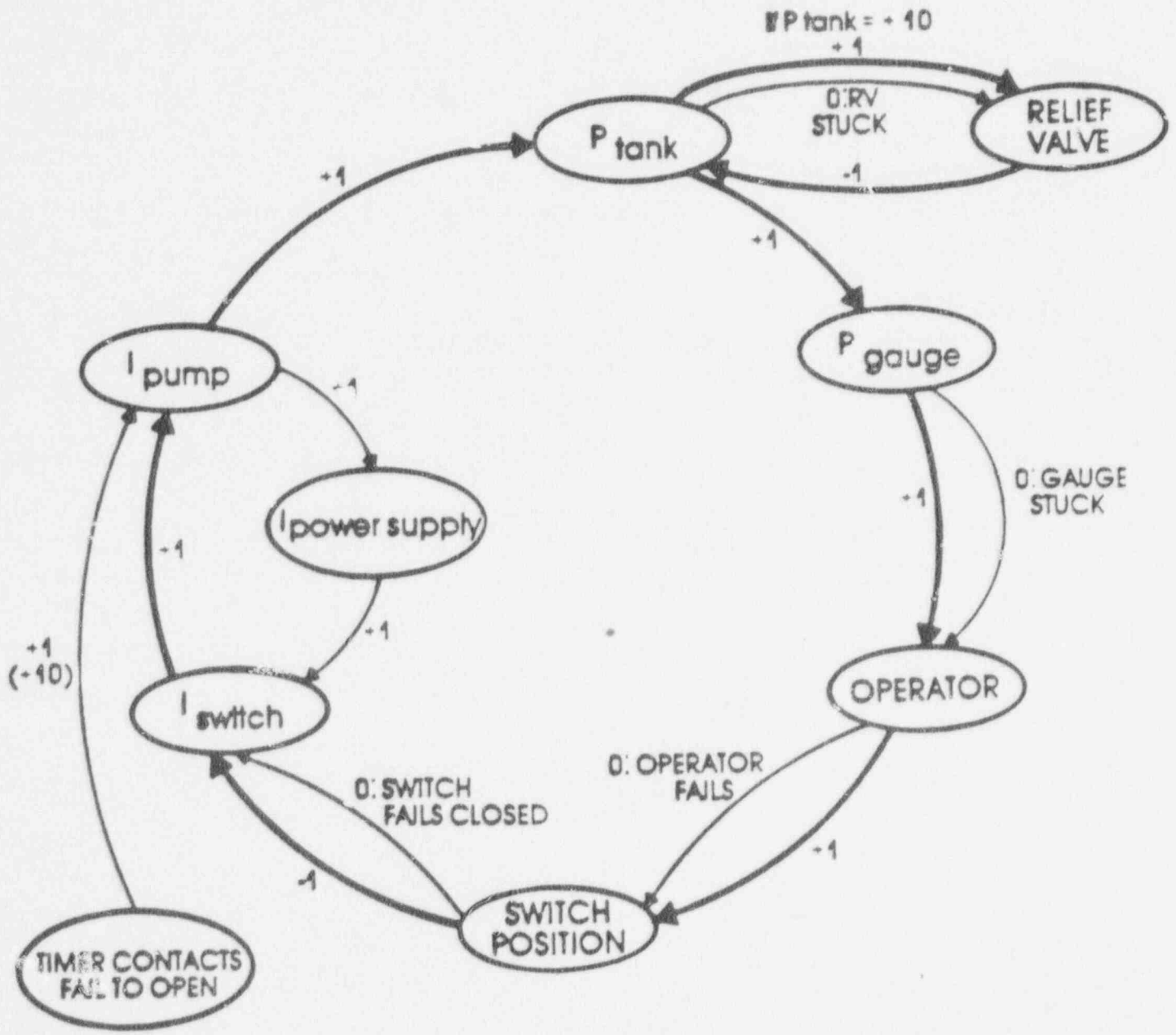


FIGURE 3-3

DIGRAPH FOR
PRESSURE TANK RUPTURE

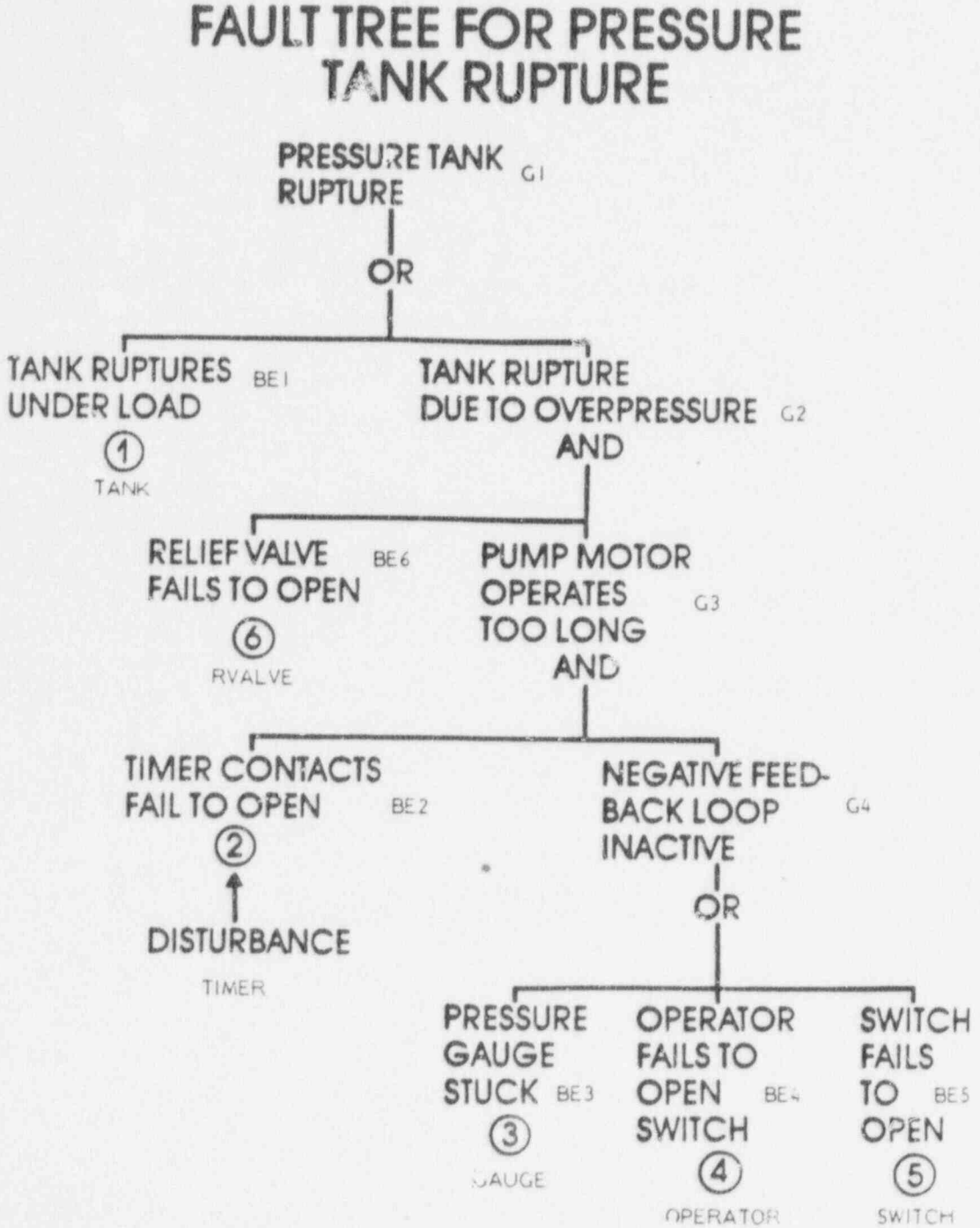


FIGURE 3-4

FAULT TREE FOR PRESSURE TANK RUPTURE

- Pressure tank ruptures under load
- Timer contacts fail to open

In the case of the second initiating event, the two loops must fail in order for the tank to rupture due to overpressure, i.e., gate events BE6 and G4 must occur.

Input/Output to SETS

The coded input to SETS is shown in Figure 3-5. The input consists of two parts:

- The SETS user program
- The fault tree specification

Note that the SETS user program must contain the command "WRTEQNDNF" in order to generate file 9, the input file to IMPORTANCE. The printed output for SETS is on file no. 2 a portion of which is displayed in Figure 3-6. This file displays 4 min cut sets (i.e., terms), one of order 1 and three of order 3.

USE OF IMPORTANCE

As indicated in Figure 2-1, basic event data is required to run IMPORTANCE (except for the structural measure). We will run the pressure tank example under two hypothetical sets of circumstances--both are encountered in practice.

- We are in the design stages of the system and failure and repair data is not known. We will assume that system components are not repairable.
- We have operated this system and have obtained data concerning failure and repair (or know failure data from data handbooks). Explosion of the tank is a recognized hazard.

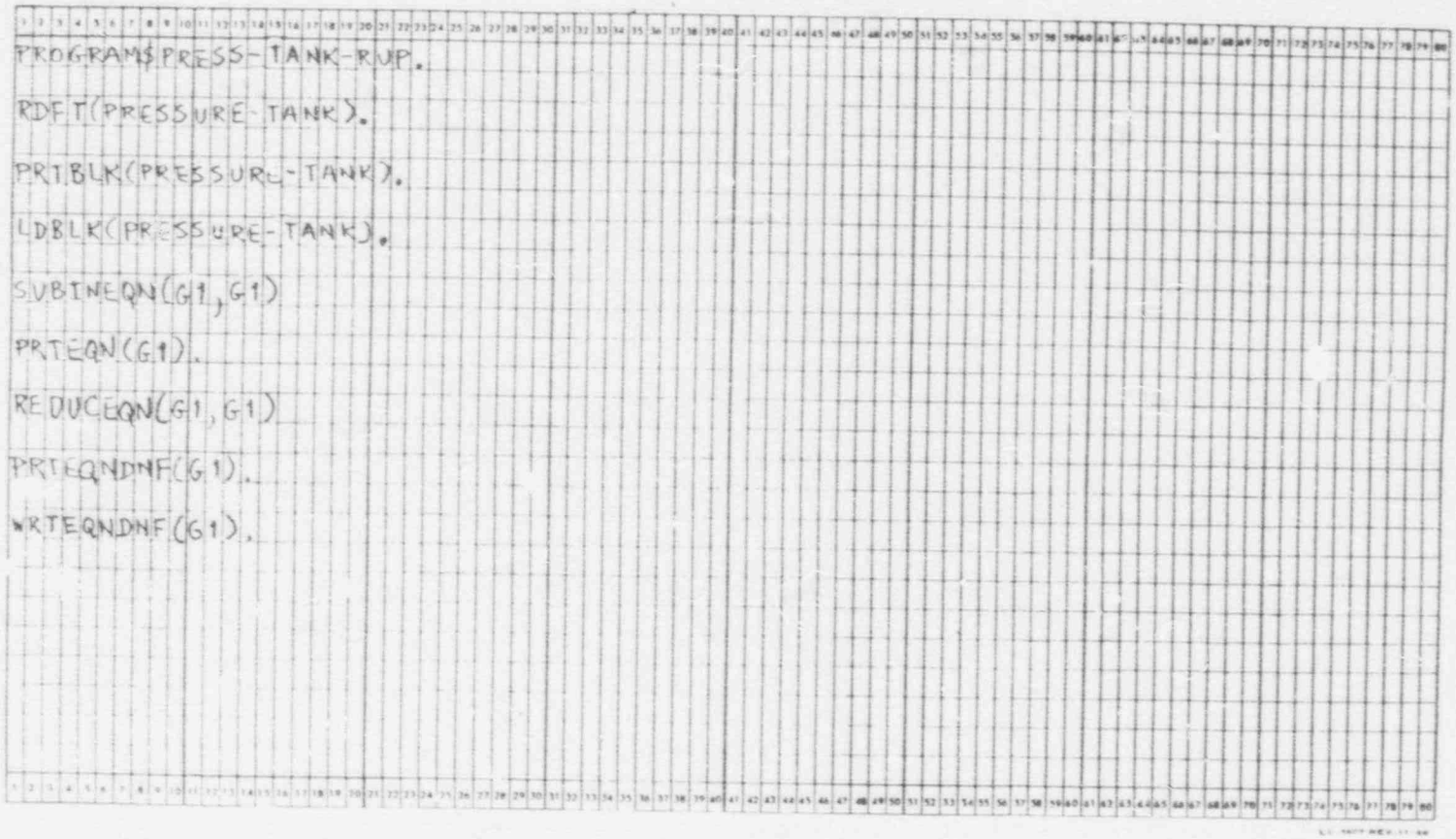


FIGURE 3-5
SETS INPUT

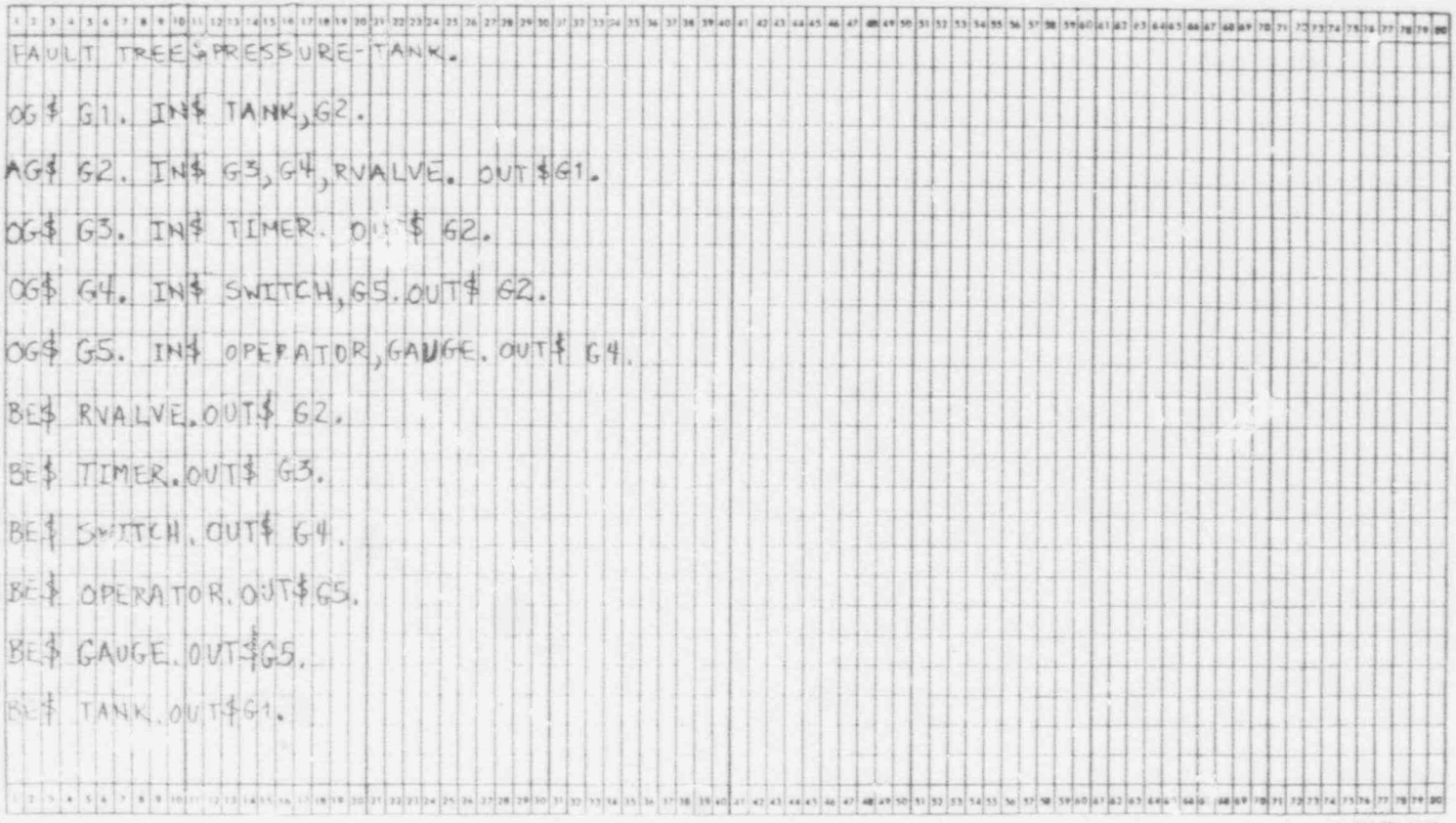


FIGURE 3-5

(CONT.)

```
* * * * LITERAL OCCURRENCE TABLE * * * *

                                NUMBER OF                    NUMBER OF
        LITERAL                 OCCURRENCES   OPPOSITION     OCCURRENCES
                                              LITERAL

        TANK                        1
        RVALVE                      3
        TIMER                       3
        SWITCH                      1
        OPERATOR                    1
        GAUGE                       1

    THERE ARE   6 DIFFERENT LITERALS IN THE
    SET EQUATION FOR G1

  TERM   NUMBER OF
NUMBER   LITERALS

                        G1 =

    1          1        TANK *

    2          3        RVALVE * TIMER * GAUGE +

    3          3        RVALVE * TIMER * OPERATOR +

    4          3        RVALVE * TIMER * SWITCH
```

FIGURE 3-6

SETS OUTPUT
FORTRAN FILE 2

In the first case the concept of proportional hazards is useful. We could for example obtain estimates of the relative failure rates as listed below with a fair degree of confidence.

	Event	Proportional Hazard
1.	Tank Ruptures Under Load	.001
2.	Timer Contacts Fail to Open	1.
3.	Gauge Reads Low or Stuck	10.
4.	Operator Fails to Open Switch	100.
6.	Relief Valve Fails to Operate	10.

The above data implies for example that the timer contacts failing to open is 1000 times more likely than the tank rupturing under load but 100 times less likely than the operator failing to open the switch.

Further we will estimate the median probability of system failure as 10^{-4} with 90 percent confidence limits estimated to be 10^{-6} and 10^{-2}. We consider this interval to see if there is any change in the importance rankings as the probability of the Top Event increases (or as time increases).

For systems in the design stages useful measures to be run include:

- Structural measure of basic event importance
- Upgrading function
- Fussell-Vesely measure of cut set importance

Option 3 in IMPORTANCE should be run since we have proportional hazards as input and we are obtaining the above measures as a function of the probability of

the Top Event. The input to IMPORTANCE is shown in Figure 3-7. The first line is the Title card. The second line indicates that we want Option 3 which implies that proportional hazards are the input for basic event data and that importance measures will be computed at the inputted values for the probability of the Top Event.

The third line indicates that three data points are given on the fourth card--in this case three values for the probability of the Top Event. The next three cards indicate that the structural measure of basic event importance, the upgrading function and the Fussell-Vesely Measure of cut set importance is to be computed for cut sets up to order 3. Following these cards are the ENDIM and NOPTION cards. The basic event data appear in the last set of cards followed by an NDATA and SETS card. The input in Figure 3-7 and file 9 generated by SETS are the two input files to IMPORTANCE. The output file is shown in Apperdix A.

Page A-1 of Appendix A clearly displays the option selected by the user and the importance measures to be calculated. Page A-2 displays the input data which the user should carefully check for errors. Page A-3 lists the number of system states (2^{NBE-1}, where NBE equals number of basic events), and the structural measure of importance for each basic event. This measure ranks the basic event "tank rupture under load" as the most important event. Some of the other structural rankings are counter intuitive--for example the operator is ranked as being of equal importance as the switch and pressure gauge.

We now consider probabilistic measures for basic events and min cut sets. Pages A-4 and A-7 confirm the importance of the tank rupturing under load for reliable systems. However, as the system becomes less reliable, the active components including the timer, relief valve and operator become more important than the pressure tank rupturing under load. Also the probabilistic measures show that the operator is always more important than the switch or pressure gauge.

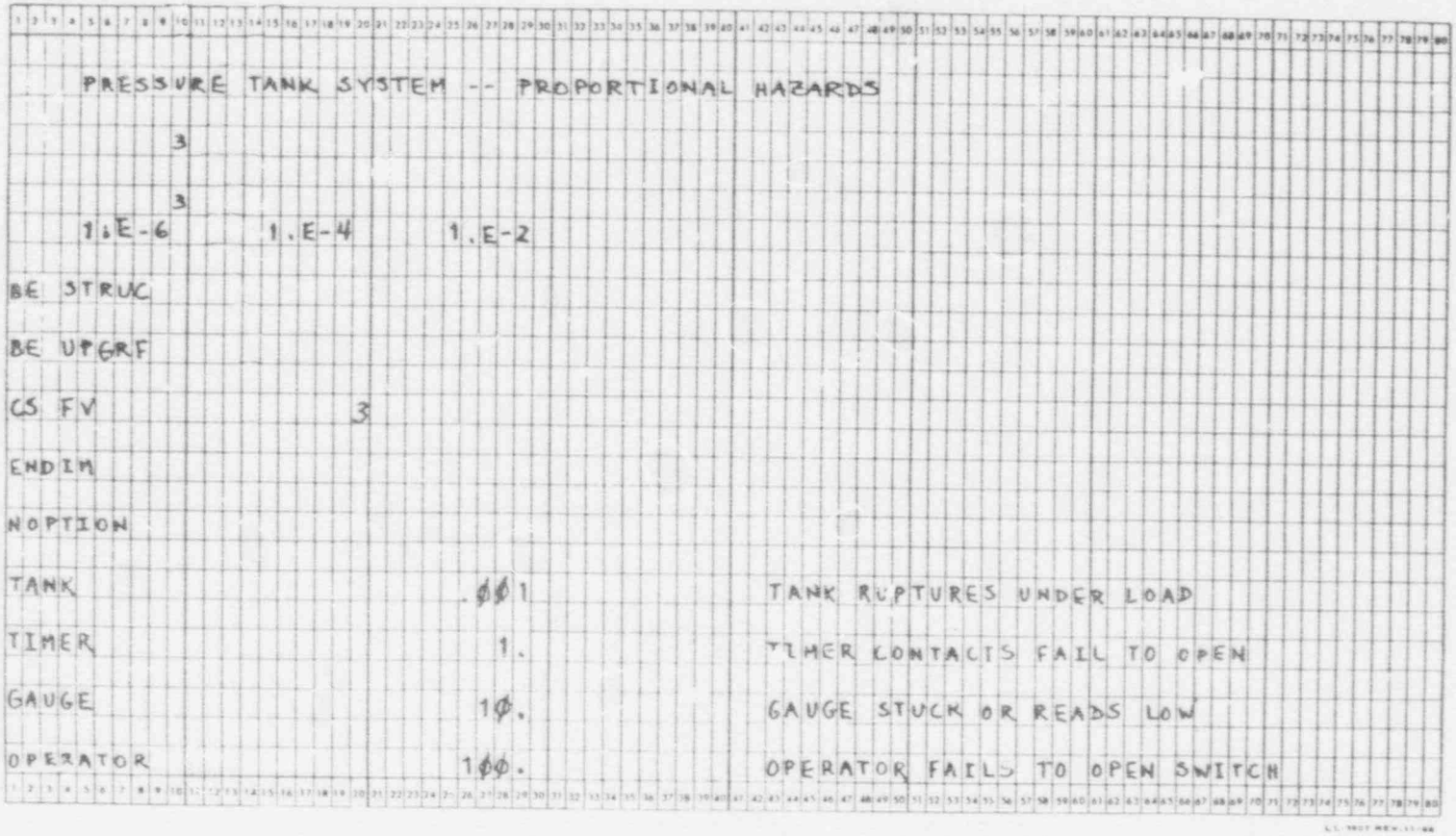


FIGURE 3-7
IMPORTANCE INPUT

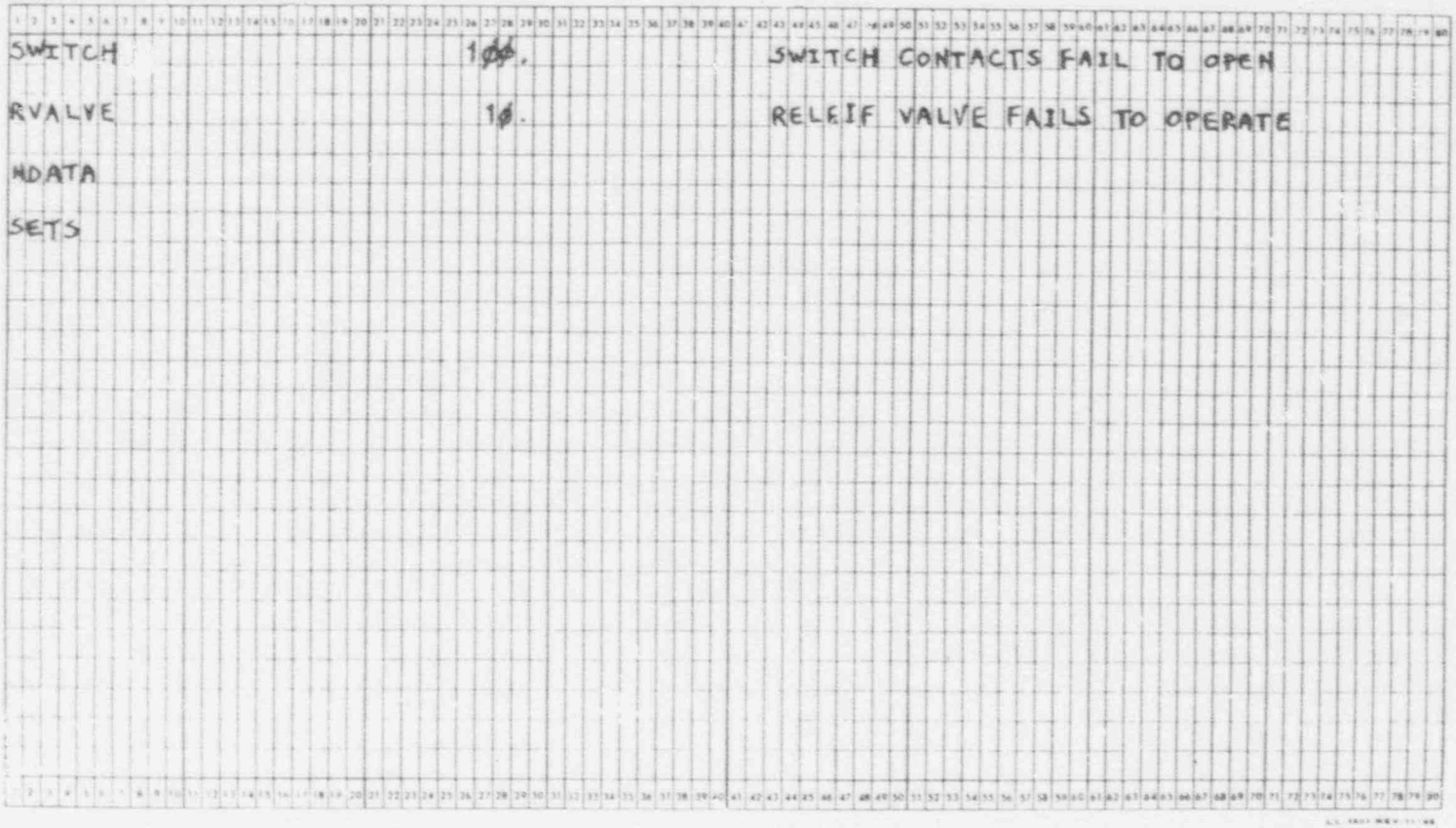


FIGURE 3-7

(CONT.)

Now we consider the pressure tank system under the second set of circumstances stated above in which we have actual operating data.

Explosion of the tank is recognized as a potential hazard to personnel. Figures of merit based on concepts of interval reliability are particularly relevant. If the explosion of the tank is not a totally intolerable event, we may also be interested in system downtime and figures of merit based on concepts of system unavailability.

Calculating system unavailability for secondary failure events, such as tank rupture due to overpressure, requires special treatment. The three min cut sets of order three in Figure 3-6 cause overpressure which causes the pressure tank to rupture. Repairing the system, however, involves more than repairing the components in whatever min cut set caused the overpressure to exist--the pressure tank itself must also be repaired. In general, this is true of any min cut set which causes a secondary failure of a component.

To conservatively account for the repair of the tank we can simply add the repair time of the initiating event (in this case the timer) and the repair time of the tank to obtain a pseudo repair time for the initiating event. This approach works when running IMPORTANCE if there is one initiating event per minimal cut set. If there are two or more events which can function as initiating events in a minimal cut set then the repair time of the secondary failure (the tank rupture) should only be added to the repair time of whichever event is acting as the initiating event in the occurrence of the minimal cut set. The current version of IMPORTANCE cannot handle differing repair times for initiating events but could be modified relatively easily.

If we do not modify the repair time of the initiating event as stated above, we will overestimate the Top Event rate. This overestimation is acceptable for interval reliability analyses of catastrophic system events.

For the pressure tank system we will assume that there is one operating cycle per hour. At the end of each 8-hour operating shift, the operator inspects the

switch and pressure gauge. (We will assume perfect inspection.) It takes 18 hours on the average to repair or replace either the switch or pressure gauge. The pressure relief valve is inspected yearly. We will assume that failure rate data is available from plant data and that it is as listed below.

Basic Event	Failure Rate*	Fault Duration
Tank	10^{-8}/hr	1 month
Timer	10^{-5}/hr	1 month
Pressure Gauge	10^{-4}/hr	22 hours *
Operator	10^{-2}/demand	----
Switch	10^{-5}/hr	22 hours *
Relief Valve	10^{-4}/hr	.5 years

* Θ = 8 hours, τ = 18 hours

where Θ equals inspection interval and τ equals repair time. The repair time of one month for the timer follows from the previous discussion, i.e., the timer is an initiating event which causes tank rupture and so the tanks' repair time is added to the timers'. The other initiating event is the tank rupturing under load. All other events are enabling events and are conditional on the occurrence the initiating event "timer contacts fail to open" when the initiating event causes the Top Event to occur. The input to IMPORTANCE for this example is shown in Figure 3-8.

The second line of Figure 3-8 indicates that Option 1 will be used and that steady state calculations will be performed. Line 3 shows that there are two mission time points--10 hours and 30 years as given on line 4. The units H, D, M and Y for hours, days, months and years are allowed. The next group of cards indicates that we will be computing the following measures of basic event importance:

- Fussell-Vesely (system unavailability weighting)
- Initiator (Barlow-Proschan)
- Enabler (sequential contributory)

---

* Note that the parameter, mean time to failure, which is the reciprocal of failure rate can also be used as input data for IMPORTANCE.

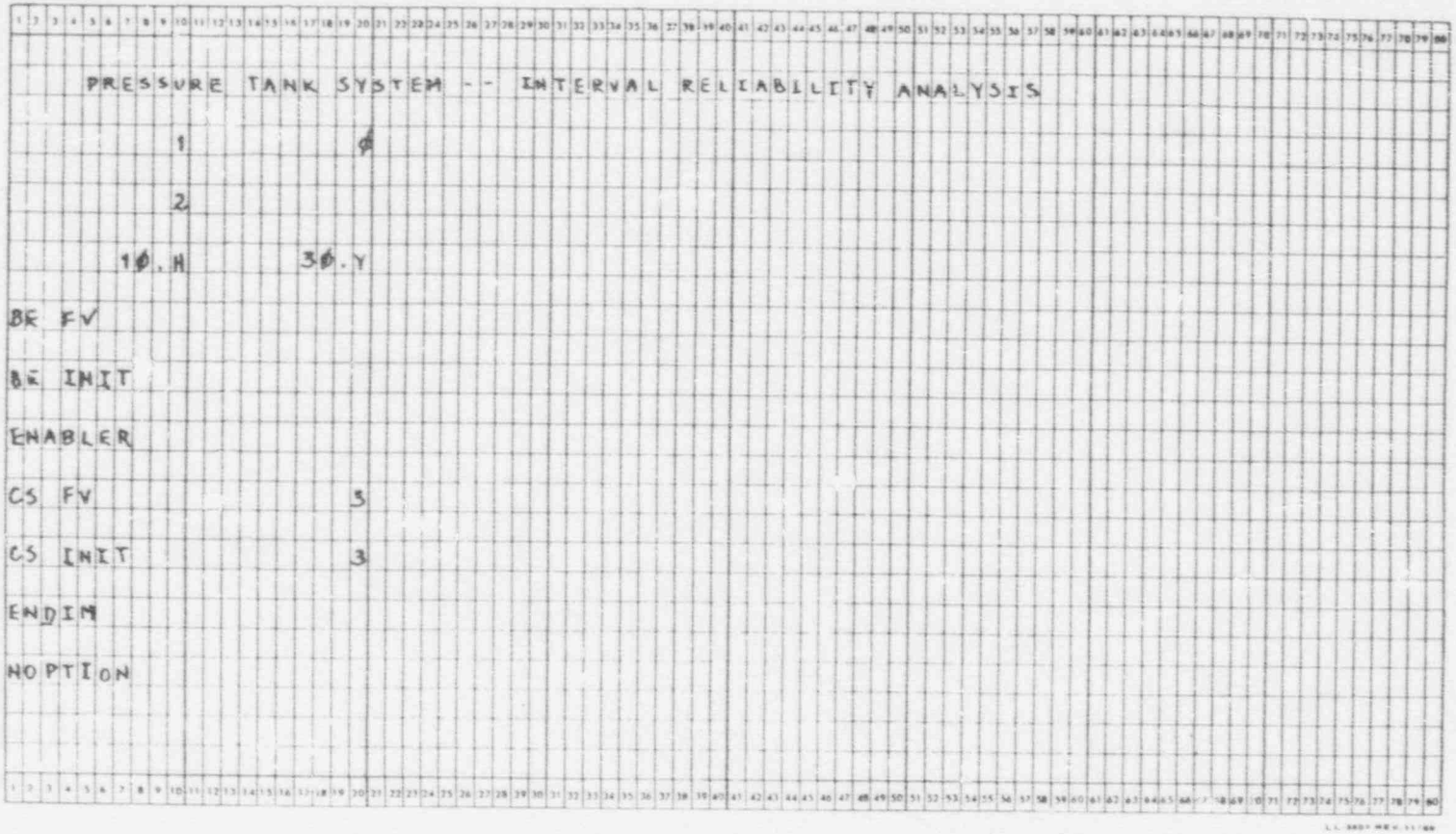


FIGURE 3-8
IMPORTANCE INPUT

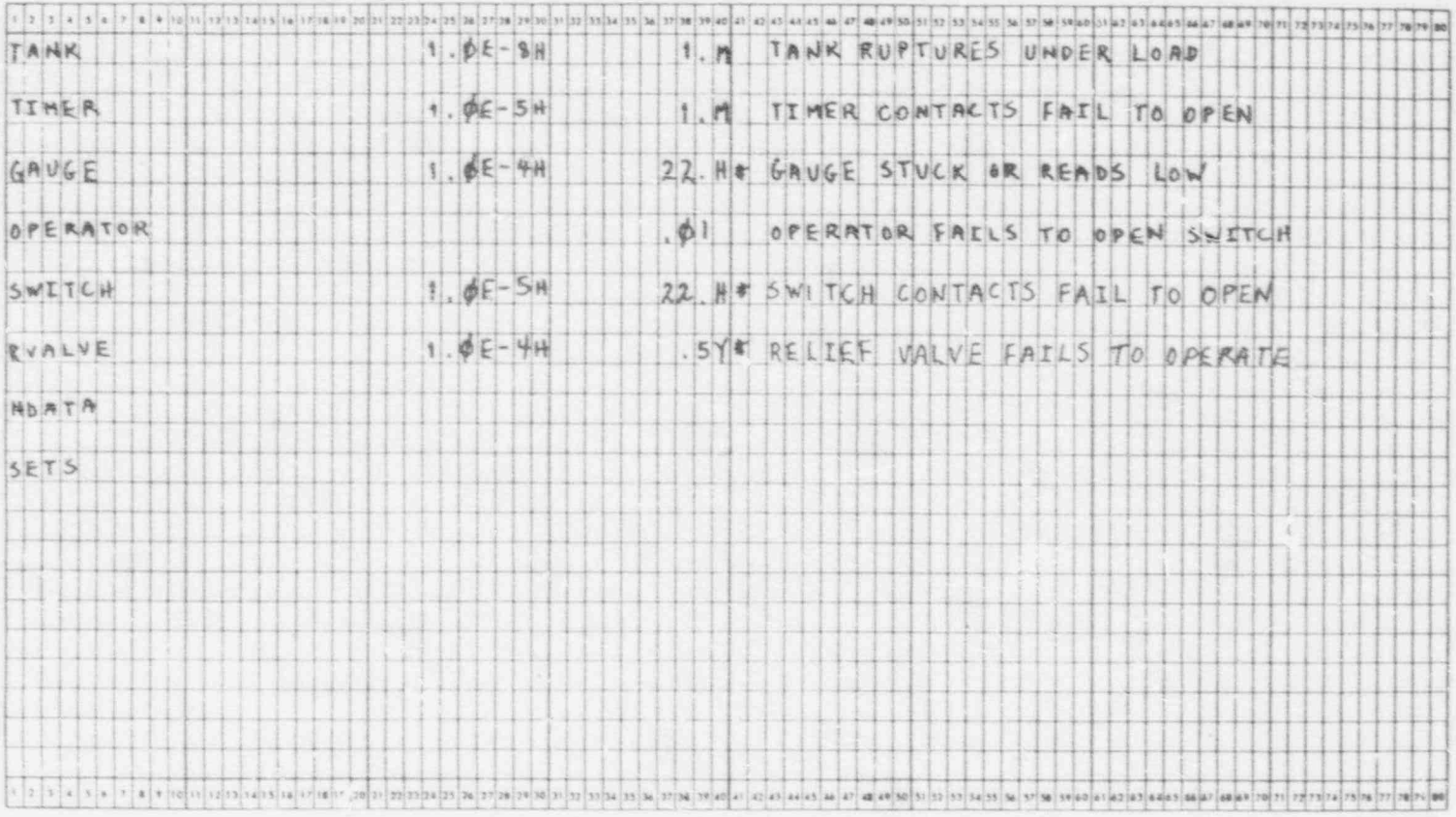


FIGURE 3-8

(CONT.)

and the following measures of min cut set importance for min cut sets of order 3 and less:

- Fussell-Vesely (system unavailability weighting)
- Initiator (Barlow-Proschan)

The next group of cards in Figure 3-8 are the basic event data. Note that the enabling events are indicated by either an asterisk in column 41 or a value of zero for LAMBDA. The asterisk indicates that we will take the product of LAMBDA times TAU to obtain a constant probability for the enabling event.

Figure 3-8 shows four cards which must be contained in the input to IMPORTANCE:

- END!M
- NOPTION
- NDATA
- SETS

The output is displayed in Appendix B. In the output of the importance measures on pages B-3 through B-9, the initiating event is identified with the letter I. In addition, the basic event data are displayed in terms of the units the user specified in the input. The full basic event description accompanies each basic event. The output on page B-4 is particularly important. When the initiator (i.e., Barlow-Proschan) measure of basic event importance is computed, the Top Event characteristics on B-4 ure generated. An important figure for catastrophic system events is the mean time to occurrence for the Top Event, given as 1784.6 years for this problem. This number can serve as a design goal for interval reliability analysis. With regard to the output of the min cut set measures on pages B-7 through B-9, the number of initiating events in the new min cut set

indicates the number of ways a min cut set can fail. Note that the listing of min cut sets provides a convenient basis to explain to management the order in which the basic events occurred in causing the Top Event. For example, on page B-7, min cut set no. 4 ranked number one. We see that the timer contacts failing to open is the initiating event. Because the relief valve failed to operate and the operator failed to respond, the pressure tank ruptured.

Note that in this problem the basic event and min cut set rankings based on the Fussell-Vesely measure are equal to those based on interval reliability. This is true because (1) the repair times of each initiator are nearly equal, (2) the system is reliable and (3) there is one initiating event per cut set. In this case, the Top Event Rate times the repair time of the initiator is the system unavailability. It follows that all importance measures are proportional to the Top Event Rate.

However, in general, rankings based on system unavailability differ from those based upon interval reliability. An interesting fact is that the role of initiating and enabling events can change. For example, say there was an emergency mode of operation for the pressure tank. During this mode, the operator knows that the timer contacts failed to open and the contacts are jumpered while repair or replacement on the timer is occurring. The operator operates the system by opening the switch when the pressure gauge reading indicates a pressurized tank. During the emergency mode the events which inactivated the loop before become initiating events for the emergency mode. The reliability of the operator has also changed since he knows that the timer has failed and he is the important component responsible in preventing overpressure. This example suggests there must be a reliability analysis conducted for each mode of system operation involving catastrophic system events.

3.5 PROGRAM IMPLEMENTATION

For convenience to the user, there are two versions of IMPORTANCE: a "small" version and a "large" version. The small version can accommodate:

200 basic events

and 4,000 min cut sets.

The large version can accommodate:

1,000 basic events

and 20,000 min cut sets.

The min cut sets are stored in a single array called the AB array. The maximum size of AB is 30K for the small version and 200K for the large version.

The following information is given on the SETS generated FORTRAN file 9 (which is generated by SETS).

- Parameter vector, PARVC, dimensioned to 11
- Variable names table, SETB, dimensioned to (2, n) where n = number of variable names
- "Information" vector SETVC, dimensioned to n where n = number of variable names
- Packed records for min cut sets (number of records defined by variable PARVC (8) = MXLITRM).

The meanings of the variables in parameter vector, PARVC, are provided in Table 3-2. Checks to be performed on the values of these variables are also indicated in Table 3-2. The associated error messages which cause the run to be terminated are given in Table 3-3. Unless IMPORTANCE is recompiled, the maximum number of cut sets to be read is 4,000 for the small version and 20,000 for the large version. Cut sets of order 105 and higher will not be accepted.

The second variable array on FORTRAN file 9 is SETB (2, n) where n = number of variable names. "n" equals the number of basic event names plus the number of gate event names. IMPORTANCE will use only the basic event names.

The third variable array is SETVC. The only variable of concern is

SETVC (n)

where n = SETNM (PARVC (1) = SETNM).

The value of bit 51 is tested. If bit 51 = 0, the following message is printed:

"EQUATION FOR VARIABLE PARV(2) PARV(3)
IS NOT SIMPLIFIED (I.E.
LAW OF ABSORPTION NOT APPLIED)"

and the program is terminated.

The fourth record consists of the min cut sets, which are packed according to a scheme illustrated in Figure 3-9 which presents a simplified example. As shown in this example, IMPORTANCE unpacks these cut sets and stores them in a single array called the AB array. The pointer array, called PTA, is also explained in Figure 3-9. Note that the cut sets originally were indexed

$\{3\}, \{5, 6\}$

corresponding to min cuts

$\{A\}, \{B, C\}$

Gate names do not appear, and the A array is reindexed starting with the number "1" and ending with NBE, where NBE equals the number of basic events. The variable names must be reindexed and then changed from R8 to A8 format. The min cut sets reindexed are

$\{1\}, \{2, 3\}$.

TABLE 3-2

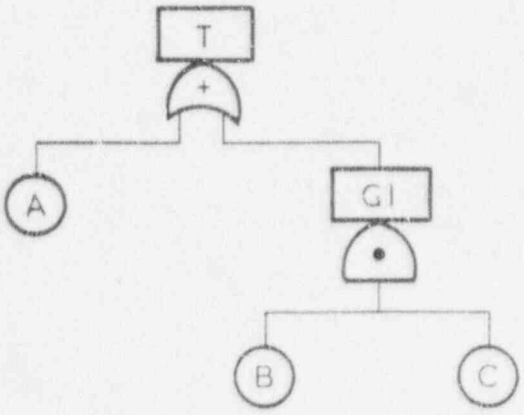
VARIABLES IN PARVC VECTOR

Variable	Variable Name	Meaning	Check When Reading In Variable
PARVC (1)	SETNM	Index Number for SETNM in SETB	None
PARVC (2)	NAM1	First Portion of Name for SETNM	None
PARVC (3)	NAM2	Second Portion of Name for SETNM	None
PARVC (4)	PGMDAT	Date	None
PARVC (5)	PGMTIM	Time	None
PARVC (6)	NMSET	Number of Variables	None
PARVC (7)	NMTRM	Number of Min Cut Sets	Cannot exceed MAXCS (parameter variable in IMPORTANCE, currently = 4,000 for small version and 20,000 for large version.)
PARVC (8)	MXLITRM	Maximum Order of Min Cut Set	Cannot exceed 105
PARVC (9)	FSTRMCL	Word Size	Check to see = 59
PARVC (10)	EXPCNTL	Expression Control	= 0 OK, 56th bit from right = 1 $\Rightarrow \Phi$ is generated, 57th bit from right = 1 $\Rightarrow \Omega$ is generated.
PARVC (11)	CMPCNTL	Check for Complements	= 0 no complements

TABLE 3-3

ERROR MESSAGES THAT CAUSE
IMPORTANCE TO BE TERMINATED

Variable Condition Generating Error Message	Message
PARVC (7) > MAXCS	The number of min cut sets exceeds MAXCS.
PARVC (8) > 105	The maximum order of min cut set exceeds 105.
PARVC (10) ≠ 0	
56th bit = 1	VARIABLE PARVC(1), PARVC(2) IS ALWAYS FALSE
	or
57th bit = 1	VARIABLE PARVC(1), PARVC(2) IS ALWAYS TRUE
PARVC (11) ≠ 0	Complement basic event variables exist



INDEX NO.	SET B NAMES	RECORD 60	59	58	...	1	EOF	RECORD 60	59	58	...	1	EOF
1	OMEGA		0	0		0			0	0		0	
2	T		0	0		0			0	0		0	
3	A		1	0		0			0	0		0	
4	G1		0	0		0			0	0		0	
5	B		0	0		0			1	0		0	
6	C		0	0		0			1	0		0	
		EQUALS (3)						EQUALS (5,6)					

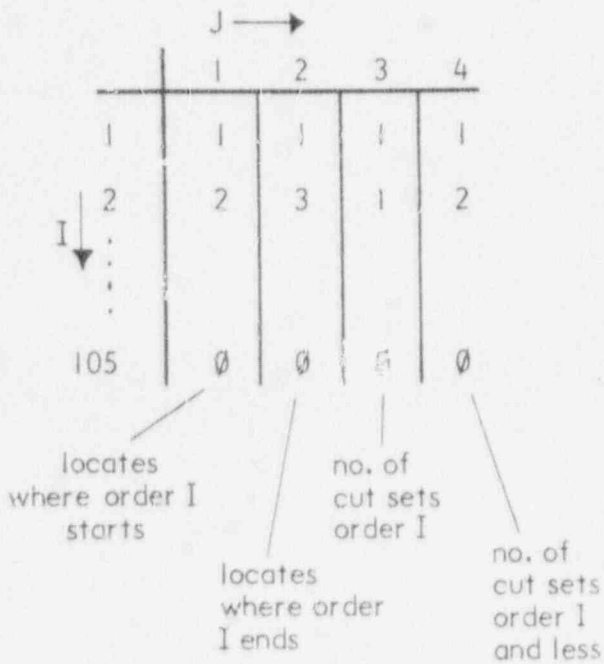
FIGURE 3-9

SIMPLIFIED EXAMPLE

INDEX NO.	NAME	
1	A	eliminate events that do not appear in the cut sets
2	B	
3	C	

AB array (1, 2, 3)

PTA (I, J)



Note that if cut sets of order I do not exist, PTA (I, J) = 0 for J = 1, 2, 3, 4

FIGURE 3-9 (cont.)

IMPORTANCE TRANSFORMATION

4.0 COMMERCIAL APPLICATION OF IMPORTANCE*

An older version of IMPORTANCE has been used at Lawrence Livermore National Laboratory on various studies which included a study of the advisability of seismic trip systems (8), (9) and for assessment of security systems (10), (11). These studies mainly addressed the problem of system unavailability. As described earlier in this report, IMPORTANCE has been modified so that its calculations can also be used for interval reliability analysis of control systems.

In this section we describe an analysis made by E. I. duPont de Nemours Co., Victoria in the reliability analysis of a chemical processing system which parallels the approach taken in analysis of the pressure tank system described in Section 3.4.

4.1 CHLORINE VAPORIZER SYSTEM

The system is the chlorine vaporizer system presented in Figure 4-1. The input process stream consists of liquid chlorine. The output stream consists of superheated chlorine gas which flows to a chemical reactor (not shown). The liquid chlorine is heated in the vaporizer and heated further in the superheater. There is a level control in the vaporizer which consists of a level transmitter and a pneumatic control valve. A concern in the operation of this system is that liquid chlorine may enter the overheads and be carried to the chemical reactor, potentially causing a reactor rupture. The original system in Figure 4-1 had an alarm indicating a high liquid chlorine level in the vaporizer and a low temperature alarm exit the vaporizer. When the alarm sounded the operator would physically close the output valve to the chlorine vaporizer to prevent liquid chlorine from entering the superheater. Two alternative designs considered by duPont were System A and System B (as shown in Figures 4-2 and 4-3). System A had the features of the original system with added control devices which included a redundant float level and interlock systems which would close pneumatic valve PV-67 in the event of an alarm condition. System B had many features of System A with added safety devices which included:

---

* Information in this section is provided by Mr. Colin Dunglinson, a process engineer at the duPont Victoria Plant.

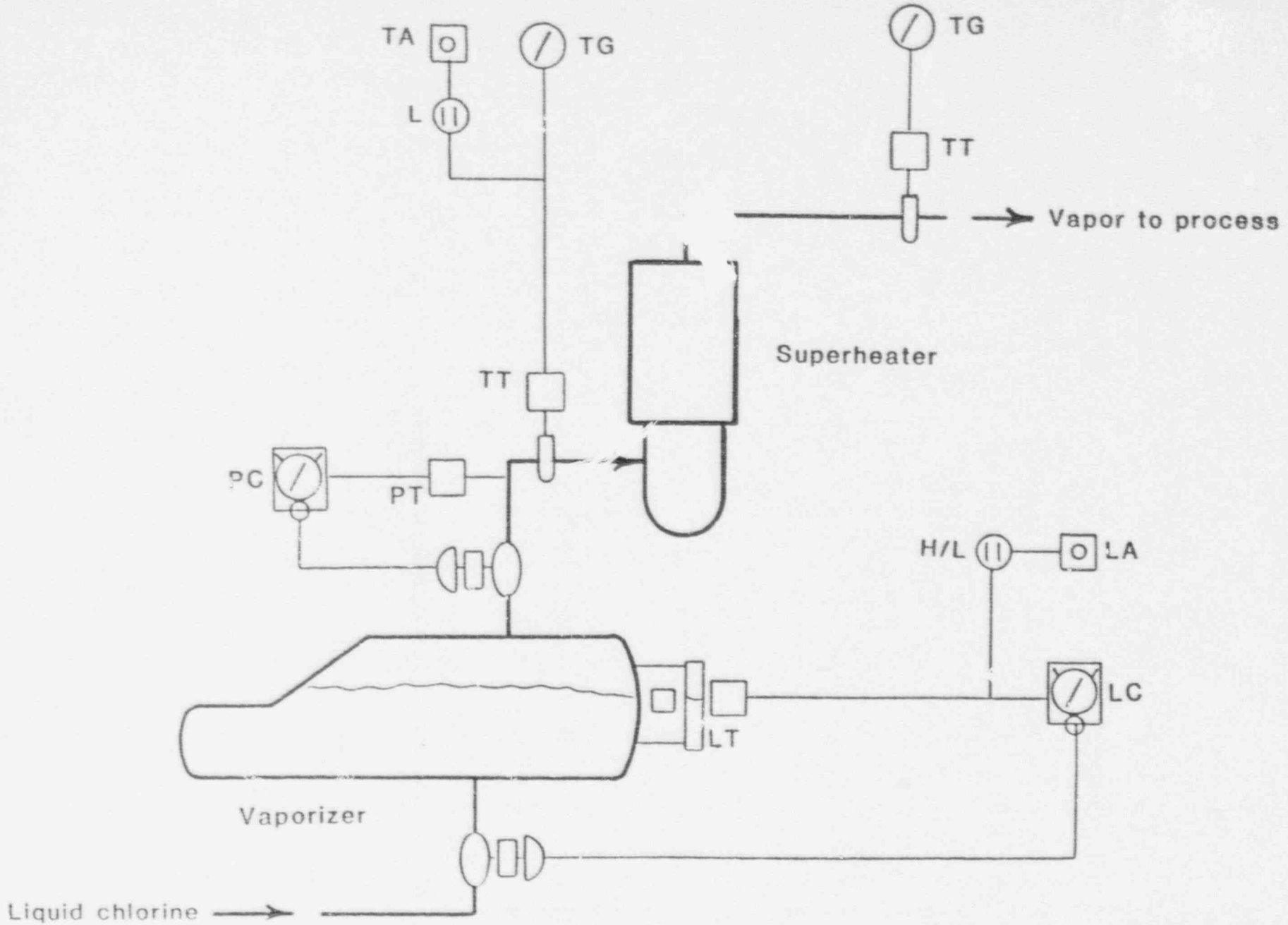


FIGURE 4-1
ORIGINAL SYSTEM

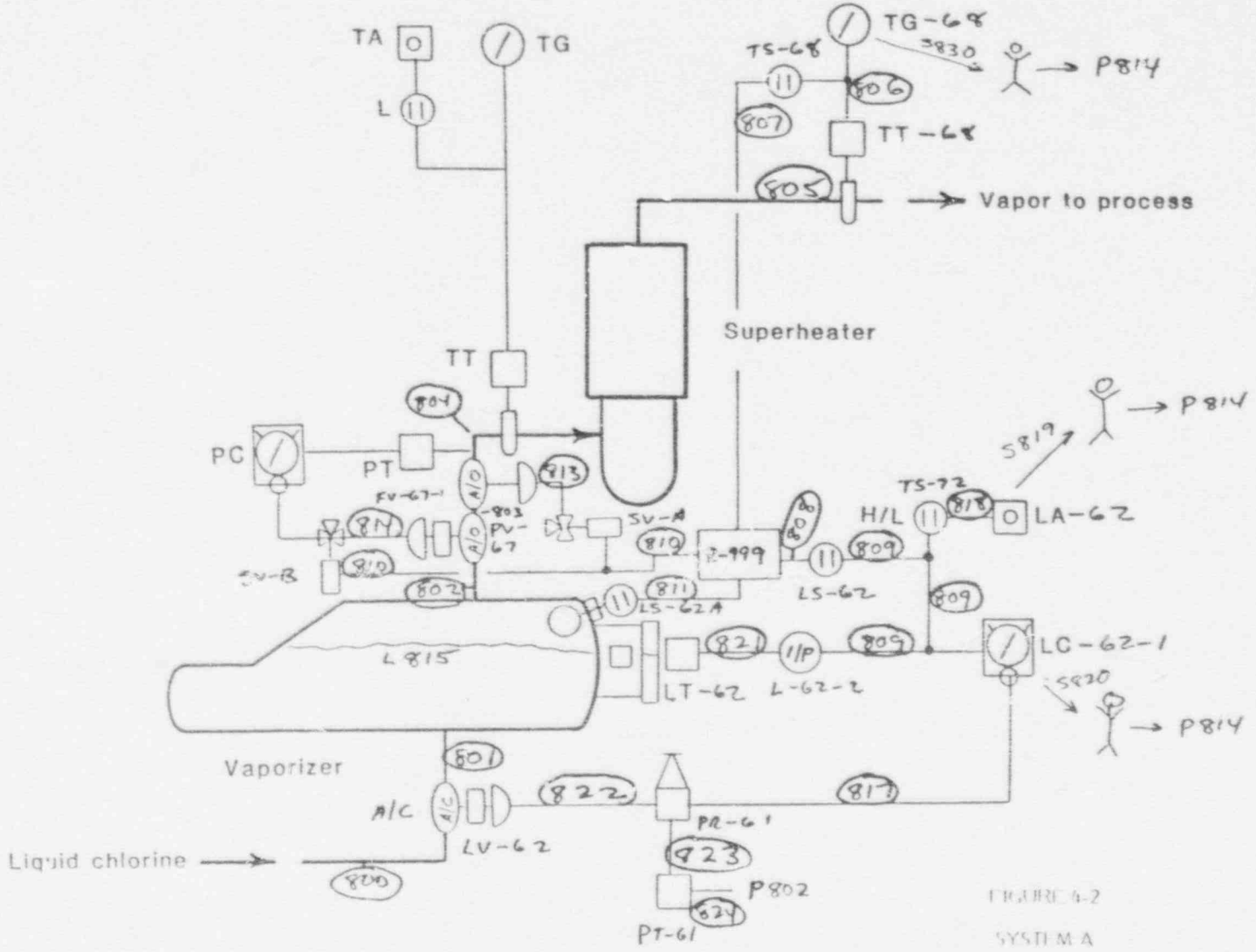


FIGURE 4-2

SYSTEM A

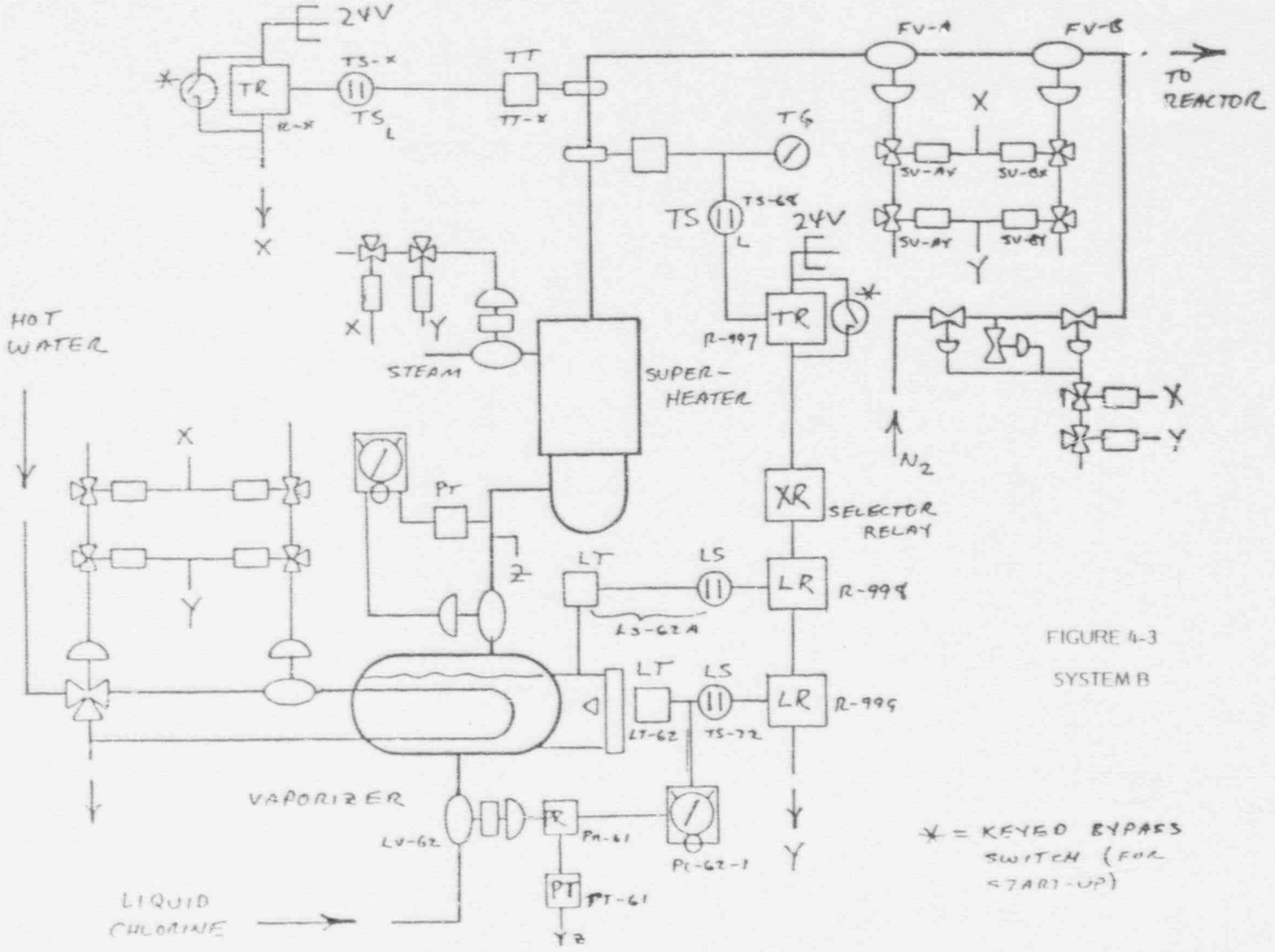


FIGURE 4-3

SYSTEM B

* = KEYED BYPASS SWITCH (FOR START-UP)

- Two interlock loops
- Dedicated relay for each sensor
- Reverse acting level transmitter
- Selector switch to select vaporizer in use (the system uses two vaporizers on-line and an installed spare)
- Bypass around low temperature trip – for startup

4.2 SYSTEM DIGRAPHS

System digraphs were used to generate fault trees for all three systems. The process variables for System A are shown in Figure 4-2 which was used to construct the system digraph given in Figure 4-4. This digraph shows three feedback loops initiated by the operator (indicated by transfer symbols (1), (2) and (3)) and these interlock feedback loops all passing through node S810 in which a common relay R999 is de-energized. Between each set of nodes in the digraph (which represent variables) are (1) edges which describe the relationship between the variables and (2) devices that cause the input-output relationships.

4.3 COMPONENT FAILURE MODE ANALYSIS

From the devices identified in the digraph in Figure 4-2, failure modes were identified and their associated failure rates and fault duration times obtained from plant data or from data banks. Typical data given in mean time to failure, MTTF, are shown in Figures 4-5 and 4-6 for pneumatic transmitters and sensors, respectively. Note there are many more failure modes that cause the transmitter to fail low than high. Also note that the modes which fail high or low are initiating events as opposed to sensor stuck which is an enabling event.

4.4 FAULT TREE GENERATION AND QUALITATIVE ANALYSIS

The synthesis algorithm was used to construct the fault tree from the digraph. The Top Event was mass flow rate at location 803 too high, [M803 (+10)].

The min cut sets were obtained from the computer code, FTAP,[12] by using a probabilistic culling function which eliminated min cut sets according to

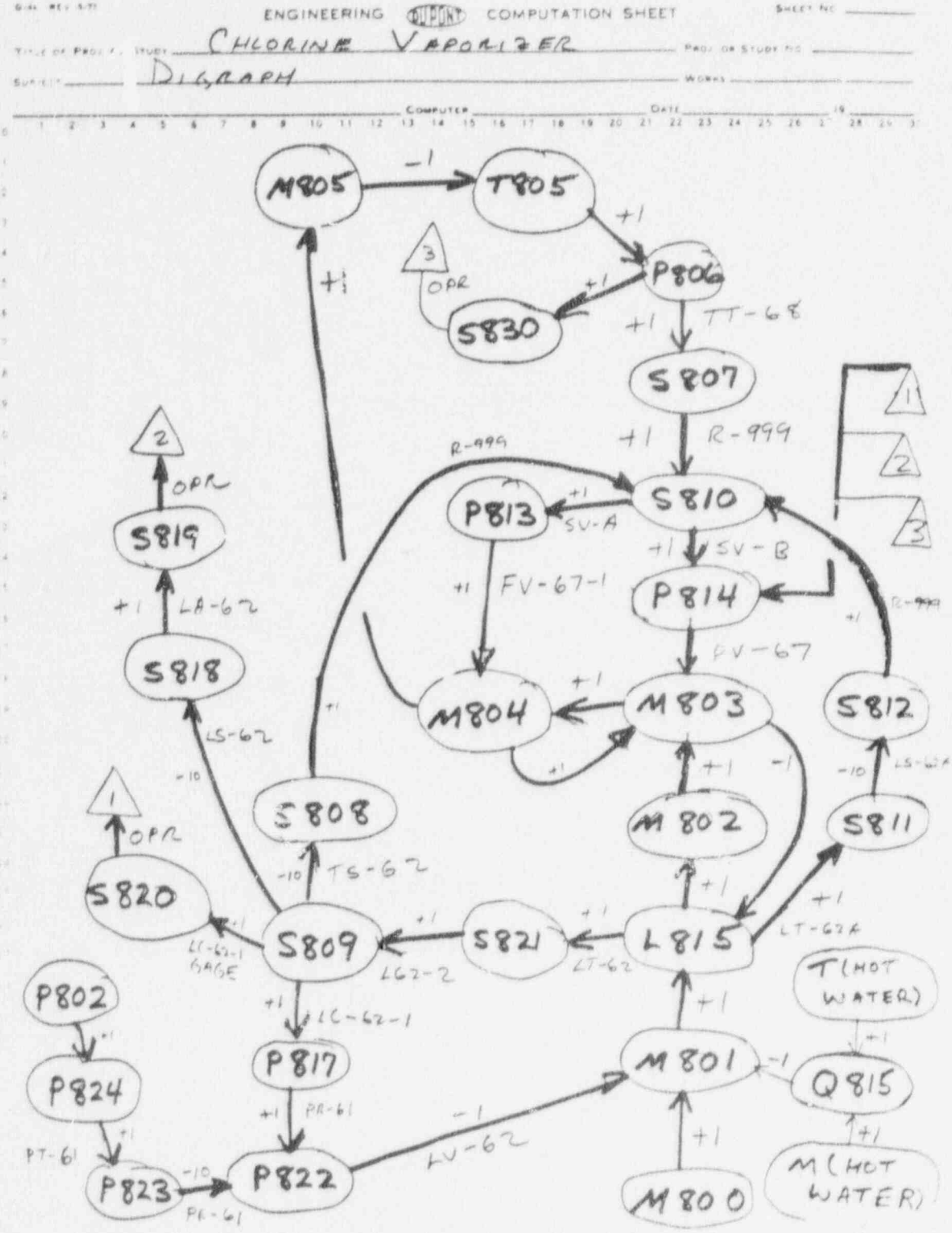


FIGURE 4-4

SYSTEM DIGRAPH FOR SYSTEM A

ENGINEERING DUPONT COMPUTATION SHEET

Title or Proj. or Study _____ Proj. or Study No. _____

Subject _____ Work _____ Sheet No. _____

Computer _____ Date _____

FT (P)

P = PNEUMATIC, E = ELECTRONIC

ZERO GAIN	λ (1/YR)	FAIL HI	λ (1/YR)	FAIL LO	λ (1/YR)
STUCK	1/20	MISC	1/20	SIGNAL LINE OUT	1/40
		PLUG IMPULSE LINES	1/3	CAPSULE FAILS	1/10
		VALVE OUT IMPULSE LINES	1/15	LOCAL AIR LOSS	1/10
				VALVED OUT	1/15
				OUTPUT LEAK	1/40
				IMPULSE LINE VALVED OUT	1/15
				IMPULSE LINE PLUGGED	1/3 ①

① SPECIFIC

NOTES:

FIGURE 4-5

FAILURE MODES

S-11 REV. 5-77

ENGINEERING DUPONT COMPUTATION SHEET

SHEET NO.

TITLE OF PROJ. OR STUDY

PROJ. OR STUDY NO.

SUBJECT

WORKS

COMPUTER DATE 19

P = PNEUMATIC, E = ELECTRONIC

X S (P)

		FAIL HI	FAIL LO		
ZERO GAIN	2		2		
FAILS-MISC		1/35			
MISSET		1/35			
SHORTED		1/40			
OPEN INPUT (HI TRIP ONLY)		1/20			
3 WAY IN TEST		1/20			

NOTES:

FIGURE 4-6

FAILURE MODES

probability. (This same feature is available in SETS.) This step was necessary because the number of min cut sets was enormous and all of them could not be generated.

4.5 RELIABILITY ANALYSIS

IMPORTANCE was run to obtain measures of system performance and importance measures for basic events and min cut sets. For this system we are concerned with measures of interval reliability since the Top Event is potentially catastrophic.* The figure of merit for system performance is the mean time to failure and the expected number of failures during the plant life (assumed to be 20 years). The analysis of the original system revealed a mean time to failure of 1.5 years with 13.1 system failures in 20 years (as shown by the IMPORTANCE output on page C-3 of Appendix C).

This frequency corresponded reasonably with plant data which recorded a frequency of approximately once every four years. The calculated number is reasonable since the plant operators may not report all incidences.

As shown by the intiator rankings and page C-4, the failure of the level transmitter and i/p transducer failing low made the dominant contribution. Likewise, as shown by the enabler rankings on page C-5, the failure modes involving the operator to respond dominated.

As shown in Figure 4-7 a series of design changes were made and IMPORTANCE rerun to assess the change in the mean time to failure. The rankings of the initiators and enablers suggested design changes. The third column in Figure 4-7 lists the type of level transmitter in the design. The transmitter in the original design had a MTTF of 1.5 years--the transmitter that was reverse acting had a MTTF of 17 years. "Fail low" modes are more common than "fail high" modes.

---

* All carryovers of liquid chlorine do not result in ruptures. Engineering analysis is necessary to perform consequence calculations.

	SYSTEM	MEAN TIME TO FAILURE (YR)	ENF (20)	LT FAILURE RATE (1/YR)
•	ORIGINAL	1.5	13	1/1.5
•	1 INTERLOCK 1 RELAY	26.7	0.70	1/1.5
•	1 INTERLOCK 3 RELAYS	59.5	0.34	1/1.5
•	1 INTERLOCK 3 RELAYS	308	0.06	1/17
•	1 INTERLOCK 3 RELAYS + SEL SW & BYPASS	273	0.07	1/17
•	2 INTERLOCKS 3 RELAYS + SEL SW & BYPASS	4,250	.0046	1/17
		796	.024	1/1.5

FIGURE 4-7

EFFECT OF SYSTEM DESIGN CHANGES

The first change to the original design was the addition of one interlock on valve PV-67 and a new valve with one relay (this interlock system serves as a redundancy to the operator). This system (system A) had a mean time to failure of 26.7 years. "Conventional wisdom" would have concluded that design A is satisfactory. However, the use of FTAP and IMPORTANCE suggested further design changes. The next change was the inclusion of a separate relay for each sensing device (two sensors for level and one for low temperature). This change increased the MTTF by a factor of two. The initiator rankings up to this point ranked the level transmitter failing low as a dominant initiator. The next change included changing the level transmitter to a reverse acting (e.g., fail-safe on loss of instrument air) level transmitter and eliminating i/p transducer L-62-2 which increased the MTTF by a factor of 5. The analysis up to this point did not include the possibility of bypassing the entire interlock system. Adding a bypass and selector switches did not adversely affect reliability (273 yr MTTF vs. 308 yr without) – a somewhat surprising result.

The final design which is system B included 2 interlocks (double valving), 3 relays, a bypass and selector switches and a reverse acting level transmitter. The overall improvement increased the MTTF to 4,250 years. The design goal was 1,000 years. An assessment of the spurious trip rate was also made. The addition of 20 control devices each with a MTTF of approximately 20 years in generating a spurious signal resulted in an estimate of one spurious trip per year.

4.6 COMMENTS

The first author of this report has had the opportunity to teach fault tree analysis courses. A comment made by one of the course participants when the above example was presented in the course was as follows:

> As a design engineer, I would have proposed a system which incorporated some of the design changes that were implemented in the modified system designs. However, I would have no idea of (1) the relative improvement in system performance or (2) the important contributors to system failure. The approach described (as above) provides a logical engineering approach to reliability analysis of control systems.

The authors agree with this statement and add one other comment.

Fault tree analysis is best used as a design tool as was illustrated in the example of the chlorine vaporizer. The basic event data which was used on the original design was also used to assess alternative designs. The basic event data in a sense was verified since the expected number of system failures for the original design agreed with the data based on operating experience.

With the advent of complex engineering systems posing potential risks to the public and property we feel reliability analysis as described in this manual is necessary. The important point to be made is that reliability analysis is not an end-all, but is a very important tool in decision making, particularly, as systems become more complex.

5.0 FUTURE DEVELOPMENTS

TERA is actively seeking funding for the project described below.

The new version of IMPORTANCE performs calculations with point estimates for the basic event parameters, failure rate and fault duration. A worthwhile project would be to alter IMPORTANCE so that it can conduct an uncertainty analysis by a Monte Carlo Analysis. This can be performed by assuming the basic event parameters are random variables with distributions of specified means and variances.

6.0 REFERENCES

1. Lambert, H.E., Fault Trees for Decision-Making in Systems Analysis, Pn.D. thesis, Lawrence Livermore National Laboratory Rept., UCRL-51829, (1975). *

2. Worrell, R. B. and Stack, D. W., A SETS User's Manual for the Fault Tree Analyst, Sandia National Laboratories, Albuquerque, Rept. SAND77-2051, (1978).*

3. Worrell, R. B. and Stack, D. W., Common Cause Analysis Using SETS, Sandia National Laboratories, Albuquerque, Rept. SAND77-1832 (1977).*

4 Boozer, D. D., et al., Safeguards Systems Effectiveness Modeling, Sandia National Laboratories, Albuquerque, Rept. SAN76-0428, (1976).*

5. Lambert, H. E., Lim, J. J. and Gilman, F. M., A Digraph-Fault Tree Methodology for the Assessment of Material Control Systems, Lawrence Livermore Laboratory, Rept. UCRL-52170 (1979), NUREG/CR-0777. *

6. Dunn, D. R., Huebel, J. G. and Poggio, A. J., Safeguards Research at Lawrence Livermore Laboratory, Lawrence Livermore National Laboratory, UCRL-82224 (1980). *

7. Worrell, R. B., Sandia National Laboratories, private communications (1980).

8. Cummings, G.E., et al., Advisability of Seismic Scram, Lawrence Livermore National Laboratory, Livermore Rept. UCRL 52158 (1976). *

9. Cummings, G.E., Wells, J.E., and Lambert, H.E., "Assessment of Seismic Trip Systems for Commercial Power Reactors," Nuclear Safety, Sept.-Oct. 1978, Vol. 19, No. 5, pp. 590-601.

10. Lambert, H.E., Lim, J.J., and Gilman, F.M., A Digraph-Fault Tree Methodology for Assessment of Material Control Programs, Lawrence Livermore National Laboratory, Livermore Rept. UCRL-52710, Rept. NUREG/CR-0777 (1979). *

11. Lambert, H.E., Lim, J.J., and Gilman, F.M., "Material Control Study: A Directed Graph and Fault Tree Procedure for Adversary Event Set Generation," (in Synthesis and Analysis Methods for Safety and Reliability Studies," G. Apostolakis, S. Garribba and G. Volta Editors, Plenum Press, N.Y., 1980), pp. 415-436.

12. Willie, R., Fault Tree Analysis Program, Operations Research Center Report No. ORC 78-14, University of California, Berkeley (1978); Rept. UCRL-13981, Lawrence Livermore National Laboratory. *

---

* Available from National Technical Information Service, Springfield, VA, 22151, USA.

APPENDIX A

IMPORTANCE OUTPUT FOR PROPORTIONAL HAZARDS

THE IMPORTANCE COMPUTER CODE - DEVELOPED FOR SANDIA NATIONAL LABORATORIES BY TERA CORP., SYSTEM SAFETY AND RELIABILITY GROUP.

****

PRESSURE TANK SYSTEM -- PROPORTIONAL HAZARDS

****

IMPORTANCE MEASURES WILL BE CALCULATED AT THE 3 INPUTTED POINTS LISTED BELOW.
PROBABILITY OF THE TOP EVENT -- .100E-05 .100E-03 .100E-01

****

** BASIC EVENT OPTIONS USED **

BIRNBAUM	CRITICALITY	UPGRADING FUNCTION	FUSSELL-VESELY	INITIATOR (BARLOW-PROSCHAN)	ENABLER (CONTRIBUTORY)	STRUCTURAL
NO	NO	YES	NO	NO	NO	YES

****

** MIN CUT SET OPTIONS USED **

INITIATOR (BARLOW-PROSCHAN)	FUSSELL-VESELY
NO	YES

****

MAXIMUM CUT SET ORDER FOR THE FUSSELL-VESELY MEASURE OF CUT SET IMPORTANCE = 3

INFORMATION ON DETAILED CUT SET OUTPUT (DEFAULT VALUES USED) -- NN = 100 AND FACTOR =.01

** BASIC EVENT DATA **

PROPORTIONAL HAZARD	NAME	DESCRIPTION
10.0	GAUGE	GAUGE STUCK OR READS LOW
100.	OPERATOR	OPERATOR FAILS TO OPEN SWITCH
10.0	RVALVE	RELIEF VALVE FAILS TO OPERATE
100.	SWITCH	SWITCH CONTACTS FAIL TO OPEN
.100E-02	TANK	TANK RUPTURES UNDER LOAD
1.00	TIMER	TIMER CONTACTS FAIL TO OPEN

********** PRESSURE TANK SYSTEM -- PROPORTIONAL HAZARDS **********

BIRNBAUM'S MEASURE OF STRUCTURAL IMPORTANCE

NUMBER OF SYSTEM STATES = .320E+02

RANK	BASIC EVENT	IMPORTANCE	BASIC EVENT DESCRIPTION
1	TANK	.670	TANK RUPTURES UNDER LOAD
2	RVALVE	.249	RELIEF VALVE FAILS TO OPERATE
2	TIMER	.249	TIMER CONTACTS FAIL TO OPEN
3	GAUGE	.132	GAUGE STUCK OR READS LOW
3	SWITCH	.132	SWITCH CONTACTS FAIL TO OPEN
3	OPERATOR	.132	OPERATOR FAILS TO OPEN SWITCH

********** PRESSURE TANK SYSTEM -- PROPORTIONAL HAZARDS **********

UPGRADING FUNCTION--BASIC EVENT IMPORTANCE

PROB OF TOP EVENT= .100E-05

TIME DEPENDENT CALCULATIONS

RANK	BASIC EVENT	IMPORTANCE	PROPORTIONAL		HAZARD	BASIC EVENT DESCRIPTION
1	TANK	.58731	.100E-02	PROP H		TANK RUPTURES UNDER LOAD
2	TIMER	.41249	1.00	PROP H		TIMER CONTACTS FAIL TO OPEN
3	RVALVE	.41147	10.0	PROP H		RELIEF VALVE FAILS TO OPERATE
4	SWITCH	.17056	100.	PROP H		SWITCH CONTACTS FAIL TO OPEN
4	OPERATOR	.17056	100.	PROP H		OPERATOR FAILS TO OPEN SWITCH
5	GAUGE	.23091E-01	10.0	PROP H		GAUGE STUCK OR READS LOW

********** PRESSURE TANK SYSTEM -- PROPORTIONAL HAZARDS **********

UPGRADING FUNCTION--BASIC EVENT IMPORTANCE

PROB OF TOP EVENT= .100E-03

TIME DEPENDENT CALCULATIONS

RANK	BASIC EVENT	IMPORTANCE	PROPORTIONAL		HAZARD	BASIC EVENT DESCRIPTION
1	TIMER	.95331	1.00	PROP	H	TIMER CONTACTS FAIL TO OPEN
2	RVALVE	.94289	10.0	PROP	H	RELIEF VALVE FAILS TO OPERATE
3	SWITCH	.37284	100.	PROP	H	SWITCH CONTACTS FAIL TO OPEN
3	OPERATOR	.37284	100.	PROP	H	OPERATOR FAILS TO OPEN SWITCH
4	GAUGE	.52584E-01	10.0	PROP	H	GAUGE STUCK OR READS LOW
5	TANK	.38208E-01	.100E-02	PROP	H	TANK RUPTURES UNDER LOAD

********** PRESSURE TANK SYSTEM -- PROPORTIONAL HAZARDS **********

UPGRADING FUNCTION--BASIC EVENT IMPORTANCE

PROB OF TOP EVENT= .100E-01

TIME DEPENDENT CALCULATIONS

RANK	BASIC EVENT	IMPORTANCE	PROPORTIONAL		HAZARD	BASIC EVENT DESCRIPTION
1	RVALVE	.87435	10.0	PROP H		RELIEF VALVE FAILS TO OPERATE
2	TIMER	.86837	1.00	PROP H		TIMER CONTACTS FAIL TO OPEN
3	SWITCH	.10889	100.	PROP H		SWITCH CONTACTS FAIL TO OPEN
3	OPERATOR	.10889	100.	PROP H		OPERATOR FAILS TO OPEN SWITCH
4	GAUGE	.91617E-01	10.0	PROP H		GAUGE STUCK OR READS LOW
5	TANK	.23466E-02	.100E-02	PROP H		TANK RUPTURES UNDER LOAD

********** PRESSURE TANK SYSTEM -- PROPORTIONAL HAZARDS **********

FUSSELL-VESELY MEASURE OF CUT SET IMPORTANCE (MEASURE OF SYSTEM UNAVAILABILITY)

LIMITING SYSTEM UNAVAILABILITY= .100E-05

RANK IMPORTANCE

1 .587E+00 CUT SET 1

BASIC EVENT	PROPORTIONAL HAZARD		BASIC EVENT DESCRIPTION
TANK	.10000E-02	PROP H	TANK RUPTURES UNDER LOAD

2 .196E+00 CUT SET 3

BASIC EVENT	PROPORTIONAL HAZARD		BASIC EVENT DESCRIPTION
RVALVE	10.000	PROP H	RELIEF VALVE FAILS TO OPERATE
SWITCH	100.00	PROP H	SWITCH CONTACTS FAIL TO OPEN
TIMER	1.0000	PROP H	TIMER CONTACTS FAIL TO OPEN

2 .196E+00 CUT SET 4

BASIC EVENT	PROPORTIONAL HAZARD		BASIC EVENT DESCRIPTION
OPERATOR	100.00	PROP H	OPERATOR FAILS TO OPEN SWITCH
RVALVE	10.000	PROP H	RELIEF VALVE FAILS TO OPERATE
TIMER	1.0000	PROP H	TIMER CONTACTS FAIL TO OPEN

3 .201E-01 CUT SET 2

BASIC EVENT	PROPORTIONAL HAZARD		BASIC EVENT DESCRIPTION
GAUGE	10.000	PROP H	GAUGE STUCK OR READS LOW
RVALVE	10.000	PROP H	RELIEF VALVE FAILS TO OPERATE
TIMER	1.0000	PROP H	TIMER CONTACTS FAIL TO OPEN

********** PRESSURE TANK SYSTEM -- PROPORTIONAL HAZARDS **********

FUSSELL-VESELY MEASURE OF CUT SET IMPORTANCE (MEASURE OF SYSTEM UNAVAILABILITY)

LIMITING SYSTEM UNAVAILABILITY= .100E-03

RANK IMPORTANCE

1 .456E+00 CUT SET 4

BASIC EVENT	PROPORTIONAL HAZARD		BASIC EVENT DESCRIPTION
OPERATOR	100.00	PROP H	OPERATOR FAILS TO OPEN SWITCH
RVALVE	10.000	PROP H	RELIEF VALVE FAILS TO OPERATE
TIMER	1.0000	PROP H	TIMER CONTACTS FAIL TO OPEN

1 .454E+00 CUT SET 3

BASIC EVENT	PROPORTIONAL HAZARD		BASIC EVENT DESCRIPTION
RVALVE	10.000	PROP H	RELIEF VALVE FAILS TO OPERATE
SWITCH	100.00	PROP H	SWITCH CONTACTS FAIL TO OPEN
TIMER	1.0000	PROP H	TIMER CONTACTS FAIL TO OPEN

2 .536E-01 CUT SET 2

BASIC EVENT	PROPORTIONAL HAZARD		BASIC EVENT DESCRIPTION
GAUGE	10.000	PROP H	GAUGE STUCK OR READS LOW
RVALVE	10.000	PROP H	RELIEF VALVE FAILS TO OPERATE
TIMER	1.0000	PROP H	TIMER CONTACTS FAIL TO OPEN

3 .382E-01 CUT SET 1

BASIC EVENT	PROPORTIONAL HAZARD		BASIC EVENT DESCRIPTION
TANK	.10000E-02	PROP H	TANK RUPTURES UNDER LOAD

********** PRESSURE TANK SYSTEM -- PROPORTIONAL HAZARDS **********

FUSSELL-VESELY MEASURE OF CUT SET IMPORTANCE (MEASURE OF SYSTEM UNAVAILABILITY)

LIMITING SYSTEM UNAVAILABILITY= .100E-01

RANK IMPORTANCE

1 .448E+00 CUT SET 4

BASIC EVENT	PROPORTIONAL HAZARD		BASIC EVENT DESCRIPTION
OPERATOR	100.00	PROP H	OPERATOR FAILS TO OPEN SWITCH
RVALVE	10.000	PROP H	RELIEF VALVE FAILS TO OPERATE
TIMER	1.0000	PROP H	TIMER CONTACTS FAIL TO OPEN

1 .448E+00 CUT SET 3

BASIC EVENT	PROPORTIONAL HAZARD		BASIC EVENT DESCRIPTION
RVALVE	10.000	PROP H	RELIEF VALVE FAILS TO OPERATE
SWITCH	100.00	PROP H	SWITCH CONTACTS FAIL TO OPEN
TIMER	1.0000	PROP H	TIMER CONTACTS FAIL TO OPEN

2 .104E+00 CUT SET 2

BASIC EVENT	PROPORTIONAL HAZARD		BASIC EVENT DESCRIPTION
GAUGE	10.000	PROP H	GAUGE STUCK OR READS LOW
RVALVE	10.000	PROP H	RELIEF VALVE FAILS TO OPERATE
TIMER	1.0000	PROP H	TIMER CONTACTS FAIL TO OPEN

3 .237E-02 CUT SET 1

BASIC EVENT	PROPORTIONAL HAZARD		BASIC EVENT DESCRIPTION
TANK	.10000E-02	PROP H	TANK RUPTURES UNDER LOAD

REFERENCE TABLE FOR MIN CUT SETS

ORDER	1	2	3
NO. OF MIN CUT SETS	1	0	3

NO. OF MIN CUT SETS = 4

CUT SET NO.	ORDER	BASIC EVENTS		
1	1	TANK		
2	3	GAUGE	RVALVE	TIMER
3	3	RVALVE	SWITCH	TIMER
4	3	OPERATOR	RVALVE	TIMER

APPENDIX B

IMPORTANCE OUTPUT FOR INTERNAL RELIABILITY ANALYSIS

THE IMPORTANCE COMPUTER CODE - DEVELOPED FOR SANDIA NATIONAL LABORATORIES BY TERA CORP., SYSTEM SAFETY AND RELIABILITY GROUP.

****

PRESSURE TANK SYSTEM -- INTERVAL RELIABILITY ANALYSIS

****

INPUT DATA OPTION 1
FAILURE RATE AND MEAN FAULT DURATION GIVEN IN TERMS OF REAL TIME

STEADY STATE CALCULATIONS

EXPECTED NUMBER OF FAILURES CALCULATED FOR TIME = 10.00H 30.00Y

****

** BASIC EVENT OPTIONS USED **

BIRNBAUM	CRITICALITY	UPGRADING FUNCTION	FUSSELL-VESELY	INITIATOR (BARLOW-PROSCHAN)	ENABLER (CONTRIBUTORY)	STRUCTURAL
NO	NO	NO	YES	YES	YES	NO

****

** MIN CUT SET OPTIONS USED **

INITIATOR (BARLOW-PROSCHAN)	FUSSELL-VESELY
YES	YES

****

MAXIMUM CUT SET ORDER FOR THE BARLOW-PROSCHAN MEASURE OF CUT SET IMPORTANCE = 3
MAXIMUM CUT SET ORDER FOR THE FUSSELL-VESELY MEASURE OF CUT SET IMPORTANCE = 3

INFORMATION ON DETAILED CUT SET OUTPUT (DEFAULT VALUES USED) -- NM = 100 AND FACTOR = .01

** BASIC EVENT DATA **

FAILURE RATE	MEAN FAULT DURATION		NAME	ENABLER	DESCRIPTION
.100E-07/HOUR	1.0	MONTHS	TANK		TANK RUPTURES UNDER LOAD
.100E-03/HOUR	.50	YEARS	RVALVE	*	RELIEF VALVE FAILS TO OPERATE
.100E-04/HOUR	1.0	MONTHS	TIMER		TIMER CONTACTS FAIL TO OPEN
.100E-04/HOUR	22.	HOURS	SWITCH	*	SWITCH CONTACTS FAIL TO OPEN
	.10E-01	CONSTP	OPERATOR	*	OPERATOR FAILS TO OPEN SWITCH
.100E-03/HOUR	22.	HOURS	GAUGE	*	GAUGE STUCK OR READS LOW

********** PRESSURE TANK SYSTEM -- INTERVAL RELIABILITY ANALYSIS **********

FUSSELL-VESELY MEASURE OF BASIC EVENT IMPORTANCE (MEASURE OF SYSTEM UNAVAILABILITY)

STEADY STATE CALCULATIONS

LIMITING SYSTEM UNAVAILIBILITY= .46087E-04

RANK	BASIC EVENT		IMPORTANCE	FAILURE RATE	MEAN FAULT DURATION		BASIC EVENT DESCRIPTION
1	TIMER	I	.844	.100E-04 HOURS	1.00	MONTHS	TIMER CONTACTS FAIL TO OPEN
1	RVALVE		.844	.100E-03 HOURS	.500	YEARS	RELIEF VALVE FAILS TO OPERATE
2	OPERATOR		.679		.100E-01		OPERATOR FAILS TO OPEN SWITCH
3	TANK	I	.156	.100E-07 HOURS	1.00	MONTHS	TANK RUPTURES UNDER LOAD
4	GAUGE		.149	.100E-03 HOURS	22.0	HOURS	GAUGE STUCK OR READS LOW
5	SWITCH		.149E-01	.100E-04 HOURS	22.0	HOURS	SWITCH CONTACTS FAIL TO OPEN

I DENOTES INITIATING EVENT

********** PRESSURE TANK SYSTEM -- INTERVAL RELIABILITY ANALYSIS **********

STEADY STATE SYSTEM CHARACTESTICS

TOP EVENT RATE (PER HOUR) = .63963E-07 TOP EVENT RATE (PER YEAR) = .56031E-03

MEAN TIME TO SYSTEM FAILURE = .15633E+08 HOURS 1784.6 YEARS

MEAN TIME TO SYSTEM REPAIR = 720.53 HOURS 30.022 DAYS.

LIMITING SYSTEM UNAVAILIBILITY= .46087E-04

MISSION TIME	10.0 H	30.0 Y
EXPECT NO OF SYSTEM FAIL	.640E-06	.168E-01

********** PRESSURE TANK SYSTEM -- INTERVAL RELIABILITY ANALYSIS **********

INITIATOR (BARLOW-PROSCHAN) MEASURE OF BASIC EVENT IMPORTANCE (MEASURE OF INTERVAL RELIABILITY)

STEADY STATE CALCULATIONS

LIMITING SYSTEM UNAVAILIBILITY= .46087E-04

MISSION TIME	10.0	H	30.0 Y
EXPECT NO OF SYSTEM FAIL	.640E-06		.168E-01

RANK	BASIC EVENT		IMPORTANCE	FAILURE RATE	MEAN FAULT DURATION		BASIC EVENT DESCRIPTION
1	TIMER	I	.844	.100E-04 HOURS	1.00	MONTHS	TIMER CONTACTS FAIL TO OPEN
2	TANK	I	.156	.100E-07 HOURS	1.00	MONTHS	TANK RUPTURES UNDER LOAD

I DENOTES INITIATING EVENT

********** PRESSURE TANK SYSTEM -- INTERVAL RELIABILITY ANALYSIS **********

ENABLER (SEQUENTIAL CONTRIBUTORY) BASIC EVENT IMPORTANCE (MEASURE OF INTERVAL RELIABILITY)

STEADY STATE CALCULATIONS

LIMITING SYSTEM UNAVAILIBILITY= .46087E-04

MISSION TIME	10.0 H	30.0 Y
EXPECT NO OF SYSTEM FAIL	.640E-06	.168E-01

RANK	BASIC EVENT	IMPORTANCE	FAILURE RATE	MEAN FAULT DURATION		BASIC EVENT DESCRIPTION
1	RVALVE	.843	.100E-03 HOURS	.500	YEARS	RELIEF VALVE FAILS TO OPERATE
2	OPERATOR	.681		.100E-01		OPERATOR FAILS TO OPEN SWITCH
3	GAUGE	.150	.100E-03 HOURS	22.0	HOURS	GAUGE STUCK OR READS LOW
4	SWITCH	.151E-01	.100E-04 HOURS	22.0	HOURS	SWITCH CONTACTS FAIL TO OPEN

1 DENOTES INITIATING EVENT

********** PRESSURE TANK SYSTEM -- INTERVAL RELIABILITY ANALYSIS **********

INITIATOR (BARLOW-PROSCHAN) MEASURE OF CUT SET IMPORTANCE (MEASURE OF INTERVAL RELIABILITY)

STEADY STATE CALCULATIONS

MISSION TIME .100E+02H .300E+02Y
EXPECT NO OF SYSTEM FAIL .640E-06 .168E-01
LIMITING SYSTEM UNAVAILABILITY= .461E-04

RANK IMPORTANCE

1 .680E+00 CUT SET 3 MEAN TIME TO OCCURRENCE = .22996E+08 HOURS 2625.1 YEARS

BASIC EVENT		FAILURE RATE	MEAN FAULT DURATION		BASIC EVENT DESCRIPTION
RVALVE		.100E-03 HOURS	.500	YEARS	RELIEF VALVE FAILS TO OPERATE
TIMER	I	.100E-04 HOURS	1.00	MONTHS	TIMER CONTACTS FAIL TO OPEN
OPERATOR			.100E-01		OPERATOR FAILS TO OPEN SWITCH

2 .156E+00 CUT SET 1 MEAN TIME TO OCCURRENCE = .10000E+09 HOURS 11416. YEARS

BASIC EVENT		FAILURE RATE	MEAN FAULT DURATION		BASIC EVENT DESCRIPTION
TANK	I	.100E-07 HOURS	1.00	MONTHS	TANK RUPTURES UNDER LOAD

3 .150E+00 CUT SET 2 MEAN TIME TO OCCURRENCE = .10453E+09 HOURS 11932. YEARS

BASIC EVENT		FAILURE RATE	MEAN FAULT DURATION		BASIC EVENT DESCRIPTION
RVALVE		.100E-03 HOURS	.500	YEARS	RELIEF VALVE FAILS TO OPERATE
TIMER	I	.100E-04 HOURS	1.00	MONTHS	TIMER CONTACTS FAIL TO OPEN
GAUGE		.100E-03 HOURS	22.0	HOURS	GAUGE STUCK OR READS LOW

4 .150E-01 CUT SET 4 MEAN TIME TO OCCURRENCE = .10453E+10 HOURS .11932E+06 YEARS

BASIC EVENT		FAILURE RATE	MEAN FAULT DURATION		BASIC EVENT DESCRIPTION
RVALVE		.100E-03 HOURS	.500	YEARS	RELIEF VALVE FAILS TO OPERATE
TIMER	I	.100E-04 HOURS	1.00	MONTHS	TIMER CONTACTS FAIL TO OPEN
SWITCH		.100E-04 HOURS	22.0	HOURS	SWITCH CONTACTS FAIL TO OPEN

I DENOTES INITIATING EVENT

********** PRESSURE TANK SYSTEM -- INTERVAL RELIABILITY ANALYSIS **********

FUSSELL-VESELY MEASURE OF CUT SET IMPORTANCE (MEASURE OF SYSTEM UNAVAILABILITY)

STEADY STATE CALCULATIONS

MISSION TIME	.100E+02H	.300E+02Y
EXPECT NO OF SYSTEM FAIL	.640E-06	.168E-01

LIMITING SYSTEM UNAVAILABILITY= .461E-04

RANK	IMPORTANCE					
1	.679E+00	CUT SET	3			
	BASIC EVENT		FAILURE RATE	MEAN FAULT DURATION		BASIC EVENT DESCRIPTION
	RVALVE		.100E-03 HOURS	.500	YEARS	RELIEF VALVE FAILS TO OPERATE
	TIMER	I	.100E-04 HOURS	1.00	MONTHS	TIMER CONTACTS FAIL TO OPEN
	OPERATOR			.100E-01		OPERATOR FAILS TO OPEN SWITCH
2	.156E+00	CUT SET	1			
	BASIC EVENT		FAILURE RATE	MEAN FAULT DURATION		BASIC EVENT DESCRIPTION
	TANK	I	.100E-07 HOURS	1.00	MONTHS	TANK RUPTURES UNDER LOAD
3	.149E+00	CUT SET	2			
	BASIC EVENT		FAILURE RATE	MEAN FAULT DURATION		BASIC EVENT DESCRIPTION
	RVALVE		.100E-03 HOURS	.500	YEARS	RELIEF VALVE FAILS TO OPERATE
	TIMER	I	.100E-04 HOURS	1.00	MONTHS	TIMER CONTACTS FAIL TO OPEN
	GAUGE		.100E-03 HOURS	22.0	HOURS	GAUGE STUCK OR READS LOW
4	.149E-01	CUT SET	4			
	BASIC EVENT		FAILURE RATE	MEAN FAULT DURATION		BASIC EVENT DESCRIPTION
	RVALVE		.100E-03 HOURS	.500	YEARS	RELIEF VALVE FAILS TO OPERATE
	TIMER	I	.100E-04 HOURS	1.00	MONTHS	TIMER CONTACTS FAIL TO OPEN
	SWITCH		.100E-04 HOURS	22.0	HOURS	SWITCH CONTACTS FAIL TO OPEN

I DENOTES INITIATING EVENT

REFERENCE TABLE FOR MIN CUT SETS

ORDER	1	2	3
NO. OF MIN CUT SETS	1	0	3

NO. OF MIN CUT SETS = 4

CUT SET NO.	ORDER	BASIC EVENTS		
1	1	TANK		
2	3	RVALVE	TIMER	GAUGE
3	3	RVALVE	TIMER	OPERATOR
4	3	RVALVE	TIMER	SWITCH

APPENDIX C

IMPORTANCE OUTPUT FOR CHLORINE VAPORIZER

```
 THE IMPORTANCE COMPUTER CODE - DEVELOPED FOR DUPONT COMP. BY TERA CORP., SYSTEM SAFETY AND RELIABILITY GROUP.
*****************************************************************************************************************

                              ***** OLD VAPORIZER - IMPORTANCE II - E-10 LIMIT *****
*****************************************************************************************************************

 INPUT DATA OPTION 4
 FAILURE RATE INPUT -- MEAN TIME TO FAILURE

 STEADY STATE CALCULATIONS

 EXPECTED NUMBER OF FAILURES CALCULATED FOR TIME =      70.00Y

 ***************************************************************

                    ** BASIC EVENT OPTIONS USED **

                                                 INITIATOR  ENABLER
            CRITICA-  UPGRADING FUSSELL-  (BARLOW-  (CONTRIB-
 BIRNBAUM     LITY     FUNCTION  VESELY     PROSCHAN)  UTORY)  STRUCTURAL

    NO        NO        NO        NO        YES       YES       NO

 ***************************************************************************

                    **  MIN CUT SET OPTIONS USED  **

                 INITIATOR
              (BARLOW-PROSCHAN)          FUSSELL-VESELY

                      YES                       NO

 ***************************************************************************

 MAXIMUM CUT SET ORDER FOR THE BARLOW-PROSCHAN MEASURE OF CUT SET IMPORTANCE =  10

 INFORMATION ON DETAILED CUT SET OUTPUT -- NN =100 AND FACTOR =.0100
```

********** ***** OLD VAPORIZER - IMPORTANCE II - E-10 LIMIT ***** **********

** BASIC EVENT DATA **

MEAN TIME TO FAILURE	MEAN FAULT DURATION	NAME	ENABLER	DESCRIPTION
50.00 YEARS	0.00 YEARS	E500		LOSE AIR - SYSTEM
50.00 YEARS	0.00 YEARS	E505		LO AIR - SYSTEM
30.00 YEARS	0.00 YEARS	E506		LOSE 24V - SYSTEM
20.00 YEARS	0.00 YEARS	E507		LO 24V - SYSTEM
20.00 YEARS	0.50 YEARS	E700	*	*PV-67-1 STUCK
45.00 YEARS	0.50 YEARS	E701	*	*SV-A STUCK
20.00 YEARS	0.50 YEARS	E702	*	*SV-A VENT BLOCKED
80.00 YEARS	0.50 YEARS	E703	*	*R-999 MISC FLS SHUT
120.00 YEARS	0.50 YEARS	E704	*	*R-999 CONTACTS WELDED
70.00 YEARS	0.50 YEARS	E705	*	*R-999 SHORTED
60.00 YEARS	0.50 YEARS	E706	*	*R-999 JUMPERED
35.00 YEARS	0.50 YEARS	E707	*	*TS-67 MISC FLS SHUT
35.00 YEARS	0.50 YEARS	E708	*	*TS-67 MISSET
40.00 YEARS	0.50 YEARS	E709	*	*TS-67 SHORTED
20.00 YEARS	0.50 YEARS	E710	*	*TS-67 OPEN INPUT
35.00 YEARS	0.50 YEARS	E717	*	*LS-67A MISC FAILS CLOSED
35.00 YEARS	0.50 YEARS	E718	*	*LS-67A MISSET
40.00 YEARS	0.50 YEARS	E719	*	*LS-67A SHORTED
35.00 YEARS	0.50 YEARS	E720	*	*TS-68 MISC FAILS CLOSED
35.00 YEARS	0.50 YEARS	E721	*	*TS-68 MISSET
40.00 YEARS	0.50 YEARS	E722	*	*TS-68 SHORTED
20.00 YEARS	0.00 YEARS	E723	*	*TT-68 MISC FAILS HI
30.00 YEARS	0.01 YEARS	E724	*	*TT-68 STUCK
10.00 YEARS	0.01 YEARS	E725	*	*TT-68 LOW AIR - LOCAL
20.00 YEARS	0.00 YEARS	E726	*	*PV-67 STUCK
10.00 YEARS	0.00 YEARS	E727	*	*PV-67 LOW AIR - LOCAL
45.00 YEARS	0.50 YEARS	E728	*	*SV-B STUCK
20.00 YEARS	0.50 YEARS	E729	*	*SV-B VENT BLOCKED
20.00 YEARS	0.00 YEARS	E730	*	*LC-67-1 STUCK GAGE
10.00 YEARS	0.00 YEARS	E731	*	*LC-67-1 LEAK GAGE
60.00 YEARS	0.00 YEARS	E732	*	*LC-67-1 GAGE WOUND-UP
40.00 YEARS	0.01 YEARS	E733	*	*L-67-2 LO 24V - LOCAL
40.00 YEARS	0.01 YEARS	E734	*	*L-67-2 HI RESISTANCE
30.00 YEARS	0.01 YEARS	E735		L-67-2 STUCK
40.00 YEARS	0.01 YEARS	E736		L-67-2 OUTPUT LEAK
10.00 YEARS	0.00 YEARS	E737		L-67-2 LOSE AIR - LOCAL
40.00 YEARS	0.00 YEARS	E738		L-67-2 LOSE 24V - LOCAL
20.00 YEARS	0.00 YEARS	E739		L-67-2 LOSE INPUT
40.00 YEARS	0.00 YEARS	E740		L-67-2 MISC FAIL LO
60.00 YEARS	0.00 YEARS	E741		L-67-2 SHORT INPUT
20.00 YEARS	0.00 YEARS	E742		L-67-2 REVERSE POLARITY
40.00 YEARS	0.01 YEARS	E743		LT-67 HI LOOP RESISTANCE
40.00 YEARS	0.00 YEARS	E744		LT-67 GROUND
30.00 YEARS	0.01 YEARS	E745	*	*LT-67 STUCK
10.00 YEARS	0.00 YEARS	E746		LT-67 MISC FAILS LO
30.00 YEARS	0.00 YEARS	E747		LT-67 REVERSE POLARITY
40.00 YEARS	0.00 YEARS	E748		LT-67 LOSE LOCAL POWER
0.0	0.0 CONSTP	E749	*	LT-67
20.00 YEARS	0.01 YEARS	E750	*	*TG-68 STUCK
20.00 YEARS	0.01 YEARS	E751	*	*TT-68 STUCK
20.00 YEARS	0.00 YEARS	E752	*	*TT-68 FAILS HI
40.00 YEARS	0.00 YEARS	E753	*	*LA-67 NO ALARM
35.00 YEARS	0.50 YEARS	E754	*	*LS-67 MISC FAILS

********** ***** OLD VAPORIZER - IMPORTANCE II - E-10 LIMIT ***** **********

STEADY STATE SYSTEM CHARACTESTICS

TOP EVENT RATE (PER HOUR) = .74909E-04 TOP EVENT RATE (PER YEAR) = .65620

MEAN TIME TO SYSTEM FAILURE = 13337. HOURS 1.5224 YEARS

MEAN TIME TO SYSTEM REPAIR = 12.832 HOURS .5346R DAYS.

LIMITING SYSTEM UNAVAILIBILITY= .96125E-03

MISSION TIME 20.0 Y
EXPECT NO OF SYSTEM FAIL 13.1

********** ***** OLD VAPORIZER - IMPORTANCE I1 - E-10 LIMIT ***** **********

INITIATOR (BARLOW-PROSCHAN) MEASURE OF BASIC EVENT IMPORTANCE

STEADY STATE CALCULATIONS

LIMITING SYSTEM UNAVAILIBILITY= .96125E-03

EXPECT NO OF SYSTEM FAIL 13.1
MISSION TIME 20.0 Y

RANK	BASIC EVENT		IMPORTANCE	MEAN TIME TO FAILURE		MEAN FAULT DURATION		BASIC EVENT DESCRIPTION	
1	E746	I	.148	10.0	YEARS	.685E-03	YEARS	LT-62	MISC FAILS LO
1	E737	I	.148	10.0	YEARS	.685E-03	YEARS	L-62-2	LOSE AIR - LOCAL
2	E739	I	.742E-01	20.0	YEARS	.685E-03	YEARS	L-62-2	LOSE INPUT
2	E742	I	.742E-01	20.0	YEARS	.685E-03	YEARS	L-62-2	REVERSE POLARITY
3	E767	I	.524E-01	10.0	YEARS	.228E-03	YEARS	LC-62-1	LOSE AIR - LOCAL
4	E747	I	.495E-01	30.0	YEARS	.685E-03	YEARS	LT-62	REVERSE POLARITY
4	E506	I	.495E-01	30.0	YEARS	.285E-04	YEARS	LOSE 24V - SYSTEM	
5	E736	I	.371E-01	40.0	YEARS	.548E-02	YEARS	L-62-2	OUTPUT LEAK
5	E740	I	.371E-01	40.0	YEARS	.685E-03	YEARS	L-62-2	MISC FAIL LO
5	E748	I	.371E-01	40.0	YEARS	.685E-03	YEARS	LT-62	LOSE LOCAL POWER
5	E738	I	.371E-01	40.0	YEARS	.685E-03	YEARS	L-62-2	LOSE 24V - LOCAL
5	E744	I	.371E-01	40.0	YEARS	.685E-03	YEARS	LT-62	GROUND
6	E500	I	.297E-01	50.0	YEARS	.285E-03	YEARS	LOSE AIR - SYSTEM	
7	E781	I	.262E-01	20.0	YEARS	.228E-03	YEARS	LC-62-1	MISC FAILS LO
7	E768	I	.262E-01	20.0	YEARS	.228E-03	YEARS	LC-62-1	OUTPUT LEAK
7	E766	I	.262E-01	20.0	YEARS	.228E-03	YEARS	PT-780	FAILS HI
8	E741	I	.247E-01	60.0	YEARS	.685E-03	YEARS	L-62-2	SHORT INPUT
9	E765	I	.175E-01	30.0	YEARS	.228E-03	YEARS	PR-GI	FAILS HI
9	E770	I	.175E-01	30.0	YEARS	.228E-03	YEARS	LC-62-1	MANUAL LOADING(-10)
9	E769	I	.175E-01	30.0	YEARS	.228E-03	YEARS	LC-62-1	SET POINT(-10)
9	E764	I	.175E-01	30.0	YEARS	.114E-03	YEARS	LY-62	REVERSED
10	E771	I	.131E-01	40.0	YEARS	.114E-03	YEARS	LY-62	FAILS OPEN
11	E776	I	.156E-02	20.0	YEARS	.114E-03	YEARS	P800(+10)	
12	E505	I	.834E-05	50.0	YEARS	.114E-03	YEARS	LO AIR - SYSTEM	
13	E735	I	.742E-05	30.0	YEARS	.548E-02	YEARS	L-62-2	STUCK
14	E743	I	.591E-05	40.0	YEARS	.548E-02	YEARS	LT-62	HI LOOP RESISTANCE
15	E507	I	.278E-05	20.0	YEARS	.114E-03	YEARS	LO 24V - SYSTEM	

I DENOTES INITIATING EVENT

********** ***** OLD VAPORIZER - IMPORTANCE II + E-10 LIMIT ***** **********

ENABLER (SEQUENTIAL CONTRIBUTORY) BASIC EVENT IMPORTANCE

STEADY STATE CALCULATIONS

LIMITING SYSTEM UNAVAILIBILITY= .96125E-03

EXPECT NO OF SYSTEM FAIL 13.1
MISSION TIME 20.0 Y

RANK	BASIC EVENT		IMPORTANCE	MEAN TIME TO FAILURE		MEAN FAULT DURATION		BASIC EVENT DESCRIPTION
1	E759		.820	.0		.800	CONSTP	*NO OPR RESPONSE TO 8814 & 8820
2	E763		.816	.0		.800	CONSTP	*NO OPR RESPONSE TO 8814
3	E774		.143	.0		.100	CONSTP	*OPERATOR BUSY
3	E773		.143	.0		.100	CONSTP	*OPERATOR NOT PRESENT
3	E772		.143	.0		.100	CONSTP	*WRONG OPERATOR RESPONSE
4	E760		.989E-01	.0		.100	CONSTP	*NO OPR RESPONSE TO 8814 & 8819
5	E775		.715E-01	.0		.500E-01	CONSTP	*OPERATOR -- MISC NO RESPONSE
6	E761		.419E-01	.0		.800	CONSTP	*NO OPR RESPONSE TO 8820
7	E758		.201E-01	.0		.100	CONSTP	*NO OPR RESPONSE TO 8820 & 8819
8	E757		.136E-01	20.0	YEARS	.500	YEARS	*LS-62 OPEN INPUT
9	E755		.777E-02	35.0	YEARS	.500	YEARS	*LS-62 MISSET
9	E754		.777E-02	35.0	YEARS	.500	YEARS	*LS-62 MISC FAILS
10	E756		.680E-02	40.0	YEARS	.500	YEARS	*LS-62 SHORTED
11	E780		.131E-02	.0		.500E-01	CONSTP	*LC-62-1 ON MANUAL
12	E751		.286E-03	20.0	YEARS	.548E-02	YEARS	*TT-68 STUCK
12	E750		.286E-03	20.0	YEARS	.548E-02	YEARS	*TG-68 STUCK
13	E745		.124E-03	30.0	YEARS	.548E-02	YEARS	*LT-62 STUCK
14	E735	I	.111E-03	30.0	YEARS	.548E-02	YEARS	L-62-2 STUCK
15	E727		.942E-04	10.0	YEARS	.685E-03	YEARS	*PV-67 LOW AIR - LOCAL
16	E743	I	.931E-04	40.0	YEARS	.548E-02	YEARS	LT-62 HI LOOP RESISTANCE
17	E734		.831E-04	40.0	YEARS	.548E-02	YEARS	*L-62-2 HI RESISTANCE
17	E733		.831E-04	40.0	YEARS	.548E-02	YEARS	*L-62-2 LO 24V - LOCAL
18	E726		.458E-04	20.0	YEARS	.685E-03	YEARS	*PV-67 STUCK
19	E752		.258E-04	20.0	YEARS	.685E-03	YEARS	*TT-68 FAILS HI
20	E753		.793E-05	40.0	YEARS	.685E-03	YEARS	*LA-62 NO ALARM
21	E731		.427E-05	10.0	YEARS	.685E-03	YEARS	*LC-62-1 LEAK CAGE
22	E767	I	.237E-05	10.0	YEARS	.228E-03	YEARS	LC-62-1 LOSE AIR - LOCAL
23	E507	I	.845E-06	20.0	YEARS	.114E-03	YEARS	LO 24V - SYSTEM
24	E505	I	.781E-06	50.0	YEARS	.114E-03	YEARS	LO AIR - SYSTEM
25	E781	I	.640E-06	20.0	YEARS	.228E-03	YEARS	LC-62-1 MISC FAILS LO
25	E768	I	.640E-06	20.0	YEARS	.228E-03	YEARS	LC-62-1 OUTPUT LEAK
25	E766	I	.640E-06	20.0	YEARS	.228E-03	YEARS	PT-780 FAILS HI
26	E770	I	.427E-06	30.0	YEARS	.228E-03	YEARS	LC-62-1 MANUAL LOADING(-10)
26	E769	I	.427E-06	30.0	YEARS	.228E-03	YEARS	LC-62-1 SET POINT(-10)
26	E765	I	.427E-06	30.0	YEARS	.228E-03	YEARS	PR-61 FAILS HI
27	E764	I	.212E-06	30.0	YEARS	.114E-03	YEARS	LV-62 REVERSED
28	E776	I	.204E-06	20.0	YEARS	.114E-03	YEARS	P800(+10)
29	E771	I	.159E-06	40.0	YEARS	.114E-03	YEARS	LV-62 FAILS OPEN

I DENOTES INITIATING EVENT

```
**********                    ***** OLD VAPORIZER - IMPORTANCE II - E-10 LIMIT *****                    **********

        INITIATOR (BARLOW-PROSCHAN) MEASURE OF CUT SET IMPORTANCE

STEADY STATE CALCULATIONS

  EXPECT NO OF SYSTEM FAIL   0.131E+02
  MISSION TIME              0.200E+02Y
LIMITING SYSTEM UNAVAILABILITY= 0.961E-03

RANK  IMPORTANCE

   1 0.122E+00  CUT SET    61 MEAN TIME TO OCCURRENCE =  .10961E+06 HOURS  12.512     YEARS

      BASIC EVENT    MEAN TIME TO FAILURE   MEAN FAULT DURATION      BASIC EVENT DESCRIPTION

       E746     1     0.100E+02 YEARS          0.001 YEARS      LT-62    RISC FAILS LO
       E763           0.0                      0.800 CONSTP     *NO OPR RESPONSE TO 8814

   1 0.122E+00  CUT SET   131 MEAN TIME TO OCCURRENCE =  .10961E+06 HOURS  12.512     YEARS

      BASIC EVENT    MEAN TIME TO FAILURE   MEAN FAULT DURATION      BASIC EVENT DESCRIPTION

       E737     1     0.100E+02 YEARS          0.001 YEARS      L-62-2   LOSE AIR - LOCAL
       E763           0.0                      0.800 CONSTP     *NO OPR RESPONSE TO 8814

   1 0.122E+00  CUT SET    63 MEAN TIME TO OCCURRENCE =  .10961E+06 HOURS  12.512     YEARS

      BASIC EVENT    MEAN TIME TO FAILURE   MEAN FAULT DURATION      BASIC EVENT DESCRIPTION

       E746     1     0.100E+02 YEARS          0.001 YEARS      LT-62    RISC FAILS LO
       E759           0.0                      0.800 CONSTP     *NO OPR RESPONSE TO 8814 & 8820

   1 0.122E+00  CUT SET   133 MEAN TIME TO OCCURRENCE =  .10961E+06 HOURS  12.512     YEARS

      BASIC EVENT    MEAN TIME TO FAILURE   MEAN FAULT DURATION      BASIC EVENT DESCRIPTION

       E737     1     0.100E+02 YEARS          0.001 YEARS      L-62-2   LOSE AIR - LOCAL
       E759           0.0                      0.800 CONSTP     *NO OPR RESPONSE TO 8814 & 8820

   2 0.609E-01  CUT SET   111 MEAN TIME TO OCCURRENCE =  .21922E+06 HOURS  25.025     YEARS

      BASIC EVENT    MEAN TIME TO FAILURE   MEAN FAULT DURATION      BASIC EVENT DESCRIPTION

       E739     1     0.200E+02 YEARS          0.001 YEARS      L-62-2   LOSE INPUT
       E763           0.0                      0.800 CONSTP     *NO OPR RESPONSE TO 8814

   2 0.609E-01  CUT SET    81 MEAN TIME TO OCCURRENCE =  .21922E+06 HOURS  25.025     YEARS

      BASIC EVENT    MEAN TIME TO FAILURE   MEAN FAULT DURATION      BASIC EVENT DESCRIPTION

       E742     1     0.200E+02 YEARS          0.001 YEARS      L-62-2   REVERSE POLARITY
       E763           0.0                      0.800 CONSTP     *NO OPR RESPONSE TO 8814
```

DISTRIBUTION:

US NRC Distribution Contractor (CDSI) (320 copies for RS)
7300 Pearl Street
Bethesda, MD 20014

4414 R. B. Norrell (50)
8214 M. A. Pound
3141 L. J. Erickson (5)
3151 W. L. Garner (3)
For DOE/TIC (Unlimited Release)
3154-3 R. B. Campbell (25)
For NRC distribution to NTIS

☆U.S. GOVERNMENT PRINTING OFFICE: 1981-0-777-023/544