NUCLEAR SCIENCE AND ENGINEERING: 62, 20-34 (1977)

Fault Trees for Diagnosis of System Fault Conditions

Howard E. Lambert

Lawrence Livermore Laboratory, P. O. Box 808, Livermore, California 94550

and

George Yadigaroglu

University of California, Department of Nuclear Engineering, Berkeley, California 94720

Received May 10, 1976
Revised August 2, 1976

Methods for generating repair checklists on the basis of fault tree logic and probabilistic importance are presented. A one-step-ahead optimization procedure, based on the concept of component criticality, minimizing the expected time to diagnose system failure is outlined. Options available to the operator of a nuclear power plant when system fault conditions occur are addressed. A low-pressure emergency core cooling injection system, a standby safeguard system of a pressurized water reactor power plant, is chosen as an example illustrating the methods presented.

I. INTRODUCTION

Fault tree analysis (FTA) is a method of system safety analysis that evolved from the aerospace industry in the early 1960's. A fault tree is a Boolean-logic model that depicts the parallel and sequential combinations of events that cause a top event to occur. The top event usually represents an undesired system state or hazardous condition. The first step in FTA is fault tree construction, i.e., the systematic identification of links and relationships between system components that could produce the conditions necessary for the occurrence of the top event and graphical display according to a standard format. Once constructed, the fault tree can be evaluated either qualitatively or quantitatively, depending on the scope, extensiveness, and use of the analysis. An important step in a qualitative evaluation is the determination of the minimal cut sets, i.e., the set of basic events whose occurrence causes the top event to occur. The basic events are events such as generic hardware failures, human error, or environmental conditions, and they represent the limit of resolution in the fault tree. Quantitative evaluations are concerned with the determination of probabilistic characteristics of the fault tree such as the probability of the top event or the probabilistic importance of basic events or minimal cut sets. The reader should consult Refs. 1 through 9 for a general discussion of FTA and

[1]G. E. CUMMINGS, "Application of the Fault Tree Technique to a Nuclear Reactor Containment System," in *Reliability and Fault Tree Analysis*, R. E. BARLOW, J. B. FUSSELL, and N. D. SINGPURWALLA, Eds., *SIAM* (1975).

[2]J. B. FUSSELL, *Fault Tree Analysis—Concepts and Techniques*, NATO Advanced Study Inst. on Generic Techniques of System Reliability Assessment, Liverpool, England (1973).

[3]D. F. HAASL, "Advanced Concepts in Fault Tree Analysis," in *Proc. Systems Safety Symp.*, University of Washington and the Boeing Company, Seattle, Washington (1965).

[4]D. F. HAASL, "Fault Tree Construction Guide," L/C F08635-75-C-0006, Safety Engineering Division, Elgin Air Force Base, Florida (1974).

[5]H. E. LAMBERT, "Systems Safety Analysis and Fault Tree Analysis," UCID 16238, Lawrence Livermore Laboratory (1973).

[6]G. J. POWERS, F. C. TOMPKINS, and S. A. LAPP, "A Safety Simulation Language for Chemical Processes: A Procedure for Fault Tree Synthesis," in *Reliability and Fault Analysis*, R. E. BARLOW, J. B. FUSSELL, and N. D. SINGPURWALLA, Eds., *SIAM* (1975).

[7]*Reactor Safety Study*, WASH-1400, NUREG-75/014, U.S. Nuclear Regulatory Commission (1975).

[8]T. H. SMITH et al., "A Risked-Based Fault Tree Analysis Method for Identification, Preliminary Evaluation, and Screening of Potential Accident Release Sequences in Nuclear Fuel Cycle Operations," BNWL-1959, Battelle Pacific Northwest Laboratories (1976).

[9]J. YOUNG, "Using the Fault Tree Techniques," in *Reliability and Fault Tree Analysis*, R. E. BARLOW, J. B. FUSSELL, and N. D. SINGPURWALLA, Eds., *SIAM* (1975).

Refs. 10 through 14 for the probabilistic evaluation of fault trees.

Traditionally, FTA has been used as a design tool. It can identify potential accidents in system design and can help eliminate costly design changes and retrofits. More recently, it has been used as a tool for evaluating the safety of existing complex systems such as nuclear power plants.[7] In this paper, FTA is used as a diagnostic tool. We show how FTA can predict the most likely causes of failure in the event of a system breakdown. The prediction or diagnosis is accomplished with maximum economy of time and effort, since learning by experience is included in the analytical framework.

To accomplish these objectives, the following topics are covered:

1. concepts of component criticality and probabilistic importance
2. generation of repair checklists on the basis of fault tree logic
3. system diagnosis under a time constraint.

As an example, we choose the low-pressure emergency coolant injection system (LPIS) of a pressurized water reactor (PWR) nuclear power plant for which we generate repair checklists.

We conclude the paper by considering the options available to an operator when system fault conditions occur and how the best future course of system operation can be determined on the basis of a risk assessment. In particular, we consider the decision regarding shutdown of a PWR plant when the LPIS is found partly inoperable during plant operation.

II. PROBABILISTIC IMPORTANCE

Some probabilistic aspects of FTA are discussed in this section to introduce the concepts of probabilistic importance. By computing probabilistic importance, we generate a numerical ranking of events in a fault tree. Then, we can determine the component malfunctions and fault conditions most likely to be contributing to the occurrence of the specified top event. As we examine the system, we can incorporate the knowledge we gain into the importance rankings, making FTA a truly interactive diagnostic tool.

The purpose of this section is to:

1. present the mathematical notation used in the remainder of the paper
2. explain the concept of component criticality
3. briefly summarize the concepts of probabilistic importance.

The reader should consult Refs. 13, 15, 16, and 17 for a more detailed treatment of the subject of probabilistic importance.

II.A. Mathematical Notation (Ref. 18)

Probabilistic definitions of importance can be expressed in terms of a g function that establishes the probability of the top event in terms of basic-event probabilities. To generate this function, we need a Boolean expression for the top event in terms of the Boolean variables of the basic events. We describe the occurrence or nonoccurrence of each basic event at time t by an indicator variable, $Y_i(t)$

$$Y_i(t) = \begin{cases} 1 \text{ if basic event } i \text{ has occurred at time } t \\ 0 \text{ otherwise} \end{cases} .$$

The top event is assigned an indicator variable or structure function, $\psi[\boldsymbol{Y}(t)]$, such that

$$\psi[\boldsymbol{Y}(t)] = \begin{cases} 1 \text{ if the top event has occurred at time } t \\ 0 \text{ otherwise} \end{cases} ,$$

where

$$[\boldsymbol{Y}(t)] = [\, Y_1(t),\ Y_2(t),\ \ldots,\ Y_n(t)]$$

is the vector of basic-event indicator variables at time t and n is the number of basic events in the fault tree.

There are two operators that can be used to express $\psi[\boldsymbol{Y}(t)]$ in terms of $\boldsymbol{Y}(t)$: the AND operator, $\prod$, and the OR operator, $\coprod$. The AND structure function is given by

$$\psi[\boldsymbol{Y}(t)] = \prod_{i=1}^{n} Y_i(t) = Y_1(t) \cdot Y_2(t) \cdot \ldots \cdot Y_n(t) \quad ,$$

[10]G. APOSTOLAKIS, "Mathematical Methods of Probabilistic Safety Analysis," UCLA-ENG-7464, University of California at Los Angeles (1974).

[11]R. E. BARLOW and F. PROSCHAN, *Statistical Theory of Reliability and Life Testing*, Holt, Rinehart, and Winston, New York (1975).

[12]J. B. FUSSELL, "How to Hand-Calculate System Reliability Characteristics," *IEEE Trans. Reliab.*, **R-24**, *3* (1975).

[13]H. E. LAMBERT, "Fault Trees for Decision Making in Systems Analysis," UCRL-51829, Lawrence Livermore Laboratory (1975).

[14]W. E. VESELY, *Nucl. Eng. Des.*, **13**, 337 (1970).

[15]R. E. BARLOW and F. PROSCHAN, *Stoch. Proc. Their Appl.*, **3**, 153 (1975).

[16]P. CHATTERJEE, "Fault Tree Analysis: Reliability Theory and Systems Safety Analysis," ORC 74-34, Operations Research Center, University of California, Berkeley (1974).

[17]H. E. LAMBERT, "Measures of Importance of Events and Cut Sets in Fault Trees," in *Reliability and Fault Tree Analysis*, R. E. BARLOW, J. B. FUSSELL, and N. D. SINGPURWALLA, Eds., *SIAM* (1975).

[18]The notation of this section is that of coherent structure theory (see Ref. 11).

while the structure function for an OR gate with n inputs is

$$\psi[\mathbf{Y}(t)] = \coprod_{i=1}^{n} Y_i(t) \stackrel{\text{def}}{=} 1 - \prod_{i=1}^{n} [1 - Y_i(t)] \quad .$$

At this point it is convenient to define basic events in the fault tree as component failures and to represent the top event as a system failure. With this convention, $Y_i = 1$ denotes failure of component i. The structure function for a parallel system is an AND structure function since *all* components must fail to cause the system to fail. For a series system, an OR structure function must be used.

Component i is *critical* to system failure at time t if the system is in a state denoted as $\mathbf{Y}(t)$ such that the system makes a transition from the unfailed state to a failed state when component i fails. In terms of the notation previously described, the above statement implies

$$\psi[1_i,\mathbf{Y}(t)] - \psi[0_i,\mathbf{Y}(t)] = \begin{cases} 1 \text{ if component } i \text{ is critical to system failure at time } t \\ 0 \text{ otherwise} \end{cases} ,$$

where the meaning of the abbreviated notation used is

$$[1_i,\mathbf{Y}(t)] = [Y_1(t), \ldots, Y_{i-1}(t), 1, Y_{i+1}(t), \ldots, Y_n(t)]$$

$$[0_i,\mathbf{Y}(t)] = [Y_1(t), \ldots, Y_{i-1}(t), 0, Y_{i+1}(t), \ldots, Y_n(t)] \quad .$$

In a parallel system, for a component to be critical to system failure at time t, we must have

$$\psi[1_i,\mathbf{Y}(t)] - \psi[0_i,\mathbf{Y}(t)] = \coprod_{\substack{j=1 \\ j\neq i}}^{n} Y_j(t) = 1 \quad ,$$

which implies that $Y_j(t) = 1$ for all $j \neq i$. Thus, in a parallel system for a component to be critical to system failure at time t, all the remaining components must have failed at time t.

For a series system, we must have

$$\psi[1_i,\mathbf{Y}(t)] - \psi[0_i,\mathbf{Y}(t)] = \prod_{\substack{j=1 \\ j\neq i}}^{n} [1 - Y_j(t)] = 1$$

$$\text{if } Y_j(t) = 0 \text{ for all } j \neq i \quad ,$$

i.e., for a series system, a component is critical to system failure at time t if all the remaining components have not failed at time t.

Now let us consider the probabilistic characteristics of basic events. If the state of each basic event is random, then the probability that event i occurs at time t is given by the expectation of the Boolean indicator variable, Y_i,

$$E[Y_i(t)] = \text{Prob}[Y_i(t) = 1] \stackrel{\text{def}}{=} q_i(t) \quad .$$

If the basic event, i, describes failure of an unrepairable component, then $q_i(t)$ is given by

$$q_i(t) = 1 - \exp\left[-\int_0^t \lambda_i(t')dt'\right] \quad ,$$

where $\lambda_i(t')dt'$ is the conditional probability of failure in $(t',t' + dt')$ and is commonly referred to as the failure rate. If repair of the failed component is permitted, either by scheduled or off-schedule maintenance,[19] then the probability that component i is failed at time t is given by its unavailability, $\overline{A}_i(t)$,

$$q_i(t) \stackrel{\text{def}}{=} \overline{A}_i(t) \quad ,$$

which represents the fraction of time component i is expected to be failed at time t. For off-scheduled maintenance, the asymptotic value of the unavailability is given by

$$\lim_{t\to\infty} \overline{A}_i(t) = \frac{\tau_i}{\tau_i + \mu_i} \quad ,$$

where τ_i is the mean time to repair for component i and μ_i is the mean time to failure for component i.

We now consider the top event or system characteristics. If the basic events are statistically independent, then the probability that the top event occurs by time t is given by the g function mentioned previously, $g[\mathbf{q}(t)]$. It can be recognized that

$$E\{\psi[\mathbf{Y}(t)]\} = \text{Prob}\{\psi[\mathbf{Y}(t)] = 1\} = g[\mathbf{q}(t)] \quad .$$

The system reliability is simply $1 - g[\mathbf{q}(t)]$. For example, for a parallel system of two components, $g[\mathbf{q}(t)]$ is given by

$$g[\mathbf{q}(t)] = q_1(t) \cdot q_2(t) \quad ,$$

and the probability that component 1 is critical to system failure is

$$g[1,q_2(t)] - g[0,q_2(t)] = q_2(t) \quad .$$

For a series system of two components,

$$g[\mathbf{q}(t)] = 1 - [1 - q_1(t)][1 - q_2(t)] \quad ,$$

and the probability that component 1 is critical to system failure is

$$g[1,q_2(t)] - g[0,q_2(t)] = 1 - q_2(t) \quad .$$

Note that for statistically independent basic events, the g function is obtained by eliminating powers of indicator variables and then merely

[19] In off-schedule maintenance, repair (or replacement) of the failed component takes place immediately on detection of the failure, whereas in scheduled maintenance, repair occurs at the end of some inspection interval.

substituting $q_i(t)$ for $Y_i(t)$ in the Boolean structure function.

The above results are well established in reliability theory (see, for example, Refs. 10, 11, and 20).

II.B. Probabilistic Importance

We now consider probabilistic expressions for ranking basic events according to their importance in a fault tree. For the remainder of the paper, we assume that all basic events are statistically independent. Further, we assume that the system structure function is *coherent*, i.e., $\psi[\boldsymbol{Y}(t)]$ is a monotonic Boolean function. The implications of this statement are discussed in Ref. 11.

We introduce two measures of importance computed in terms of $g[\boldsymbol{q}(t)]$, a function that describes the state of the system at one point in time.

In 1969, Birnbaum[21] introduced the concept of importance for coherent systems. He defined the reliability importance of a component i as the rate at which system reliability improves as the reliability of component i improves. If by following our convention we construct a fault tree where the top event is system failure and the basic events are component failures, then the Birnbaum definition of component importance becomes

$$\frac{\partial g[\boldsymbol{q}(t)]}{\partial q_i(t)} = g[1_i, \boldsymbol{q}(t)] - g[0_i, \boldsymbol{q}(t)] \stackrel{\text{def}}{\equiv} \Delta g_i(t) \quad .$$

The partial derivative relationship holds by the idempotency law for Boolean variables, i.e., $\psi[\boldsymbol{Y}(t)]$ is a linear function of $Y_i(t)$, which implies that $g[\boldsymbol{q}(t)]$ is linear in $q_i(t)$ when independence is assumed. Stated in other terms, the Birnbaum measure of importance is the probability of a component being critical to system failure. It is possible that by the time system failure is observed, more than one min cut sets could have failed. In this case, restoring a failed component to a working state does not necessarily restore the system to a working state. In other words, it is possible that failure of a component can be contributing to system failure without being critical. (Component i is contributing to system failure if a min cut set containing i has failed.) If we let

$\psi_K^i[\boldsymbol{Y}(t)]$ = Boolean structure function for the union of all cut sets that contain basic event, i

and

$$E\{\psi_K^i[\boldsymbol{Y}(t)]\} \stackrel{\text{def}}{=} g_i[\boldsymbol{q}(t)] \quad ,$$

then the probability that component i is contributing to system failure is given by

$$\frac{g_i[\boldsymbol{q}(t)]}{g[\boldsymbol{q}(t)]} \stackrel{\text{def}}{=} I_i^{FV}(t) \quad .$$

This concept of importance was first proposed by Vesely[22] and Fussell,[12] who introduced it in the literature. Both the Birnbaum and Fussell-Vesely measures of importance are used here.

As an example of the Fussell-Vesely measure of importance, we consider a series and a parallel system of two components. In a series system, there are two min cut sets, (component 1 fails) and (component 2 fails), simply denoted as (1) and (2). The probability that component 1 is contributing to system failure given that system failure has occurred is given by

$$I_1^{FV} = \frac{g_1[\boldsymbol{q}(t)]}{g[\boldsymbol{q}(t)]} = \frac{q_1(t)}{1 - [1 - q_1(t)][1 - q_2(t)]} \quad .$$

In the parallel system of two components, there is one min cut set (1, 2). The Fussell-Vesely measure for component 1 in this case is

$$I_1^{FV} = \frac{q_1(t)q_2(t)}{q_1(t)q_2(t)} = 1 \quad .$$

Other measures of importance can be defined to describe system failure in terms of sequences of component failures. These are discussed by Barlow and Proschan[15] and by Lambert.[13]

III. GENERATION OF REPAIR CHECKLISTS

In this section we present methods by which repair checklists can be generated. If a fault tree can accurately simulate system failure, i.e., if all failures can be described in terms of Boolean logic, then the fault tree can be quantitatively evaluated to determine the critical events. In the event of system or subsystem breakdown, a repair checklist can be generated for an operator to follow in diagnosing the particular system failure. The basic events on this checklist can be ordered according to their importance when system failure occurs.

III.A. Checklist Generation Scheme

The order in which the components are listed on the checklist should reflect the knowledge that the operator gains about the system as he sequentially examines each component in the checklist. The ranking of the basic events should be done on a conditional basis, i.e., in the framework of

[20] A. E. GREEN and A. J. BOURNE, *Reliability Technology*, John Wiley and Sons, Inc., London (1972).

[21] Z. W. BIRNBAUM, "On the Importance of Different Component and a Multicomponent System," *Multivariate Analysis-II*, P. R. KRISHNAIAH, Ed., Academic Press, New York (1969).

[22] W. E. VESELY, Division of Reactor Safety Research, U.S. Nuclear Regulatory Commission, Private Communication (1972).

learning by experience. For example, if the operator finds that the first event on the checklist has not occurred, then the second event on the checklist should be the most critical to system failure, *given* that the first event has not occurred. In general, the i'th event is most critical to system failure, given that the first $(i - 1)$ events have not occurred.

If a component, say i, in the checklist is found to be failed and is contained in a cut set of order two or higher, then a *sublist* is generated for component i. In this sublist, we rank the cut sets containing the failed component, i, according to their importance computed on a conditional basis. The operator then checks the components in the cut sets that contain component i.

In general, it is unwise to include the triple or higher order cut sets in the sublist since for maintained or inspected systems, the simultaneous occurrence of three independent events is rare. It is felt that the criteria adopted by the Reactor Safety Study[7] also are valid for checklist generation. According to these criteria, we retain the most important cut sets only:

1. single passive faults
2. single active faults
3. double active faults.[7]

If these criteria are adopted, the sublist becomes a list of active components ranked according to their probability of occurrence. The advantage of keeping only the most important cut sets is that a multitude of trival combinations that are generated normally from typical fault trees are eliminated from consideration. It must be kept in mind that the purpose of the checklist is to aid the operator in making decisions under a time constraint.

Although all basic events are assumed to be independent, dependent failures can be incorporated into the scheme outlined above. This is accomplished by including basic events that cause secondary failures, i.e., environmental or operational conditions capable of simultaneously failing two or more system components. When we check for these secondary failure conditions, we generate a sublist of the components sensitive to these conditions.

In generating the checklist, the possibility of false alarms should also be taken into account by considering the reliability of the monitoring device that indicated system failure.

III.B. Checklist Generation for the LPIS

The system that is chosen for checklist generation is the LPIS of a PWR power plant. The LPIS is a standby safety system, part of the emergency core cooling system (ECCS). A simplified piping schematic of this system is shown in Fig. 1. Following a loss-of-coolant accident (LOCA), the LPIS operation is considered successful when at least one of its legs discharges water continuously at a rate of 3000 g/min and a pressure of 300 psi into the cold legs of the reactor.

Part of the control circuit that actuates the LPIS is shown in Fig. 2, which includes a brief system description. For simplicity, it is assumed that this system is tested by closing a switch (not shown) that energizes relays that in turn close contacts P1, P2, and P3.

A checklist is generated for leg A for the case when the pressure gauge fails to indicate 300 psi when the test switch is closed. This checklist contains the list of events that are most likely to have occurred under those conditions.

Part of the fault tree[13] that illustrates the failure of leg A of the LPIS system is shown in Fig. 3. The remainder of the fault tree consists of four additional pages and is omitted for sake of space. However, a Boolean equivalent of the entire fault tree is shown in Fig. 4. In Fig. 4, the numbers that are listed as gate inputs represent basic events that are listed alphabetically in Table I. The basic events in the LPIS fault tree are coded according to a seven-digit alphanumeric designator following the practice adopted for the Reactor Safety Study.[7] The first digit indicates the event type, X represents a circle, and Z represents a diamond. The second and third digits indicate the component type, e.g., PM stands for pump, MV for motor-operated valve. The fifth and sixth digits identify the specific events or components listed in the event description of Table I. The seventh digit represents the failure mode of the component; e.g., Q stands for short-circuit, A stands for "does not start," etc. Note

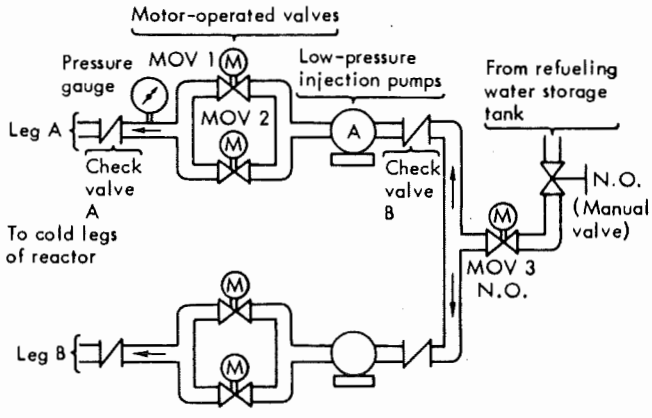


Fig. 1. Low-pressure injection system.

TABLE I

Basic Event Data for LPIS Leg-A Fault Tree

Event	Number	Event Description	Unavailability[a]
XCB01K[b]	1	Circuit breaker contacts fail to close	$10^{-3}/d$
XCV01C[b]	2	Check valve A jammed closed	$10^{-4}/d$
XCV02C[b]	3	Check valve B jammed closed	$10^{-4}/d$
XMV01D	4	MOV 1 fails to open	Hardware $1 \times 10^{-3}/d$ Maintenance $3.0 \times 10^{-3}\ \Delta t/T_M$ $\Sigma = 4.0 \times 10^{-3}$
XMV02D	5	MOV 2 fails to open	Hardware $1 \times 10^{-3}/d$ Maintenance $3.0 \times 10^{-3}\ \Delta t/T_M$ $\Sigma = 4.0 \times 10^{-3}$
XPD01K	6	Pressure transducer contacts P1 fail to close	$3 \times 10^{-3}/d$
XPD02K	7	Pressure transducer contacts P2 fail to close	$3 \times 10^{-3}/d$
XPD03K	8	Pressure transducer contacts P3 fail to close	$3 \times 10^{-3}/d$
XPM01A[b]	9	Pump motor fails to start	Hardware $1 \times 10^{-3}/d$ Maintenance $2.5 \times 10^{-3}\ \Delta t/T_M$ $\Sigma = 3.5 \times 10^{-3}$
XRE01K[b]	10	#1 contacts fail to close	$10^{-4}/d$
XRE02K[b]	11	#4 contacts fail to close	$10^{-4}/d$
XRE03K	12	#2 contacts fail to close	$10^{-4}/d$
XRE04K	13	#5 contacts fail to close	$10^{-4}/d$
XRE05K[c]	14	#7 contacts fail to close	$10^{-4}/d$
XRE06K	15	#3 contacts fail to close	$10^{-4}/d$
XRE07K	16	#6 contacts fail to close	$10^{-4}/d$

Event	Number	Event Description	Fault Duration Time (h), τ	Failure Rate λ	Unavailability[d]
XXV01D[c]	17	Manual valve fails to open		$10^{-4}/d$	10^{-4}
ZBS01N[b]	18	No power on bus 480 1H			5×10^{-4} $(\overline{A})$
ZBS02N[b]	19	No power on bus DC1A			5×10^{-6} $(\overline{A})$
ZBS03N[b]	20	No power on bus MCC1H1-1			5×10^{-4} $(\overline{A})$
ZCB02O	21	Circuit breaker #1 open	720	10^{-6}/h	7.2×10^{-4}
ZCB03O	22	Circuit breaker #2 open	720	10^{-6}/h	7.2×10^{-4}
ZMV03C	23	N.O. MOV 3 inadvertantly closes	720	10^{-6}/h	7.2×10^{-4}
ZPP01P[b]	24	Piping in leg A plugged	8760/2	10^{-8}/h	4.4×10^{-5}
ZPP02P[c]	25	Piping from RWST plugged	8760/2	10^{-8}/h	4.4×10^{-5}
ZPP01R[b]	26	Rupture In leg A of LPIS	720	10^{-7}/h	7.2×10^{-5}
ZPP02R[c]	27	Rupture in pipe from RWST	720	10^{-7}/h	7.2×10^{-5}
ZTR01O	28	Open circuit or short circuit transfer #1	720	10^{-6}/h	7.2×10^{-4}
ZTR02O	29	Open circuit or short circuit transfer #2	720	10^{-6}/h	7.2×10^{-4}
ZWR01O[b]	30	O.C. or S.C. in cable from LPI PP to bus 4801H	720	10^{-6}/h	7.2×10^{-4}
ZWR02O	31	O.C. or S.C. in wiring of close coil circuit	720	10^{-8}/h	7.2×10^{-6}
ZWR03O[b]	32	O.C. or S.C. in wiring of K1 coil circuit	720	10^{-8}/h	7.2×10^{-6}
ZWR04O[b]	33	O.C. or S.C. in wiring of K4 coil circuit	720	10^{-6}/h	7.2×10^{-6}
ZWR05O	34	O.C. or S.C. in cable from MOV-1 to bus MCC1H1-1	720	10^{-6}/h	7.2×10^{-4}
ZWR06O	35	O.C. or S.C. in wiring of K2 coil circuit	720	10^{-8}/h	7.2×10^{-6}
ZWR07O	36	O.C. or S.C. in wiring of K5 coil circuit	720	10^{-6}/h	7.2×10^{-6}
ZWR08O[c]	37	O.C. or S.C. in wiring of K7 coil circuit	720	10^{-8}/h	7.2×10^{-6}
ZWR09O	38	O.C. or S.C. in cable from MOV-2 to bus MCC1H1-1	720	10^{-6}/h	7.2×10^{-4}
ZWR10O	39	O.C. or S.C. in wiring of K2 coil circuit	720	10^{-8}/h	7.2×10^{-6}
ZWR11O	40	O.C. or S.C. in wiring of K6 coil circuit	720	10^{-8}/h	7.2×10^{-6}
ZXV01Y[c]	41	Maintenance crew inadvertently closes manual valve		$10^{-4}/d$	10^{-4}

[a] d = demand; $\Delta t/T_M$ = the fractional downtime due to maintenance.
[b] A basic event whose occurrence can cause leg A of the LPIS to fail on demand.
[c] A basic event whose occurrence can cause the LPIS to fail on demand.
[d] $\overline{A}$ = limiting unavailability.

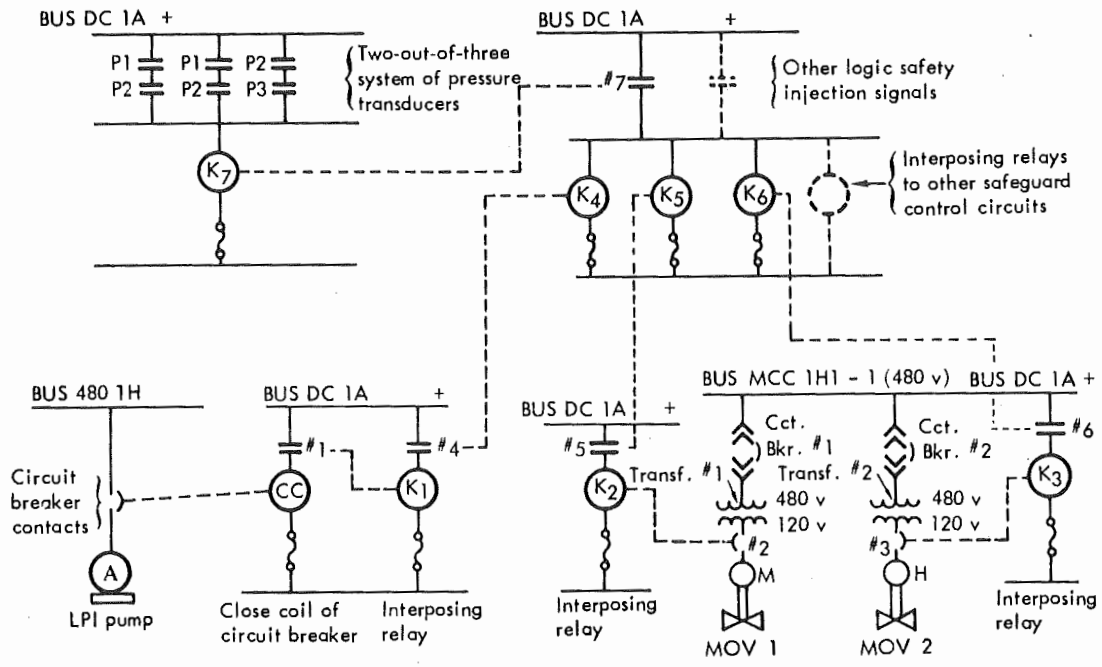


Fig. 2. The LPIS control circuit: The ECCS, including the LPIS, is actuated by a safety injection signal (SIS). The LOCA creates conditions such as "low-pressurizer water level" and "low-pressurizer pressure" that are detectable by transducers. For simplicity, the actuation of the LPIS is described for the case when the SIS is generated from the two-out-of-three circuit for high containment pressure.

In the event of high containment pressure, pressure transducers 1, 2, and 3 (not shown) close contacts P1, P2, and P3. Then, dc current energizes relay coil K7 and the #7 contacts close. In turn, the interposing relays, K4, K5, and K6, are energized. Then, the #4, #5, and #6 contacts close and energize, respectively, relay coils K1, K2, and K3, which in turn close the #1, #2, and #3 contacts. The "close" coil to the circuit breaker of LPI pump A closes its contacts, which in turn provide 480-V three-phase power to pump A. Similarly, the #2 and #3 contacts close and provide 120-V power to the motors that open valves MOV 1 and MOV 2, respectively.

that human error is also included in the fault tree as a cause of LPIS failure. For example, the basic event ZXV01Y represents the event "operator (or maintenance crew) inadvertently closes the manual valve."

The unavailabilities[13] of all the basic events in the fault tree of Fig. 3 are listed in Table I. The unavailability of all active components required to change state is given by their cyclic failure rate, i.e., the probability of failing to change state on demand. The emergency power buses are continuously operating systems; their unavailabilities are given by their limiting asymptotic values, $\overline{A}$. The unavailability of all other components is given by the product $\lambda\tau$, where λ is an hourly failure rate and τ is the effective exposure time or fault duration time.[23] The possibility of maintenance of these components is allowed since the entire LPIS is periodically tested.

The events are listed by decreasing values if the Fussell-Vesely measure of importance in Table II. Inspection of this table shows that pump A failing to start has the greatest probability of causing failure of the LPIS to start. If pump A is working satisfactorily, we should check the circuit breaker for pump A. We see that events 23 and 30 are of equal importance and should be checked next. At this point in the checklist, we check for failure of a quasi-static component, i.e., a cable failure. At this point it is decided to check for a false alarm, since failure of an active component—in this case a pressure gauge—is more likely to occur than failure of a passive component. The components listed eighth in order in Table II are components contained in second-order cut sets. (Components in Table II with no asterisks are contained in second-order cut sets.) A sublist for motor-operated valve #1 is given in Table III. It is simply a listing of basic events contained in the same cut sets as MOV 1, listed in order of their probability of occurrence.

For this particular example, the iteration process described previously was used to generate a checklist based on conditional probabilities.[13] This checklist ranked components according to the same checking order as the initial listing of probabilistic importances in Table II. However,

[23]Similar types of calculations involving component unavailabilities are given in Ref. 7.

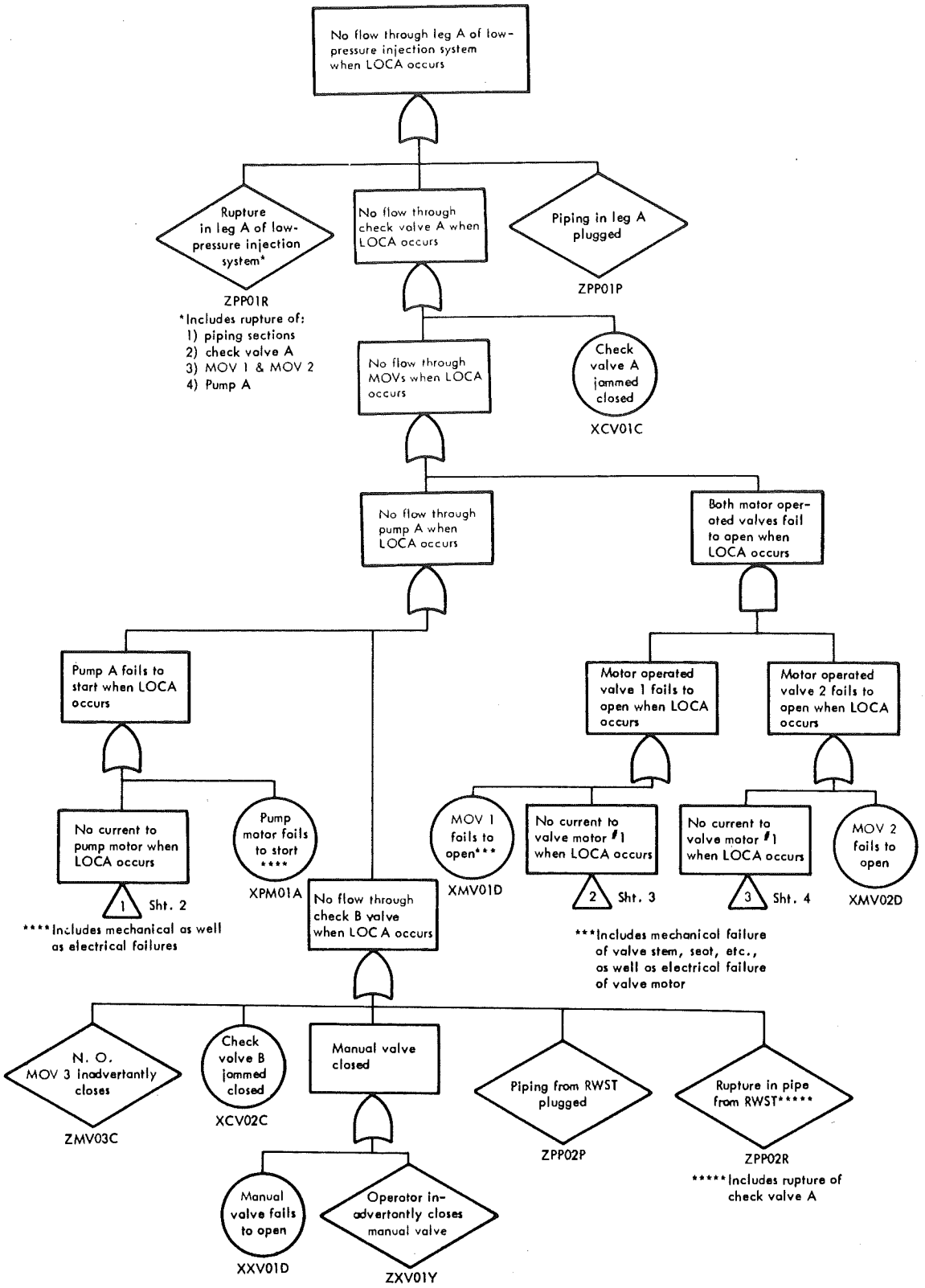


Fig. 3. Fault tree for the LPIS.

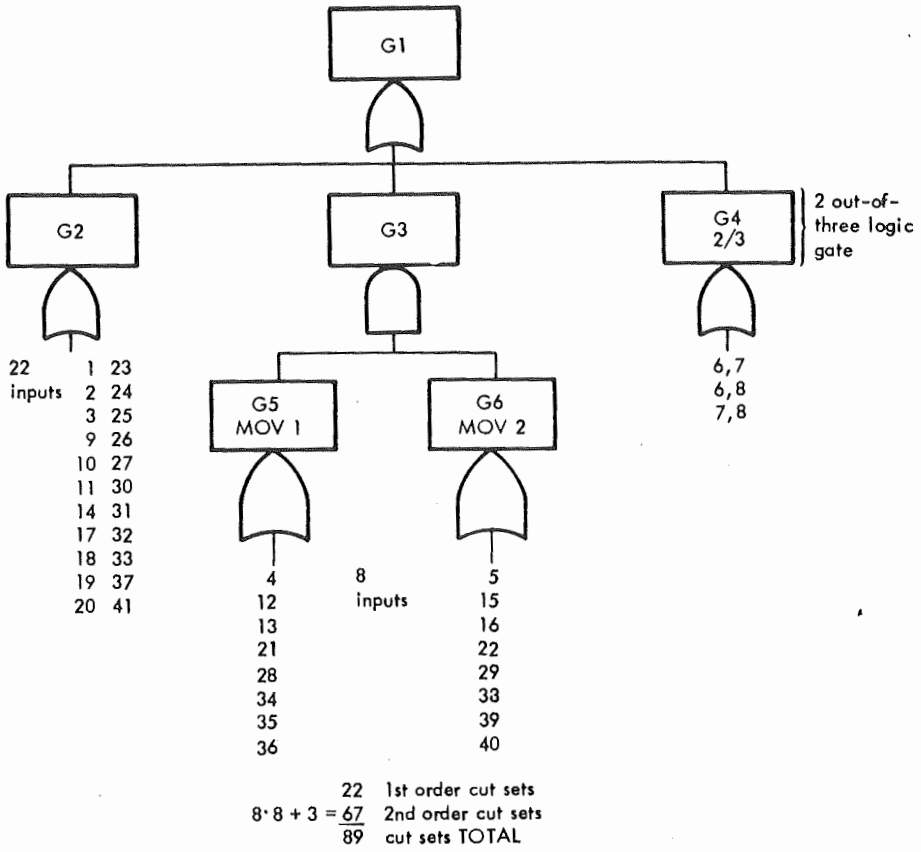


Fig. 4. Boolean equivalent of the LPIS fault tree.

by varying the values of the unavailabilities of components in Table I, for this example it was shown that the ranking done on a conditional basis differed from the ranking done on the initial listing.[13] In general, the iteration process is necessary for ordering events on the checklist.

A useful feature of the checklist generation scheme is that a library of checklists can be prepared ahead of time so that a computer is not needed at the time the diagnosis is made. As time progresses, the checklists may have to be revised periodically to reflect increased knowledge concerning the system.

IV. SYSTEM DIAGNOSIS UNDER A TIME CONSTRAINT

In Sec. III, we generated repair checklists solely on the basis of probabilistic importance. We did not consider the time required to check components. In some cases, there may be a considerable risk or system degradation while a system or subsystem is down. In this section, we propose a checking scheme based on the concept of component criticality that minimizes the expected time required to diagnose system failure. The scheme makes use of an expression that is a function of the component checking times as well as their probabilistic importance. Under the proposed scheme, if all components in the system had equal checking times, then the component that has the highest probability of being critical to system failure would be checked first. However, later in this section we show that the order in which the components are checked may change if component checking times are unequal.

It is assumed that the system is failed and that all causes of failure, i.e., basic events, in the fault tree are statistically independent. Under the proposed scheme, we check components one by one until failure of all the elements of at least one min cut set is confirmed. If after the cut set(s) is (are) repaired, system failure persists, we continue to check until another failure of a min cut set is observed. We continue in this manner until no more failed cut sets are found.

Each time we check a component in the system, there are three possible outcomes:

1. The component has not failed.
2. The component has failed but is not critical to system failure.

TABLE II

Importance Listing and Checklist for LPIS

(Probability that the LPIS fails on demand = 5.0×10^{-4}; probability that the LPIS fails on demand when pump A has failed = 8.0×10^{-3}.)

Order	Event Number	Event	Importance	Order	Event Number	Event	Importance
1	9	XPM01A[a]	4.380E-01[b]	9	6	XPD01K	2.238E-03
2	1	XCB01K[a]	1.248E-01		7	XPD02K	2.238E-03
3	23	ZMV03C	8.984E-02		8	XPD03K	2.238E-03
Check for false alarm				10	31	ZWR02O[a]	8.978E-04
					32	ZWR03O[a]	8.978E-04
3	30	ZWR01O[a]	8.984E-02		33	ZWR04O[a]	8.978E-04
4	18	ZBS01N[a]	6.238E-02		37	ZWR08O[c]	8.978E-04
	20	ZBS03N[a]	6.238E-02	11	19	ZBS02N[a]	6.235E-04
5	2	XCV01C[a]	1.247E-02	12	21	ZCB02O	5.680E-04
	3	XCV02C[a]	1.247E-02		22	ZCB03O	5.680E-04
	10	XRE01K[a]	1.247E-02		28	ZTR01O	5.608E-04
	11	XRE02K[a]	1.247E-02		29	ZTR02O	5.680E-04
	14	XRE05K[c]	1.247E-02		34	ZWR05O	5.680E-04
	17	XXV01D[c]	1.247E-02		38	ZWR09O	5.680E-04
	41	ZXV01Y[c]	1.247E-02	13	12	XRE03K	7.885E-05
6	26	ZPP01R[a]	8.978E-03		13	XRE04K	7.885E-05
	27	ZPP02R[c]	8.978E-03		15	XRE06K	7.885E-05
7	24	ZPP01P[a]	5.487E-03		16	XRE07K	7.885E-05
	25	ZPP02R[c]	5.487E-03	14	35	ZWR06O	5.676E-06
8	4	XMV01D	3.166E-03		36	ZWR07O	5.676E-06
	5	XMV02D	3.166E-03		39	ZWR10O	5.676E-06
					40	ZWR11O[a]	5.676E-06

[a]A basic event whose occurrence can cause leg A of the LPIS to fail on demand.
[b]Read as 4.380×10^{-1}.
[c]A basic event whose occurrence can cause the LPIS to fail on demand.

TABLE III

Sublist for Motor Operated Valve #1

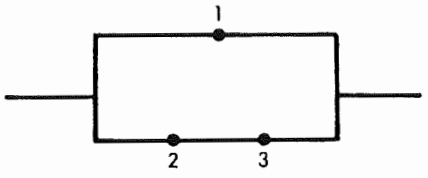
Order	Event Number	Event
1	5	XMV02D
2	22	ZCB03O
	29	ZTR02O
	38	ZWR09O
3	15	XRE06K
	16	XRE07K
4	39	ZWR10O
	40	ZWR11O

3. The component has failed and is critical to system failure.[24]

If failure of a min cut is confirmed while checking the n'th component, then outcome 3 must be true for that component.

[24]Recall from Sec. II that a component is critical to system failure if $\psi[1_i, \boldsymbol{Y}(t)] - \psi[0_i, \boldsymbol{Y}(t)] = 1$.

When the n'th component is found to be failed, it is possible that more than one min cut sets containing this component are failed. At this point, we introduce the concept of a critical cut set that enables us to handle this situation. First, as an example consider the reliability network diagram given below,



where nodes represent the components of some system. If the system fails in time according to the sequence of component failures 2, 3, 1, then component 1 is critical at the time of system failure and two min cut sets (1, 2) and (1, 3) are failed. The set of components (1, 2, 3) is called a *critical cut set* for component 1, since each cut set in the set (1, 2, 3) contains a min cut set that contains component 1. In general, for a set of

events to be a critical cut set for event i, each min cut set in this set must contain event i.

We now set up an expression for the expected time required for system diagnosis to confirm that a critical cut set has occurred. First, we consider notation.

IV.A. Notation

We adopt the notation of Sec. III. In addition, let T_i denote the time required to check component i; let $q_i(t) \equiv q_i$; $p_i = 1 - q_i$; let T_s = time to diagnose system failure; let $(1^k, 0^{n-k}, \boldsymbol{Y}^{N-n})$ be the state vector of a system of N components from which n components have been checked $(n \leq N)$, k components have been found to be failed, and $n - k$ components are not failed. Let $C'(\boldsymbol{Y})$ denote the set of components that have been checked and $C^\circ(\boldsymbol{Y})$ the set of components that have not been checked yet.

IV.B. Expression to Minimize Checking Time

An expression for the expected time to diagnose system failure, $E(T_s)$, involves $\sum_{i=1}^{N} 2^{i-1}$ terms, where i is the checking order. The first seven terms of $E(T_s)$ according to checking order or stage are given by

$$E(T_s) = \underbrace{T_1}_{\substack{\text{First-Order}\\ \text{Term}}} + \underbrace{\begin{cases} T_2 p_1 \Delta g_2(0_1, \boldsymbol{q}) \\ T_2 q_1 \Delta g_2(1_1, \boldsymbol{q}) \end{cases}}_{\substack{\text{Second-Order}\\ \text{Terms}}} + \underbrace{\begin{cases} T_3 p_1 p_2 \Delta g_3(0_1, 0_2, \boldsymbol{q}) \\ T_3 p_1 q_2 \Delta g_3(0_1, 1_2, \boldsymbol{q}) \\ T_3 q_1 p_2 \Delta g_3(1_1, 0_2, \boldsymbol{q}) \\ T_3 q_1 q_2 \Delta g_3(1_1, 1_2, \boldsymbol{q}) \end{cases}}_{\substack{\text{Third-Order}\\ \text{Terms}}} , \tag{1}$$

where the terms following the vertical braces are summed. Recall that

$$\Delta g_i(\boldsymbol{q}) \stackrel{\text{def}}{=} g(1_i, \boldsymbol{q}) - g(0_i, \boldsymbol{q}) \quad .$$

Order refers to the number of components that have been checked.

The terms listed above have the following meaning: The first-order term reflects the fact that at least one component in the system must be checked to confirm that a critical cut set has occurred. Second-order terms appear when the occurrence of a critical cut set on the first step has not been observed. The product, $p_1 \Delta g_2(0_1, \boldsymbol{q})$, in the second-order term represents the probability that the first component to be checked was not failed *and* the second component to be checked is critical to system failure when the first component has not failed. The corresponding product in the other second-order term has a similar probabilistic meaning with regards to the criticality of the second component except that now the first component was observed to be failed. Third-order terms appear when occurrence of a critical cut set on the second step has not been observed. Once we observe the occurrence of a critical cut set, say on the n'th step, higher-order terms drop out since the criticality expression, Δg_i, in the $(n + 1)$'th and higher terms is zero.

There are $N!$ possible expressions for and values of $E(T_s)$ according to the checking order of the various components. Note, however, that in the ordering given above, if we check component 2 first and component 1 second, the terms involving $T_3, \ldots, T_n$ do not change. To determine which component to check first, we propose to minimize $E(T_s)$ with respect to the first two terms and neglect the third- and higher order terms.

$$T_j + \begin{cases} T_i p_j \Delta g_i(0_j, \boldsymbol{q}) \\ T_i q_j \Delta g_i(1_j, \boldsymbol{q}) \end{cases} > T_i + \begin{cases} T_j p_i \Delta g_j(0_i, \boldsymbol{q}) \\ T_j q_i \Delta g_j(1_i, \boldsymbol{q}) \end{cases} , \tag{2}$$

for all $j(\neq i)$, then component i should be checked first. This reduces the number of expressions for $E(T_s)$ from $N!$ to $N(N - 1)/2$.

The argument can be extended each time we check a component in the system. In general, if we have checked n components in the system, the next component we should check again is determined by an expression similar to Eq. (2),

$$T_j + \begin{cases} T_i p_j \Delta g_i(0_j, 1^k, 0^{n-k}, \boldsymbol{Y}^{N-n}) \\ T_i q_j \Delta g_i(1_j, 1^k, 0^{n-k}, \boldsymbol{Y}^{N-n}) \end{cases} > T_i + \begin{cases} T_j p_i \Delta g_j(0_i, 1^k, 0^{n-k}, \boldsymbol{Y}^{N-n}) \\ T_j q_i \Delta g_j(1_i, 1^k, 0^{n-k}, \boldsymbol{Y}^{N-n}) \end{cases} \quad \ldots , \tag{3}$$

where i and $j \epsilon C^\circ(\boldsymbol{Y})$. The optimization procedure implied by the expression, Eq. (3), is referred to in decision theory as a one-step-ahead optimization policy.[25]

If, on the n'th step, we observe that a critical cut set, say K_j, has failed, we still must somehow determine if K_j is the only critical cut set failed. If it is not, then in the expression, Eq. (3), we set $Y_l = 0$ for all $l \epsilon K_j$ and continue to check for another failed critical cut set.

IV.C. Series System

We use the expression, Eq. (2), to determine which component should be checked first for a series system with N components. Such a system will fail if any component fails. In this case,

$$g(\boldsymbol{q}) = 1 - \prod_{k=1}^{N} (1 - q_k) = 1 - \prod_{k=1}^{N} p_k \quad ,$$

$$\Delta g_i(\boldsymbol{q}) = \prod_{\substack{k=1 \\ k \neq i}}^{N} p_k \quad ,$$

and Eq. (2) becomes

[25] S. ROSS, *Applied Probability Models with Optimization Applications*, pp. 31-84, Holden-Day, San Francisco (1970).

$$T_j + \begin{cases} T_i p_j \prod_{\substack{k \\ k\neq i \\ k\neq j}} p_k \\ T_i q_j \cdot 0 \end{cases} > T_i + \begin{cases} T_j p_i \prod_{\substack{k \\ k\neq i \\ k\neq j}} p_k \\ T_j q_i \cdot 0 \end{cases} .$$

This implies that

$$T_j + T_i p_j \prod_{\substack{k \\ k\neq i \\ k\neq j}} p_k > T_i + T_j p_i \prod_{\substack{k \\ k\neq i \\ k\neq j}} p_k .$$

Since for reliable system $\prod_{\substack{k \\ k\neq i \\ k\neq j}} p_k \approx 1$. We obtain

$$T_j + T_i p_j > T_i + T_j p_i$$

or

$$\frac{T_j}{q_j} > \frac{T_i}{q_i} \text{ for all } j \neq i .$$

The above inequality states that the component with the minimum value of T_i/q_i should be checked first, an intuitive result for a series system. Note that in the series case, the above result is globally optimal since third-order terms and higher are zero.

IV.D. Parallel System

For a parallel system of N components that will fail if all components fail,

$$g(\mathbf{q}) = \prod_{l=1}^{N} q_l ,$$

$$\Delta g_i(\mathbf{q}) = \prod_{\substack{l=1 \\ l\neq i}}^{N} q_l ,$$

and Eq. (2) becomes

$$T_j + T_i q_j \prod_{\substack{l\neq i \\ l\neq j}} q_l > T_i + T_j q_i \prod_{\substack{l\neq i \\ l\neq j}} q_l$$

or

$$T_j \left(1 - \prod_{l\neq j} q_l\right) > T_i \left(1 - \prod_{l\neq i} q_l\right) .$$

Again, for reliable system

$$\prod_{l\neq i} q_l \approx 0, \quad \prod_{l\neq j} q_l \approx 0 ,$$

which implies

$$T_j > T_i \text{ for all } j \neq i .$$

Thus, according to this inequality for a parallel system, the component with the minimum checking time should be checked first, again an intuitive result.

The obvious disadvantage to the above scheme is that it minimizes $E(T_s)$ with respect to the first two terms only. In a rigorous analysis, third- and higher order terms should also be considered in finding the true optimal checking order. However, it is conjectured that it is extremely difficult and time consuming to set up a generalized expression that minimizes $E(T_s)$. On the contrary, the expression, Eq. (2), is easy to compute and gives intuitively verifiable results for the series and parallel cases.

If the fault tree on which the checking scheme is based includes all system failure modes, then all the failed min cuts will be found using the above scheme. However, some components may still be failed after finding all the failed min cut sets. Hence, the above scheme is suited for diagnosis under emergency conditions, where the immediate goal is to return the system to the unfailed state in the shortest time possible.

V. DECISIONS REGARDING SYSTEM OPERATION WHEN SYSTEM FAULT CONDITIONS OCCUR

Following identification by the operator of the basic events such as hardware failures and maintenance faults that have occurred, the increased risk of operating the system can be determined by quantitatively reevaluating the fault tree for the entire system. On the basis of such factors as the length of time it may take to repair components or to rectify human errors, or the hazard associated with loss of subsystems or components, decisions may be made regarding the continuing operation of the system. Basically, four choices are available to an operator when system fault conditions occur:

1. shut the system down and repair failed components
2. change the mode of system operation while repairing the components
3. operate the system and simultaneously repair it
4. operate the system without immediate repair.

For example, all four choices are, in principle, available to the operator of a nuclear power plant if an engineered safeguard system is found inoperable. Choices 1 and 4 are available to a pilot who finds a hydraulic system inoperable in flight; i.e., he may land his aircraft at the nearest airport or continue his flight to his final destination.

The choice the operator makes is influenced basically by the costs and hazards associated with system shutdown and restart versus the costs and hazards of continuing to operate at a higher risk level. For example, hazards and economic penalties associated with shutdown in the chemical industry are numerous: When hydrocarbon plants are shut down, the equipment must be purged to remove all oxygen before restart to avoid the

potential for fire. When shut down, stirred chemical reactors may develop hot spots if not thoroughly stirred, and explosions may result.

When nuclear power plants are shut down, thermal transients are induced, causing increased stresses on piping and equipment. Shutdown and restart also involve system transients that might increase the potential for accidents. Shutdown of these complex system also results in lost production time and lost revenue. From this brief discussion, it is obvious that a trade-off analysis should be conducted when considering shutdown of highly complex and potentially hazardous systems.

V.A. Shutdown Decision at a Nuclear Power Plant

As an example of a shutdown decision made on a risk-assessment basis, consider a failure of low-pressure injection pump A in the example from Sec. III. Assume that this failure was revealed during a routine monthly test. The operator would like to know if this failure warrants plant shutdown. Technical specifications by the U.S. Nuclear Regulatory Commission (NRC) require the plant to be shut down to a hot standby condition if repair time, Υ, is longer than 24 h, and to a cold standby condition if $\tau > 48$ h. The effect of the failure of pump A is that leg A is incapacitated until pump A can be repaired, and results in loss of LPIS redundancy. If a primary coolant system pipe rupture were to occur and if the leg-B pump failed to start, the potential for a large radiological release is increased. However, there is also a finite risk associated with plant shutdown.[26] In Sec. V.A.1, we use the quantitative information presented in the Reactor Safety Study and in Table II of this paper to compute the risk of shutting down the plant versus the risk of plant operation with one LPIS pump out of service. The effect of thermal transients induced by shutdown and startup is included in this analysis. We then determine the repair time interval, τ, for which the risk associated with continuing plant operation becomes comparable to the risk of shutting down the plant. This analysis is necessarily of a simplified nature and is included here for illustration purposes only.

V.A.1. Establishing Maximum Allowable Repair Time, Υ

From Table II we see that with one LPIS pump out of service, the probability that the entire LPIS fails on demand is 7.9×10^{-3}, while the probability of both LPIS legs failing is 5.0×10^{-4} per demand. In case of a large pipe break, failure of the LPIS leads to core meltdown. For small pipe breaks, the high-pressure injection system can provide sufficient emergency cooling. The probability of a large pipe break is obtained from the Reactor Safety Study[7] as 10^{-4}/yr. Thus, the incremental hourly risk associated with plant operation with one LPIS pump out of service is

$$\begin{aligned}
&\text{Prob (core meltdown/h}\,|\,\text{one LPIS pump failure)} \\
&\quad = \text{Prob (large pipe break/h) Prob (LPIS failure}\,|\,\text{one LPIS pump failure)} \\
&\quad = 10^{-4}/\text{yr} \times (1\ \text{yr}/8760\ \text{h}) \\
&\qquad \times (7.9 \times 10^{-3} - 5.0 \times 10^{-4}) \\
&\quad = 8.4 \times 10^{-11}/\text{h} \quad . \qquad (4)
\end{aligned}$$

The Reactor Safety Study considered PWR accident chains with loss of off-site power as the initiating event and concluded that these accident sequences contributed significantly to the overall risk of plant operation. If both the main feedwater and auxiliary feedwater systems fail to operate following this transient, the heat sink for decay heat removal is lost. The steam generators would be emptied in $\sim\frac{1}{2}$ h, causing the reactor coolant in the primary loop to heat up. The reactor coolant would be discharged through the pressurizer relief valves, causing the reactor core to be uncovered. Within $\sim 1\frac{1}{2}$ h after the transient, core melting would start. Various accident sequences were hypothesized that would result in loss of the main feedwater and auxiliary feedwater and auxiliary feedwater systems with loss of off-site power as the initiating event. As shown in Table IV, these sequences make a significant contribution to the probabilities of release across the entire release spectrum. For our example, we consider an orderly shutdown of the plant during which an operator error is committed that causes a turbine trip, which in turn imposes a transient instability in the electrical grid resulting in loss of off-site power. We estimate that the probability of operator error during shutdown causing a turbine trip is 10^{-2}. Based on Federal Power Commission data, the probability of an off-site power loss during a turbine trip is 10^{-3} (Ref. 7). Thus, the probability of a core meltdown caused by loss of off-site power due to an operator error during shutdown is obtained by multiplying $P_{TE,R}$ in Table IV by the ratio

$$\frac{10^{-2} \times 10^{-3}}{0.2} = 5 \times 10^{-5} \quad .$$

This probability per shutdown is

$$5 \times 10^{-5} \sum_{R=1}^{7} P_{TE,R} = 8.0 \times 10^{-10} \quad . \qquad (5)$$

[26]Here, risk is defined for simplicity only in terms of a core meltdown.

TABLE IV

Transient-Event Probability Contributions*

Release Category R	$P_{TE,R}(\text{yr}^{-1})$	$P_{TE,R}/R_{\text{total},R} \times 100\%$ (%)
1	3×10^{-7}	38
2	3×10^{-6}	41
3	4×10^{-7}	10
4	7×10^{-8}	15
5	2×10^{-7}	32
6	2×10^{-6}	41
7	1×10^{-5}	26

*From Ref. 7:

$P_{\text{total},R}$ = probability of release of a category R per year from all causes

$P_{TE,R}$ = probability of release of category R due to loss of off-site power as an initiating event.

The probability of the transient-event accident sequence, P_{TE}, took the general form

$$P_{TE} = P_1 \prod_{i=2}^{n} P_i \quad ,$$

where

P_1 = probability of loss off-site power during normal operation

= 0.2 occurrence/yr

P_i = probability of occurrence of the i'th event in the accident sequence.

During shutdown and startup, thermal transients may also increase the hourly probability of a LOCA. We assume that the probability of a LOCA is the same during shutdown and startup, but different from the value during steady-state generation. We define the probability ratio, α, as

$$\alpha = \frac{\text{Prob (LOCA during shutdown or startup/h)}}{\text{Prob (LOCA at steady state/h)}} \quad .$$

After repair or replacement of the LPIS pump, plant startup begins. The LPIS unavailability is given in Table II as 5.0×10^{-4}. We estimate that the time required for plant shutdown and startup is 12 h for each. Then, the increased risk due to shutdown and startup includes the contributions from operation with a partly failed LPIS and an unimpaired LPIS:

$$\alpha(10^{-4}/\text{yr})(1\ \text{yr}/8760\ \text{h})(7.9 \times 10^{-3} + 5.0 \times 10^{-4}) \times 12\ \text{h} - (10^{-4}/\text{yr})(1\ \text{yr}/8760\ \text{h})(5.0 \times 10^{-4})\ 24\ \text{h} = 1.2 \times 10^{-9}\ \alpha - 1.4 \times 10^{-10} \quad . \qquad (6)$$

We have not considered possible failure of other ECCSs and small pipe breaks to simplify the analysis.[27] We obtain the allowed repair time, Υ, as a function of α by equating the incremental risks associated with the two options from Eqs. (4), (5), and (6).

$$8.4 \times 10^{-11}\ \Upsilon = 8.0 \times 10^{-10} + 1.2 \times 10^{-9}\ \alpha - 1.4 \times 10^{-10}$$

or

$$\alpha = 0.07\ \Upsilon - 0.55 \quad . \qquad (7)$$

Some values of the maximum permissible repair time versus α from Eq. (7) are given in Table V.

We see that if $\alpha = 1$, Υ is given as 22 h, a lower bound in this analysis. The actual value of α dictates the value for Υ. The above analysis is not intended to be rigorous. However, it does show how decisions regarding system operation based on a risk assessment can be made when system fault conditions occur.

Polk[28] performed a similar analysis based on economic penalty. He considered the NRC regulation requiring PWR plant shutdown 2 h after the loss of one of the two redundant emergency dc-power buses. He computed the cost of lost revenue while the plant is shut down and compared it to the increased expected cost of an accident involving radiological releases that might occur during continuing plant operation while repair or replacement is taking place. Thus, he has determined the optimal allowable repair time based on cost.

Expected cost or increased risk may not be the only consequences considered in a trade-off analysis. A multiplicity of values involving safety, ecology, cost, availability of electrical power, etc. is involved in the process of imposing regulations on nuclear power plants. This suggests the use of *multi-attribute utility theory* in the decision process.[29] Such an attempt is, however, clearly beyond the scope of this paper.

TABLE V

Values of Maximum Permissible Repair Times Versus Alpha

α	1.0	1.1	11	50
Υ	22 h	1 day	1 week	1 month

[27]The unavailability of the LPIS with one pump out of service should dominate all other engineered safeguard system unavailabilities, making the expression, Eq. (6), an accurate approximation.

[28]R. E. POLK, "A Risk/Cost Assessment of Administrative Time Restrictions on Nuclear Power Plant Operation," MS Thesis, University of Houston, Department of Electrical Engineering (1976).

[29]R. L. KEENEY and K. NAIR, "Decision Analysis for Siting of Nuclear Power Plants—The Relevance of Multiattribute Utility Theory," *Proc. IEEE*, **63**, 3 (1975).

VI. CONCLUSION

The checklist generation scheme presented here provides an efficient way of diagnosing system malfunctions for complex systems. If the times required to check components vary widely, we may consider implementing the one-step-ahead optimization procedure on a computer. This is particularly desirable for potentially complex and hazardous systems where time available for diagnostic checking might be limited. The advantage to checklists is that an on-line computer is not needed since those can be prepared in advance for possible system malfunctions. In either method, we use the information gained as the system is examined to determine what component should be checked next.

When shutdown of a complex and hazardous system is considered following occurrence of system fault conditions, we should perform a trade-off analysis based on cost, safety, and other factors to actually determine if shutdown is the optimal course of system operation.

ACKNOWLEDGMENTS

The material for this article was extracted from Ref. 13, the PhD thesis of the first author. The authors wish to thank Richard Barlow of the University of California, Berkeley, for his valuable guidance of the research.

This work was performed under the auspices of the U.S. Energy Research and Development Administration.