4

Fault Trees and Common Cause Failures

4.1 INTRODUCTION

This chapter discusses fault trees, which are to analyze complex systems. This technique has rapidly gained favor because of its versatility in degree of detail of complex systems. The fault tree technique was originated by H. A. Watson of Bell Telephone Laboratories to analyze the Minuteman Launch Control System. It was further refined by a study team at the Bell Telephone Laboratories.

Further work on fault tree techniques was carried out at the Boeing company in which Haasl [37] played an instrumental role. A turning point took place in 1965 when several papers on the technique were presented at the 1965 Safety Symposium held at the University of Washington, Seattle, [37]. Ever since several experts have made further advances in this technique.

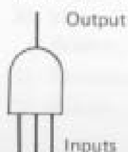
Again another symposium on the technique was organized at the University of California at Berkeley [2]. A comprehensive bibliography on the technique is presented in reference 21.

Most of the material presented in this chapter is taken from the listed fault tree bibliography at the end of this chapter. The second part of this chapter deals with the subject of common-cause failures.

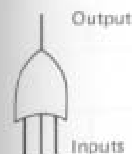
4.2 FAULT TREE SYMBOLS AND DEFINITIONS

This section presents most of commonly used fault tree symbols and definitions. For more comprehensive symbols and definitions one should consult references 65 and 124.

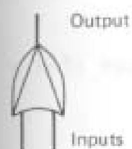
AND Gate. The AND gate denotes that an output event occurs if and only if all the input events occur.



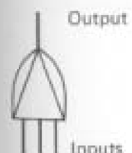
OR Gate. The OR gate denotes that an output event occurs if any one or more of the input events occur.



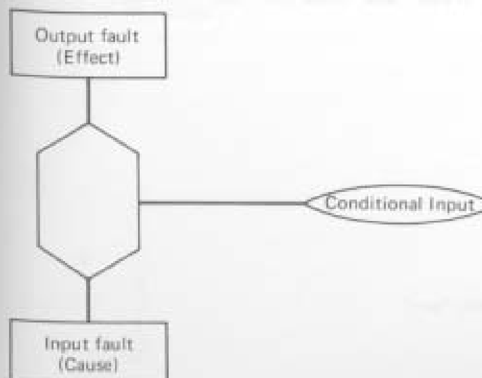
Exclusive OR Gate. The output of this gate is an intermediate event. This gate denotes that there is no output unless one and only one of the input events occurs.



Priority AND Gate. It is logically equivalent to an AND gate with the exception that the input events must occur in a specific order. It is represented by the following symbol:

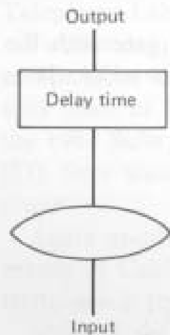


Inhibit Gate. This gate produces output only when the conditional input is satisfied. The inhibit gate is logically equivalent to an "AND" gate with two input events.

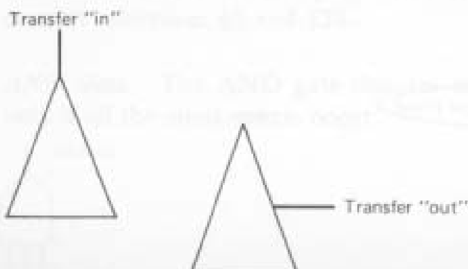


Special Gate. This gate represents any other legitimate combination of the input events.

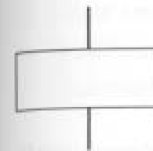
Delay Gate. This represents a gate whose output only occurs after a specified delay time has elapsed.



The Triangle. A triangle denotes a transfer IN or OUT. It is used to avoid repeating sections of the fault tree. A line from the top of the triangle indicates "transfer in." A line from the side of the triangle denotes "transfer out."



Resultant Event. A rectangle denotes an event which results from the combination of fault events through the input of a logic gate.

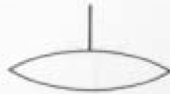


Basic Fault Event. A circle represents a basic fault event or the failure of an elementary component. The failure parameters such as unavailability, probability, failure, and repair rates of a fault event are obtained from the empirical date or other sources.

Incomplete Event. A diamond represents a fault event whose causes have not been fully developed. This event could be further developed to show basic contributary failures; however, it is not developed either due to lack of information or due to lack of interest.

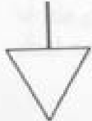
Trigger Event. The house shape symbol denotes a fault event which is expected to occur.

The Conditional Event. This is denoted by an ellipse. This symbol indicates any condition or restriction that applies to a logic gate.



Double Diamond Event. This symbol represents an undeveloped fault event that requires further development to accomplish the fault tree.

The Upside Down Triangle. This symbol denotes a similarity transfer, that is, the input is similar but not identical to the like identified input.



4.3 GENERAL PROCEDURE TO ANALYZE FAULT TREES

To develop fault trees, the following basic steps are generally required:

1. Define the undesired event (top event) of the system under consideration.
2. Thoroughly understand the system and its intended use.
3. To obtain the predefined system fault condition cause, determine the higher order functional events. In addition, continue the fault event analysis to determine the logical interrelationship of lower level events that can cause them.
4. After accomplishing steps 1–3 construct a fault tree of logical relationships among input fault events. These are to be defined in terms of basic, identifiable, and independent faults.

To obtain quantitative results for the top event (undesired event) assign failure probability, unavailability, failure, and repair rates data to basic events provided the fault tree events are redundancy free.

A more rigorous and systematic approach requires the following steps:

1. System definition.
2. Fault tree construction.
3. Qualitative evaluation.
4. Quantitative evaluation.

The above steps are outlined in detail in the following sections:

4.3.1 System Definition

To establish the system definition in fault tree analysis is a very difficult task. A system is normally represented by a functional layout diagram showing all functional interconnections and components of the system in question. To draw a fault tree of a system, it is strongly recommended that the system boundary conditions be established. However, care must be taken so that these boundary conditions are not confused with the physical bounds of the system.

One of the most important boundary requirements is the top event (undesired event). Therefore, care must be taken to define the system top event for which the fault tree is to be drawn, because this is a major system failure. In addition to make the fault tree analysis understandable to others, the analyst must list all the assumptions on system definition and fault tree.

4.3.2 Fault Tree Construction

The major objective of fault tree construction is to represent system conditions symbolically, which may cause the system to fail. Furthermore, the fault tree construction can pinpoint the system weaknesses in a visible form. This acts as a visual tool in communicating and supporting decisions based on the analysis and to perform trade off studies or determine the adequacy of the system design.

Generally the analyst is expected to understand the system thoroughly before he proceeds to construct a system fault tree. To enhance the fault tree analysis, a system description should be part of the analysis documentation.

There are three generally accepted approaches to construct fault trees:

1. Primary failure technique.
2. Secondary failure technique.
3. Commanded failure technique.

The above techniques are used at the discretion of the reliability analyst according to the main requirements of the failure fault tree analysis.

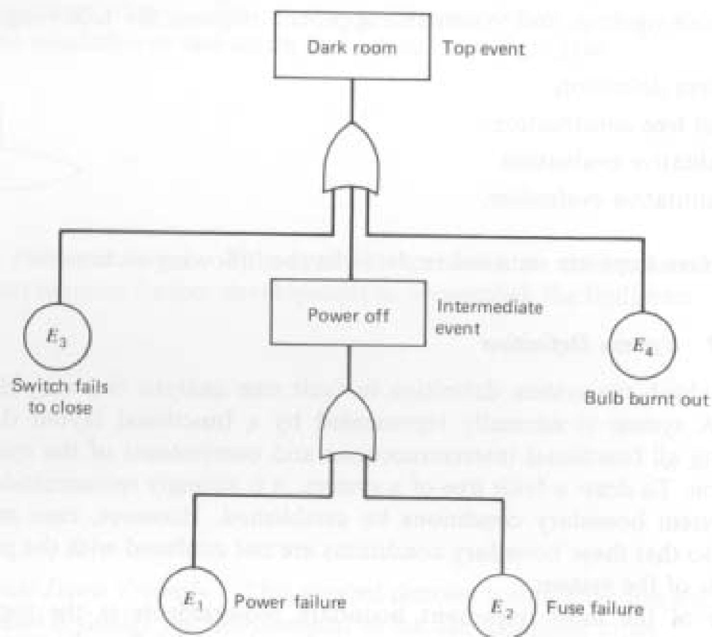


Figure 4.1 A primary failure fault tree.

Primary Failure Fault Tree Construction. The failure of a component is called primary failure if it occurs while the part is functioning within the operating parameters for which it was designed. To construct a fault tree by only using primary failures is a straightforward process, because a fault tree is only developed to the point where identifiable primary component failures will produce fault events. The following example is presented to illustrate this technique.

Example 1. Construct a fault tree of a simple system concerning a room containing a switch and a light bulb. Assume the switch only fails to close. In addition, the top event is the dark room.

The system fault tree is shown in Figure 4.1. The basic or primary events of the fault tree are as follows:

1. Power failure, E_1.
2. Fuse failure, E_2.
3. Switch fails to close, E_3.
4. Bulb burnt out, E_4.

The intermediate event is the "power off." The failure event of main concern is the top event, labeled "dark room." Therefore, the major emphasis of this analysis is toward the darkness in the room. The fault tree

in Figure 4.1 shows that the input events are gated through OR gates. At the occurrence of any one of the basic four events E_1, E_2, E_3, E_4, the system top event ("dark room") will occur.

Secondary Failure Fault Tree Construction. To include secondary failures in fault tree analysis requires a greater insight into the system. The fault tree analysis is carried out beyond the basic component failure level. The secondary failures are due to excessive environmental or operational stress placed on the system components.

Example 2. A simple fault tree with the top event "motor fails to deliver power" is shown in Figure 4.2. The fault tree shows the primary events such as switch fails to close, internal motor circuitry failure, power failure,

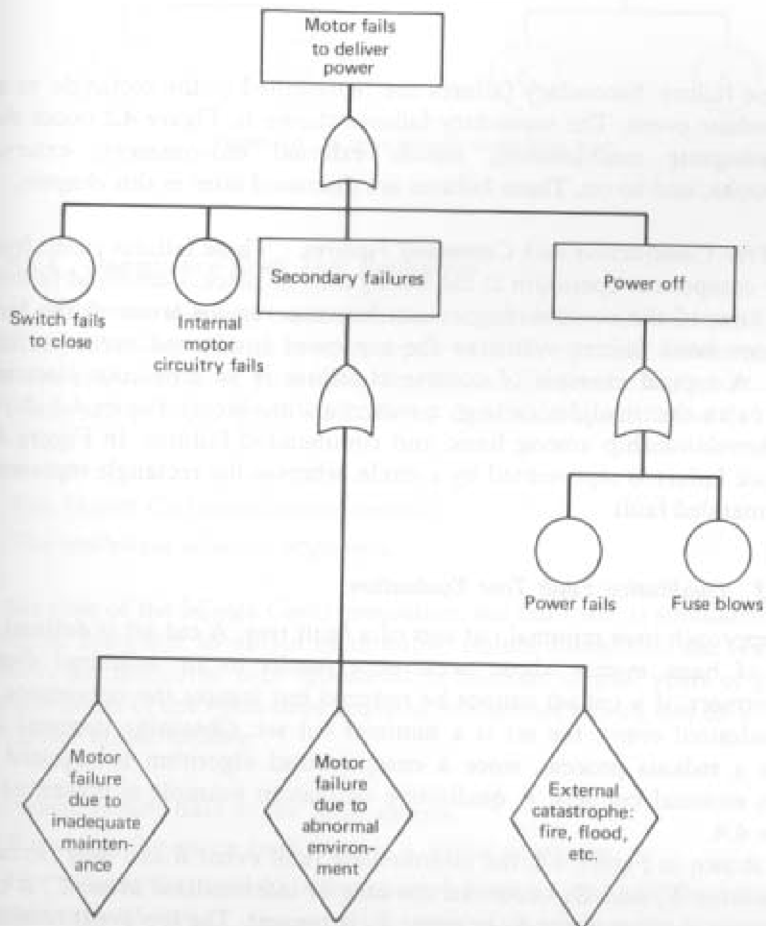


Figure 4.2 A fault tree with secondary failures.

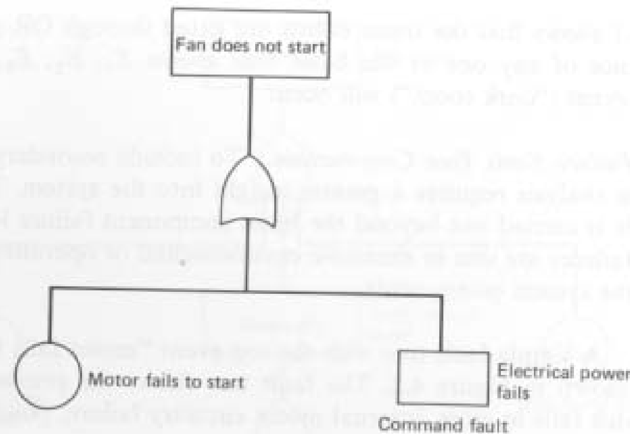


Figure 4.3 A basic and command failure fault tree.

and fuse failure. Secondary failures are represented in the rectangle as an intermediate event. The secondary failures shown in Figure 4.2 occur due to inadequate maintenance, hostile external environment, external catastrophe, and so on. These failures are discussed later in this chapter.

Fault Tree Construction with Command Failures. These failures result from proper component operation at the wrong time or place. Command failures are failures of the coordinating events between various levels of the fault tree from basic failure events to the top event (undesired event or final event). A typical example of command failure is an erroneous electrical signal to an electrical device (e.g., a motor, a transducer). Figure 4.3 shows the interrelationship among basic and commanded failures. In Figure 4.3 the basic failure is represented by a circle, whereas the rectangle represents a commanded fault.

4.3.3 *Qualitative Fault Tree Evaluation*

This approach uses minimal cut sets of a fault tree. A cut set is defined as a set of basic events whose occurrence results in an undesired event. Furthermore, if a cut set cannot be reduced but insures the occurrence of the undesired event, the set is a minimal cut set. Obtaining minimal cut sets is a tedious process, since a computerized algorithm is required to obtain minimal cut sets. A qualitative evaluation example is presented in Figure 4.4.

As shown in Figure 4.4, the intermediate fault event B can only occur if both events E_1 and E_2 occur. In the case of intermediate event C, it can only occur if either event E_3 or event E_4 is present. The top event results if either one of the intermediate event B or C occurs.

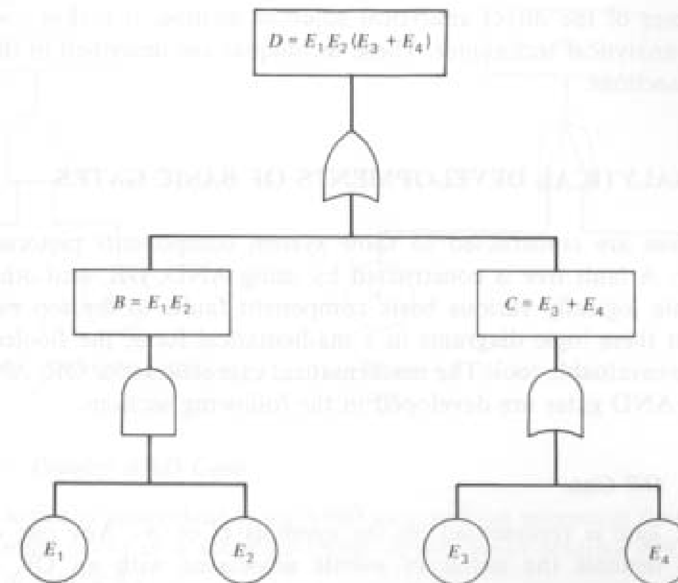


Figure 4.4 A hypothetical event fault tree.

4.3.4 *Quantitative Fault Tree Evaluation*

This evaluation uses top event quantitative reliability information, such as failure probability, failure rate, or repair rate. Component failure parameters are evaluated first, then critical path, and finally the top event.

There are two accepted methods to determine quantitative fault tree results:

1. The Monte Carlo simulation method.
2. The analytical solution approach.

In the case of the Monte Carlo simulation, the fault tree is simulated using a digital computer to obtain quantitative results. Generally, the fault tree failures are simulated over thousands or millions of trial years of performance. Some of the main steps required to simulate a fault tree on a digital computer are as follows:

1. Assign failure data to the basic events.
2. Represent the entire fault tree on a digital computer.
3. List failures that lead to occurrence of the top event and the associated minimal cut sets.
4. Compute the desired end results.

In the case of the direct analytical solution method, it makes use of the existing analytical techniques. These techniques are described in the forthcoming sections.

4.4 ANALYTICAL DEVELOPMENTS OF BASIC GATES

Fault trees are constructed to show system components pictorially and logically. A fault tree is constructed by using AND, OR, and other gates that relate logically various basic component faults to the top event. To represent these logic diagrams in a mathematical form, the Boolean algebra is an invaluable tool. The mathematical expressions for OR, AND, and Priority AND gates are developed in the following sections.

4.4.1 OR Gate

The OR gate is represented by the symbols U or $+$. Any one of these symbols denotes the union of events associated with an OR gate. A mathematical representation of two inputs OR gate is shown in Figure 4.5. The output event B_0 of an OR gate in Boolean algebra is written as

$$B_0 = B_1 + B_2 \tag{4.1}$$

where B_1 and B_2 are the input events.

4.4.2 AND Gate

In Boolean algebra the AND situation is represented by the symbol $\cdot$ or $\cap$. This symbol represents intersection of events. The two-input AND gate is shown in Figure 4.6. The output event, B_0, of the AND gate in Boolean algebra is represented by (4.2):

$$B_0 = B_1 \cdot B_2 \tag{4.2}$$

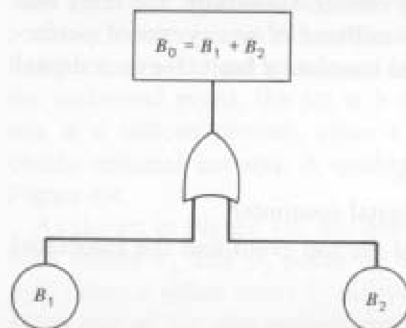


Figure 4.5 An OR gate with two input events.

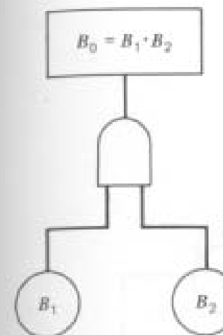


Figure 4.6 A two input AND gate.

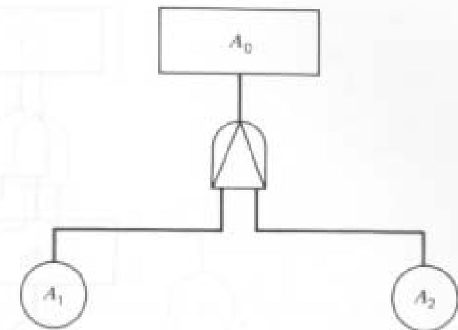


Figure 4.7 A two input priority AND gate.

4.4.3 Priority AND Gate

This is logically equivalent to an AND gate with an exception that its input events must occur in a specified order. A two input priority AND gate is shown in Figure 4.7.

In this situation it is supposed that the event A_1 must occur before event A_2. The development of a mathematical expression for the gate is presented in reference 31.

4.5 A FAULT TREE WITH REPEATED EVENTS

This type of situation is illustrated in Figure 4.8. The alphabetic letters in the diagram represent the fault events; A_1, A_2, A_3, and C indicate the basic fault events; B_1, B_2, B_0, the mean intermediate fault events; T the top event.

The fault tree shown in Figure 4.8 can be represented by the Boolean expressions as follows:

$$T = C \cdot B_0 \tag{4.3}$$

$$B_0 = B_1 \cdot B_2 \tag{4.4}$$

$$B_1 = (A_1 + A_2) \tag{4.5}$$

$$B_2 = (A_1 + A_3) \tag{4.6}$$

By substituting expressions (4.4) and (4.6) in expression (4.3) we get

$$T = C \cdot (A_1 + A_2) \cdot (A_1 + A_3) \tag{4.7}$$

It is clearly shown in Figure 4.8 that the event A_1 is the repeated basic fault event. Therefore, the expression (4.7) has to be simplified by applying the basic Boolean algebra properties.

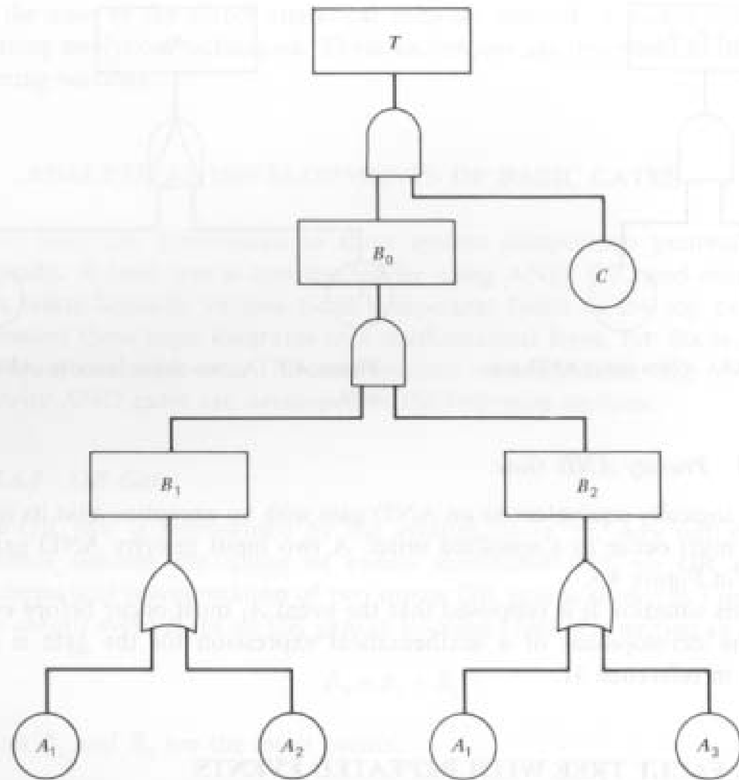


Figure 4.8 A fault tree with repeated events.

Basic Boolean Algebra Properties

1. Laws of absorption:

$$A+(A\cdot B)=A \tag{4.8}$$

$$A\cdot(A\cdot B)=A\cdot B \tag{4.9}$$

2. Identities:

$$A+A=A \tag{4.10}$$

$$A\cdot A=A \tag{4.11}$$

3. Distributive laws:

$$A+B\cdot C=(A+B)(A+C) \tag{4.12}$$

By applying distributive law of expression (4.12) to expression (4.4) we get

$$B_0=A_1+A_2\cdot A_3 \tag{4.13}$$

By using expressions (4.10) and (4.11) in (4.3), expression (4.7) reduces to

$$T=C[A_1+A_2\cdot A_3] \tag{4.14}$$

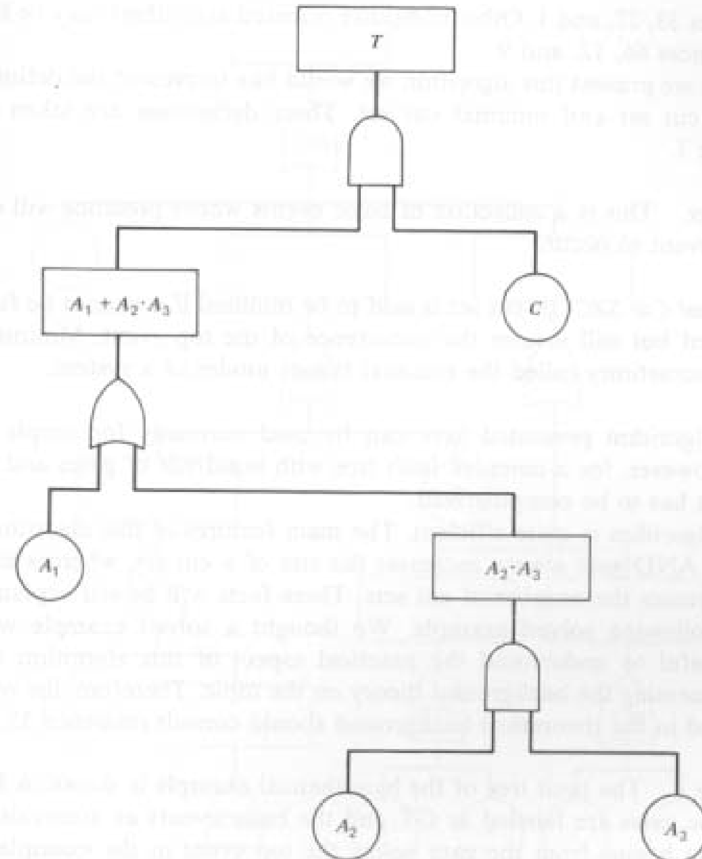


Figure 4.9 A simplified fault tree.

Because of expression (4.14) our original fault tree of Figure 4.8 reduces to the one shown in Figure 4.9.

Therefore, it is always recommended to reduce the repeated event expression by applying the Boolean properties before obtaining the quantitative reliability parameter results. Otherwise, the quantitative results will be misleading. Algorithms to obtain repeated events free fault tree are presented in references 1, 27, 33, 66, and 12. One such algorithm is presented in the section to follow:

4.6 AN ALGORITHM TO OBTAIN MINIMAL CUT SETS

A difficult problem associated with the fault tree technique is to obtain minimal cut sets of a fault tree. Here we present an algorithm developed in

references 33, 27, and 1. Other computer oriented algorithms may be found in references 66, 12, and 9.

Before we present this algorithm we would like to present the definitions of both cut set and minimal cut set. These definitions are taken from reference 1.

A Cut Set. This is a collection of basic events whose presence will cause the top event to occur.

A Minimal Cut Set. A cut set is said to be minimal if it cannot be further minimized but still insures the occurrence of the top event. Minimal cut sets are sometimes called the minimal failure modes of a system.

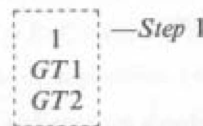
The algorithm presented here can be used manually for simple fault trees. However, for a complex fault tree with hundreds of gates and basic events, it has to be computerized.

The algorithm is quite efficient. The main features of this algorithm are that the AND gate always increases the size of a cut set, whereas an OR gate increases the number of cut sets. These facts will be self-explanatory in the following solved example. We thought a solved example will be more useful to understand the practical aspect of this algorithm rather than presenting the background theory on the topic. Therefore, the readers interested in the theoretical background should consult reference 33.

Example 3. The fault tree of the hypothetical example is shown in Figure 4.10. The gates are labeled as GT and the basic events as numerals. This algorithm begins from the gate below the top event in the example. It is labeled as GT0. As we know from our past basic knowledge on fault trees, the top event gate may normally be AND or OR gate.

However, if the top event gate, GT0, is an OR gate then each input to the OR gate represents an entry for each row of the list matrix. Whereas, in the case of an AND gate, each input represents an entry for each column of the list matrix.

For example, as shown in Figure 4.10, the top event gate, GT0, is an OR gate, therefore, we begin the formulation of the list matrix by listing inputs, GT1 and GT2 (output events) in a single column but in separate rows as follows:



Any one input of an OR gate will cause the occurrence of an output event. Therefore, the inputs of the GT0 are the members of separate cut sets.

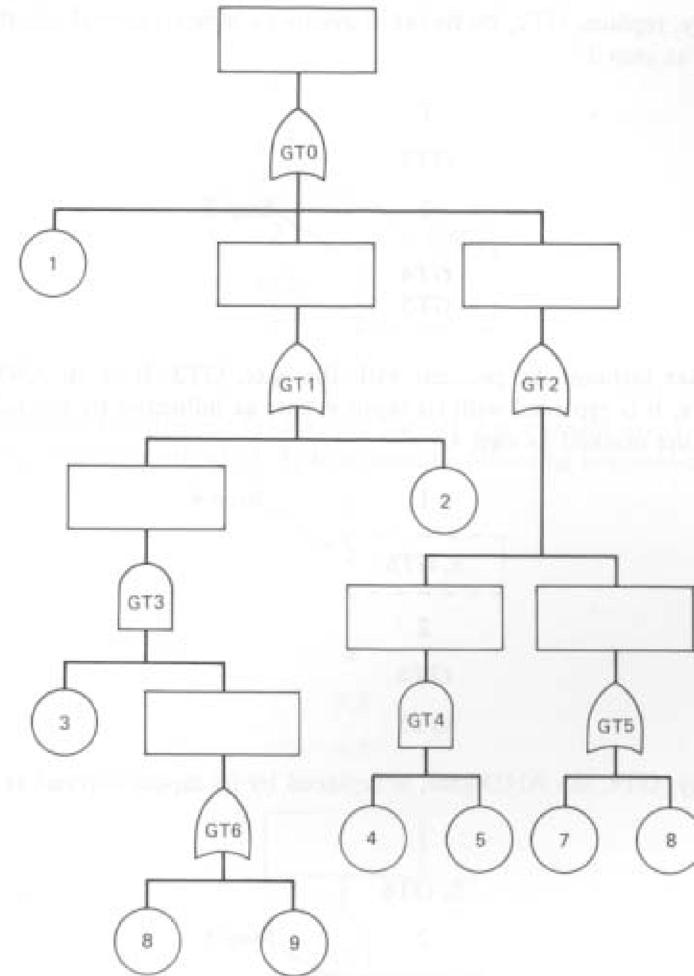
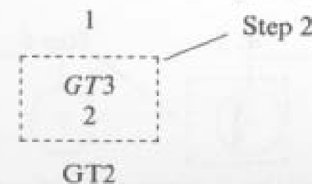


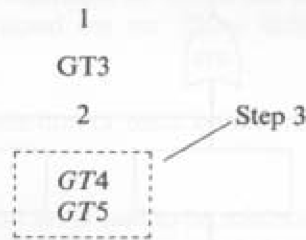
Figure 4.10 An event tree.

A simple rule to follow to develop this technique is to replace each gate by its inputs. The inputs may be the outputs of gates or basic events until all the fault tree gates are replaced with the basic event entries. At this stage the list matrix is fully completed.

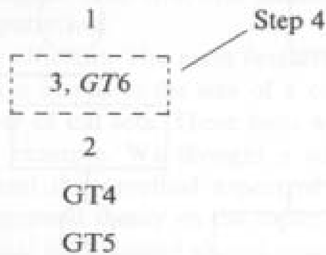
For this example, to obtain a fully constructed list matrix we now replace the OR gate GT1 by its input events as separate rows, as indicated below by the dotted line. The dotted line is marked as step 2:



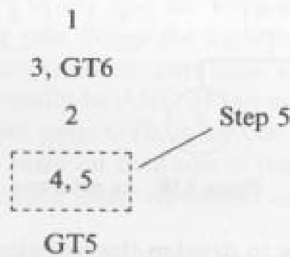
Similarly, replace, GT2, by its input events as indicated by the dotted line marked as step 3:



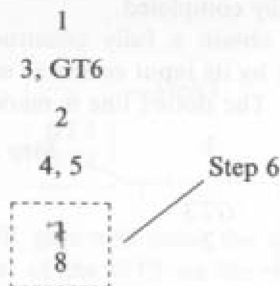
In similar fashion, we proceed with the gate, GT3. It is an AND gate, therefore, it is replaced with its input events as indicated by the following dotted line marked as step 4;



Similarly, GT4, the AND gate, is replaced by its inputs marked as step 5:

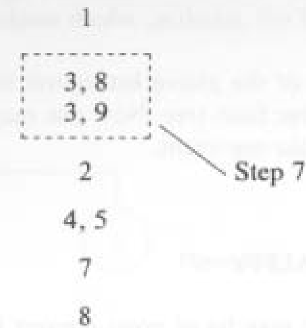


Since GT5 is an OR gate, it is replaced by its input events 7, 8 shown as step 6 below:



Similarly, the gate, GT6, is also an OR gate; therefore it is replaced by its

input events 8 and 9 (marked as step 7) as follows:



As shown above in the list matrix, the cut set 8 is a single event cut set. Therefore, eliminate cut set {3, 8} to obtain the following minimal cut sets:

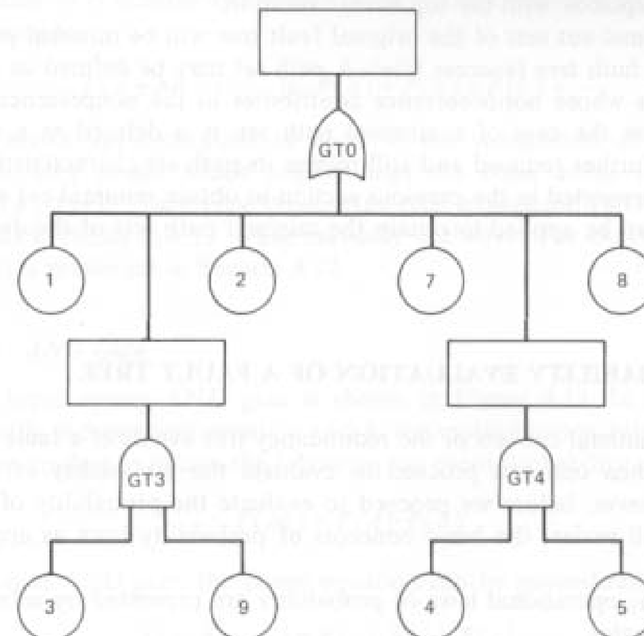


Figure 4.11 A repeated event fault tree.

Finally, if there is no repeated event in the list matrix then the cut sets generated by this method will be minimal cut sets. If this is not so, then eliminate the nonminimal cut sets (i.e., which contain other sets) from the final list matrix.

The reduced fault tree of the above list matrix is drawn in Figure 4.11. This is a repeated event free fault tree. Now one may proceed to obtain the quantitative measures of the top event.

4.7 FAULT TREE DUALITY

To reliability engineers it may be of great interest to obtain the dual fault tree. For example, in the case of top event "A system does not fail" is the dual of "system failure." Generally the occurrence of the top event is of interest more from the system safety view point to the safety analyst. The case of nonoccurrence of top event, may be of more interest to the reliability analyst.

As words "occurrence" and "nonoccurrence" of a top event suggest duality, it is simple to obtain a "success tree" from a "fault tree." To obtain a success tree (i.e., dual of a fault tree) replace all AND gates with OR gates in the original fault tree and vice-versa. In addition, the top, intermediate, and basic fault events are to be replaced by their corresponding duals (success events). In other words, the occurrence events with nonoccurrence events. For example, if the top event was "room dark" then it is to be replaced with the top event "room lit."

The minimal cut sets of the original fault tree will be minimal path sets of the dual fault tree (success tree). A path set may be defined as a set of basic events whose nonoccurrence contributes to the nonpresence of the top event. In the case of a minimal path set, it is defined as a set that cannot be further reduced and still retains its path set characteristics. The algorithm presented in the previous section to obtain minimal cut sets of a fault tree can be applied to obtain the minimal path sets of the dual fault tree.

4.8 PROBABILITY EVALUATION OF A FAULT TREE

Once the minimal cut sets or the redundancy free events of a fault tree are obtained, then one can proceed to evaluate the probability of the top event. However, before we proceed to evaluate the probability of a fault tree, we will review the basic concepts of probability laws as applied to logic gates.

Two basic operational laws of probability are presented by solving OR and AND gates.

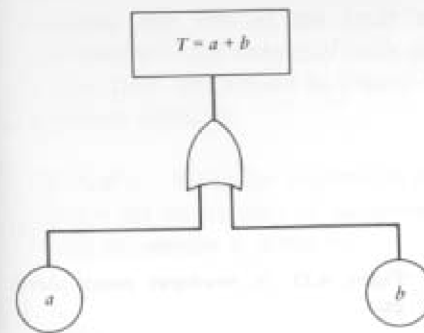


Figure 4.12 A two-input OR gate.

4.8.1 OR Gate

To explain the OR gate probability concept we are analyzing a two input OR gate as shown in Figure 4.12. For Figure 4.12, the probability expression for the top event is given by

$$P(T)=P(a)+P(b)-P(a\cdot b) \tag{4.15}$$

If a and b are statistically independent events and $P(a)\cdot P(b)$ is very small, then the above expression (4.15) can be approximated as

$$P(T)\simeq P(a)+P(b) \tag{4.16}$$

In the case of n number of inputs OR gate, the expression (4.16) may be generalized to,

$$P(a+b+c+\cdots)\simeq P(a)+P(b)+P(c)+\cdots \tag{4.17}$$

The above approximation is good if the summation of expression (4.17) is very small, which implies that the basic event probabilities $P(a)$, $P(b)$, $P(c)$, $\cdots$ are very small. However, expression (4.17) yields exact result if events $a, b, c, \cdots$ are mutually exclusive. The exact expression of (4.17) is presented in Section 4.12.

4.8.2 AND Gate

A two input events AND gate is shown in Figure 4.13. In the case of statistically independent events a and b, the multiplication rules of probability are applied to obtain the following top event probability expression:

$$P(ab)=P(a)\cdot P(b) \tag{4.18}$$

For n input AND gate, the above equation can be generalized as

$$P(a\cdot b\cdot c\cdots)=P(a)\cdot P(b)\cdot P(c)\cdots \tag{4.19}$$

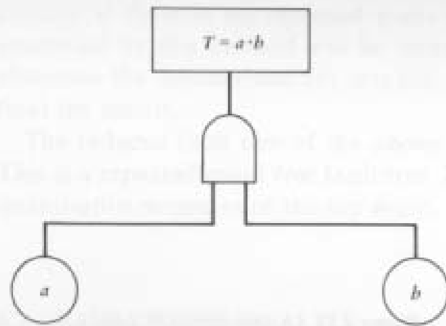


Figure 4.13 A two-input events AND gate.

Example 4. Evaluate the top event failure probability of the fault tree shown in Figure 4.14. Assume, the basic events A, B, C, D, and E are statistically independent and $P(A)=P(B)=P(C)=P(D)=P(E)=\frac{1}{4}$. The fault tree of Figure 4.14 shows that it does not have any repeated basic events. Therefore, the probability of occurrence can be evaluated at the output of each gate. However, if the repeated events in each fault tree were present then first of all one must eliminate the repeated events (i.e., obtain

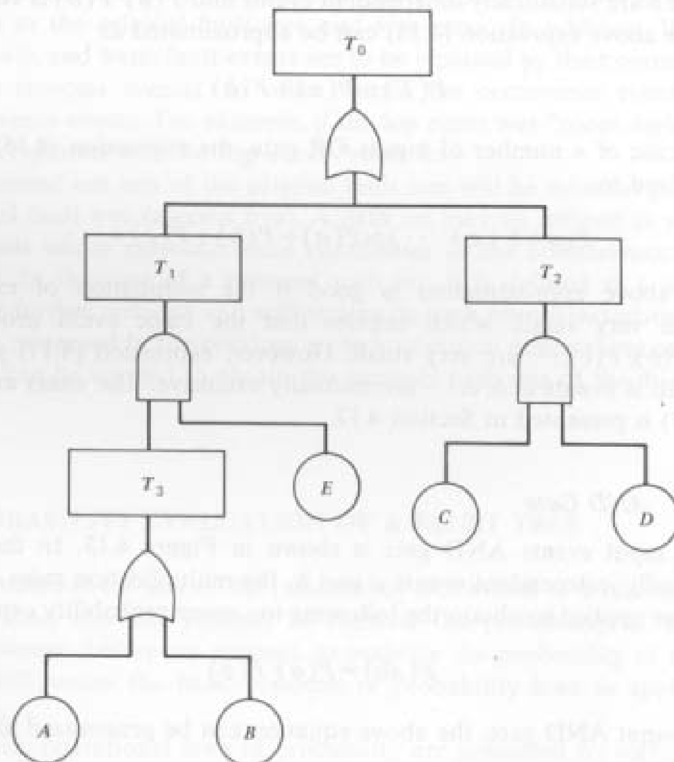


Figure 4.14 A hypothetical event tree.

minimal cut sets of the fault tree), before taking the probability of occurrence at the output of each gate.

The fault tree shown in Figure 4.14 can be solved by the following two different methods.

Method 1. Write the expression for the top event in terms of basic events. Obtain the probability of occurrence of this expression as follows. The top event expression is given by

$$T_0 = T_1 + T_2 \tag{4.20}$$

where

$$T_2 = CD \tag{4.21}$$

$$T_1 = T_3 \cdot E \tag{4.22}$$

$$T_3 = A + B \tag{4.23}$$

Hence,

$$T_0 = E(A+B) + CD \tag{4.24}$$

Therefore

$$P(T_0) = P(EA + EB + CD) \tag{4.25}$$

Now expression (4.25) can be expanded to obtain top event probability expression. If we assume the statistical occurrence of failure events then we can obtain the quantitative probability result of the top event.

Method 2. This is an alternative method to obtain the quantitative value of the top event probability by calculating the intermediate events probabilities and then using these results to obtain the top event probability result. One must note here that we assume that the failure events are statistically independent. By using expressions (4.15) and (4.18), the intermediate and top event quantitative results and expressions are as follows:

$$P(T_3) = P(A) + P(B) - P(A) \cdot P(B) = 1/4 + 1/4 - 1/16 = 7/16 \tag{4.26}$$

$$P(T_2) = P(C) \cdot P(D) = 1/4 \cdot 1/4 = 1/16 \tag{4.27}$$

$$P(T_1) = P(T_3) \cdot P(E) = 7/16 \cdot 1/4 = 7/64 \tag{4.28}$$

$$P(T_0) = P(T_1) + P(T_2) - P(T_1) \cdot P(T_2)$$

$$= 7/64 + 1/16 - 7/64 \cdot 1/16 = 169/1024 \tag{4.29}$$

$\therefore$ Probability of occurrence of top event $= 169/1024$

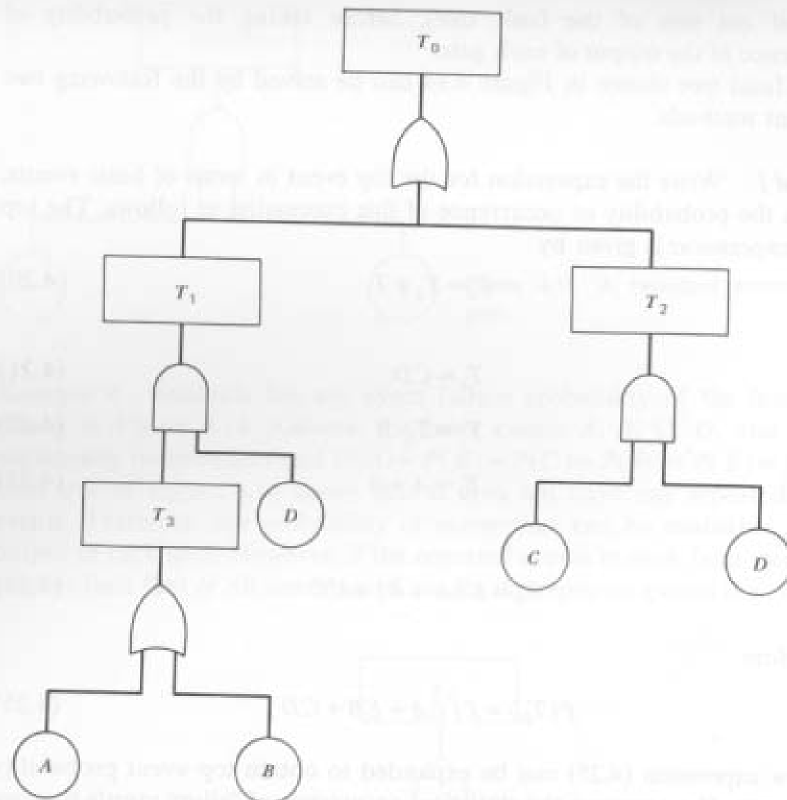


Figure 4.15 A fault tree with repeated event D.

Example 5. Suppose in Figure 4.14, the event E is replaced by event D as shown in Figure 4.15. To obtain the top event probability of the fault tree shown in Figure 4.15, we apply method 1 of the previous example. The top event expression in terms of basic events (without eliminating the repeated event D) is given by

$$T_0=(A+B)D+CD \tag{4.30}$$

Thus,

$$T_0=DA+BD+CD \tag{4.31}$$

By taking the probability of the top event, we get

$$P(DA+BD+CD)=P(DA)+P(BD)+P(CD)-P(DABD)$$
$$-P(DACD)-P(BDCD)+P(DABDCD) \tag{4.32}$$

The redundancy-free expression with statistically independent events is given by

$$P(DA+BD+CD)=P(A)P(D)+P(B)P(D)+P(C)P(D)$$
$$-P(D)P(A)P(B)-P(A)P(C)P(D)$$
$$-P(B)P(C)P(D)+P(A)P(B)P(C)P(D) \tag{4.33}$$

$$\therefore P(DA+BD+CD)=1/16+1/16+1/16-1/64$$
$$-1/64-1/64+1/256=37/256$$

The probability of occurrence of the top event is

$$37/256$$

However, if one eliminates the repeated events first then the fault tree shown in Figure 4.15 reduces to the one shown in Figure 4.16. The top event expression for Figure 4.16 becomes

$$T_0=DT_1 \tag{4.34}$$

where

$$T_1=A+B+C \tag{4.35}$$

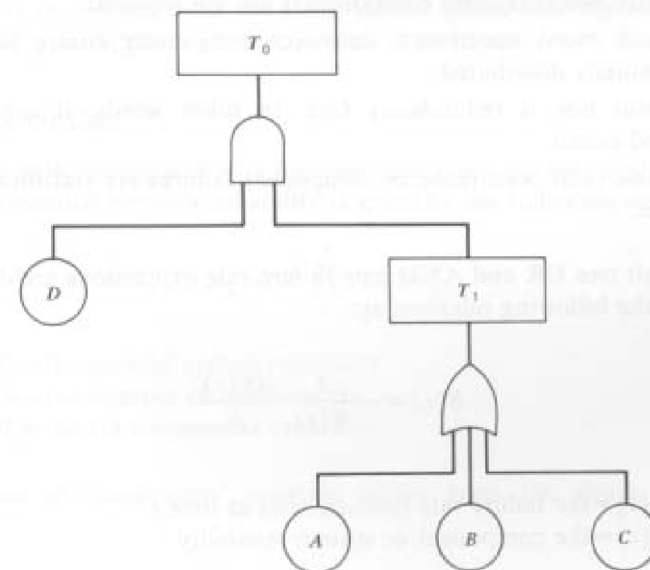


Figure 4.16 A repeated event free fault tree.

For the statistically independent events (4.34) and (4.35), probability expressions are given by

$$P(DT_1)=P(D)\cdot P(T_1)=37/64\cdot 1/4=37/256 \tag{4.36}$$

where $P(A+B+C)=P(A)+P(B)+P(C)-P(A)P(B)-P(A)P(C)-P(B)P(C)+P(A)P(B)P(C)=37/64$

4.8.3 Concluding Remarks

In cases where the basic event failure probabilities are very small, the inability to remove dependencies will not introduce a significant error in the end result [65]. However, one must try to remove all the dependencies in a fault tree before obtaining the final probability result.

4.9 FAILURE RATE EVALUATION OF FAULT TREES

This section outlines, how to obtain the failure rate of the fault tree top as well as the intermediate events. The following assumptions are made to develop this procedure:

1. The basic events (system components) are not repaired.
2. The fault event occurrence times (or component failure times) are exponentially distributed.
3. The fault tree is redundancy free. In other words, it contains no repeated events.
4. The basic fault occurrence or component failures are statistically independent.

The fault tree OR and AND gate failure rate expressions are developed by using the following relationship:

$$\lambda(t)=-\frac{1}{R(t)}\cdot\frac{dR(t)}{dt} \tag{4.37}$$

where $\lambda(t)$ = the failure rate (hazard rate) at time t
$R(t)$ = the component or system reliability

For the component constant failure rates, the OR and AND gates failure rate (hazard rate) formulas are developed in the following sections.

4.9.1 OR Gate

Logically this gate corresponds to a series system. A series system reliability can be obtained from the following equation:

$$R_S=\prod_{i=1}^{n} R_i \tag{4.38}$$

where R_i = the constant reliability of the ith component
R_S = the series system reliability
n = the number of components

When components failure times follows exponential failure laws, (4.38) becomes

$$R_S(t)=\exp-\left(\sum_{i=1}^{n}\lambda_i\right)t \tag{4.39}$$

where λ_i = constant failure rate of the ith component
t = the time

Substituting (4.39) into (4.37) yields the series system hazard rate

$$\lambda_s(t)=\sum_{i=1}^{n}\lambda_i \tag{4.40}$$

It can be recognized from the series system failure rate equation (4.40) that an OR gate output is simply the sum of its inputs.

4.9.2 AND Gate

The AND gate corresponds to a logically connected parallel configuration system. A parallel network reliability is given by the following equation:

$$R_p=1-\prod_{i=1}^{n}(1-R_i) \tag{4.41}$$

where R_p = the parallel system reliability
n = the number of components
R_i = the ith component reliability

In the case of components' constant failure rates, the above equation becomes

$$R_p(t)=1-\prod_{i=1}^{n}(1-e^{-\lambda_i t}) \tag{4.42}$$

where λ_i = the ith component constant failure rate
t = the time

After substituting (4.42) into (4.37), we get the following [53] results:

$$\lambda_p(t)=\left\{\sum_{j=1}^{n}\lambda_j(z_j-1)\right\}\left\{\prod_{j=1}^{n}z_j-1\right\}^{-1} \tag{4.43}$$

where $1/z_j=(1-e^{-\lambda_j t})$ for $j=1,2,3,\ldots,n$.

Example 6. Evaluate top event failure rate of the fault tree shown in Figure 4.17, for a 100-hour mission. Assume

$$\lambda_1=\lambda_2=\lambda_3=\lambda_4=\lambda_5=\lambda_6=\lambda_7=0.001 \text{ failure/hour}$$

By utilizing (4.40), the output event failure rates of OR gates GT1, GT3,

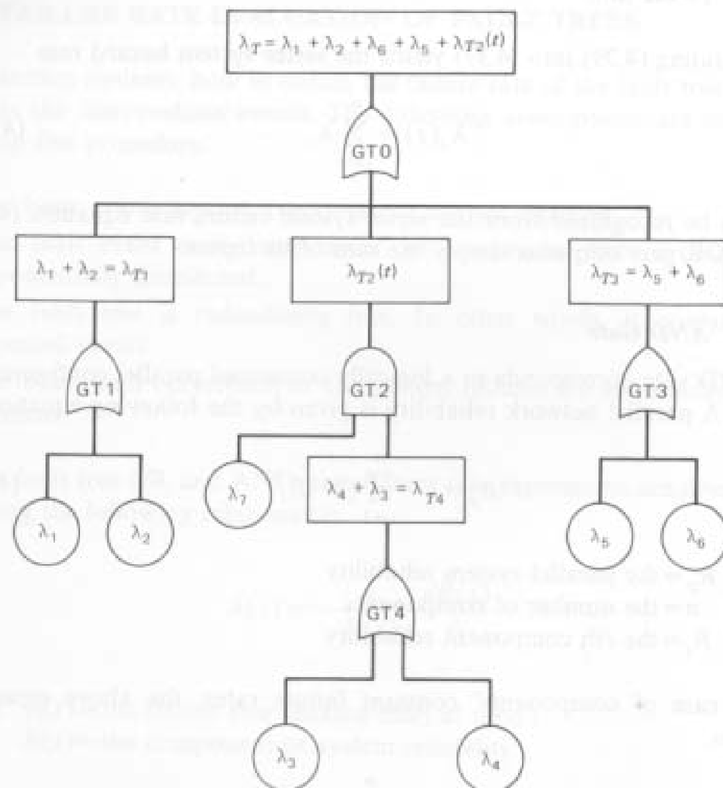


Figure 4.17 A hypothetical failure rate evaluation fault tree.

GT4, and GT0 are evaluated as follows:

$$\lambda_{T0}=\lambda_{T1}+\lambda_{T2}(t)+\lambda_{T3}=0.0040082 \text{ failure/hour} \tag{4.44}$$

$$\lambda_{T1}=\lambda_1+\lambda_2=0.002 \text{ failure/hour} \tag{4.45}$$

$$\lambda_{T3}=\lambda_5+\lambda_6=0.002 \text{ failure/hour} \tag{4.46}$$

and

$$\lambda_{T4}=\lambda_3+\lambda_4=0.002 \text{ failure/hour} \tag{4.47}$$

Similarly, we utilize (4.43) to obtain the output event failure rate of the AND gate GT2 as follows for a 100-hour mission:

$$\lambda_{T2}(t)=\frac{\lambda_7(z_7-1)+(z_{T4}-1)\lambda_{T4}}{z_7 z_{T4}-1}=0.0000082 \text{ failure/hour} \tag{4.48}$$

where $z_i=1/(1-e^{-\lambda_i t})$ for $i=7, T4$.

When an AND gate output event is an input event to another AND gate then the hazard rates of all the intermediate (including the top event) events can only be obtained from the reliability function of these events. In other words, the hazard rate or failure rate result obtained for an AND gate output event cannot be used as an input to another AND gate.

If two or more AND gates are encountered in series, it is strongly advised to establish the reliability function at the output event level of each gate then apply the hazard rate formula of (4.43).

Example 7. A two-AND-gates-in-series fault tree, shown in Figure 4.18, is required to compute the failure rate of the top event for a 100-hour mission. Assume $\lambda_1=\lambda_2=\lambda_3=0.001$ failure/hour and the basic failures are statistically independent. By utilizing (4.43) we get

$$\lambda_{GT1}(t)=\frac{2\lambda}{z+1}=0.00018 \text{ failure/hour} \tag{4.49}$$

where $z=1/(1-e^{-\lambda t})$.

Gates GT1 and GT0 output event unreliability and reliability equations are given by

$$P_{GT1}(t)=P_1(t)\cdot P_2(t) \tag{4.50}$$

$$R_{GT0}(t)=1-P_1(t)\cdot P_2(t)\cdot P_3(t) \tag{4.51}$$

where $P_i(t)$ = the unreliability of the event i at time t for $i=1,2,3$
$P_{GT1}(t)$ = the unreliability of the gate, GT1 output event
$R_{GT0}(t)$ = the reliability of the top event

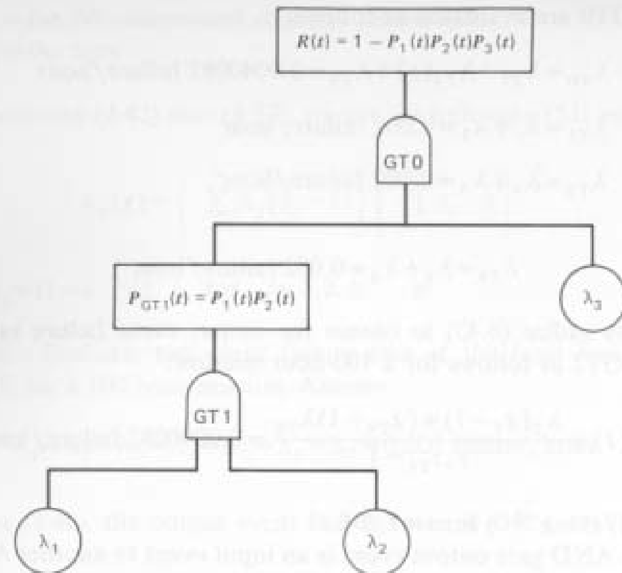


Figure 4.18 A fault tree with two AND gates in series.

To obtain the top event hazard rate, substitute (4.51) into (4.37). Since $\lambda_1 = \lambda_2 = \lambda_3$, we use (4.43) to obtain the following top event hazard rate result:

$$\lambda_{GT0}(t) = \frac{3\lambda}{z^2 + z + 1} = 0.00002 \text{ failure/hour} \tag{4.52}$$

where $z = 1/(1 - e^{-\lambda t})$.

4.10 FAULT TREE EVALUATION OF REPAIRABLE COMPONENTS

In this section we are concerned only with the fault tree evaluation of repairable components [22]. This type of situation is frequently encountered in real life where the system components are normally repaired whenever they fail. The method presented in this paper assumes that the component failures are statistically independent and that the component failure and repair rates are constant; in addition, the repaired system components are considered as good as new. Furthermore, this method is only applicable to the cases where one may be concerned with calculating the top or intermediate event steady-state unavailability, limiting mean repair rate, limiting mean failure rate, and steady-state failure rate. Another major assumption of this method is that it assumes that fault trees are redundancy free, (i.e., no basic repeated events are allowed).

In most cases a redundancy-free expression can be obtained by applying basic Boolean reduction techniques. For certain cases it is simpler to obtain Boolean indicated cut sets (BICS) [33] and then eliminate the redundant cut sets by inspection. It may also be useful to eliminate as many repeated (redundant) events as possible at the fault tree construction stage and eliminate the remaining ones with the Boolean reduction techniques. However, if some of the repeated events are impossible to eliminate and if the probability of occurrence for basic events is less than 0.1 [65], the error generated in the end result will be either negligible or of very small magnitude.

The main advantage of applying this technique is that, the original dependency free fault tree is unchanged; and the OR and AND gate steady-state unavailability, limiting mean failure rate, limiting mean repair rate, and limiting steady-state failure rate formulas, can be applied directly to both the intermediate and top events of the fault tree. These formulas [128] for the OR and AND gates are discussed in the following sections.

4.10.1 OR Gate

This gate simply represents a series system with n nonidentical repairable components. The OR gate output event unavailability $\bar{A}_s$, can be obtained from the following equation:

$$\bar{A}_s = 1 - \prod_{i \in X} (1 - \bar{A}_i) \tag{4.53}$$

where $\bar{A}_i$ = the unavailability of the repairable component i
X = a set of n number of components

For a repairable component with constant failure and repair rates the equation for the unavailability $\bar{A}$ may be expressed [129] as follows:

$$\bar{A}(t) = \frac{\lambda}{\mu + \lambda}(1 - e^{-(\lambda+\mu)t}) \tag{4.54}$$

where t = time
λ = the component failure rate
μ = the component repair rate

For large t, the above equation becomes

$$\bar{A} = \frac{\lambda}{\lambda + \mu} \tag{4.55}$$

By substituting (4.55) into (4.53) we obtain for the series system

$$\bar{A}_s = 1 - \prod_{i \in X} \frac{\mu_i}{\lambda_i + \mu_i} \tag{4.56}$$

Similarly, the following OR gate output event, limiting failure rate, limiting mean failure rate, and limiting mean repair rate equations, is

$$\lambda_{ss} = \{\text{series system steady state availability, } (1-\bar{A}_s)\} \times \{\text{series system failure rate, } \hat{\lambda}_{sm}\}$$

$$= (1-\bar{A}_s) \sum_{i \in X} \lambda_i \tag{4.57}$$

where λ_{ss} is the series system steady-state failure frequency:

$$\hat{\lambda}_{sm} = \sum_{i \in X} \lambda_i \tag{4.58}$$

where $\hat{\lambda}_{sm}$ = the series system limiting mean failure rate
$\hat{\mu}_{sm}$ = {series system steady-state availability, $(1-A_s)$} × (series system failure rate, $\hat{\lambda}_{sm}$)/(series system unavailability, $\bar{A}_s$).

$$\hat{\mu}_{sm} = \frac{\lambda_{ss}}{\bar{A}_s} \tag{4.59}$$

where $\hat{\mu}_{sm}$ is the series system limiting mean repair rate.

4.10.2 AND Gate

An AND gate is the representation of a parallel system composed of n (number) of nonidentical components. Since the parallel system is a dual of the series system AND gate output event, steady-state unavailability, steady-state failure rate, limiting mean failure rate, and limiting mean repair rate equations can be obtained directly from (4.56), (4.57), (4.58), and (4.59):

$$\bar{A}_p = \prod_{i \in X} \left\{1 - \frac{\mu_i}{\mu_i + \lambda_i}\right\} \tag{4.60}$$

where p denotes a parallel system.

$$\lambda_{ps} = \sum_{i \in X} \mu_i (\bar{A}_p) \tag{4.61}$$

$$\hat{\lambda}_{pm} = \frac{\lambda_{ps}}{1-\bar{A}_p} \tag{4.62}$$

and

$$\hat{\mu}_{pm} = \sum_{i \in X} \mu_i \tag{4.63}$$

Similarly, the respective equations, in the case of a m-out-of-n identical inputs AND gate are

$$\bar{A}_{m/n} = \sum_{i=m}^{n} \binom{n}{i} (\bar{A})^i (1-\bar{A})^{n-i} \tag{4.64}$$

$$\lambda_{m/n} = \frac{n!}{(n-m)!(m-1)!} \frac{(1/\lambda)^{m-1}}{(1/\mu)^m} \bar{A}^n \tag{4.65}$$

$$\hat{\lambda}_{m/n} = \frac{m!(1/\lambda)^{m-1}(1/\mu)^{n-m}}{(n-m)!(m-1)! \sum_{i=m}^{n} \binom{n}{i} (1/\lambda)^i (1/\mu)^{n-i}} \tag{4.66}$$

and

$$\hat{\mu}_{m/n} = \frac{n!(1/\lambda)^{m-1}(1/\mu)^{n-m}}{(n-m)!(m-1)! \sum_{i=0}^{m-1} \binom{n}{i} (1/\lambda)^i (1/\mu)^{n-i}} \tag{4.67}$$

It is easily seen from the above equations that, for identical inputs OR and AND gate, the equations are special cases of the m-out-of-n inputs AND gate equations. In the case of an AND gate, m takes on the value of the number of inputs to that AND gate, whereas in the case of an OR gate, m is equal to unity.

Example 8. Suppose the objective in Figure 4.19 is to obtain the top event steady-state unavailability, steady-state failure frequency, limiting mean failure rate, and limiting mean repair rate. Assume that all of the basic events of the fault tree have the same failure and repair rate respectively, that is, $\lambda = 0.001$ failure/hour; and $\mu = 0.05$ repair/hour. Furthermore, assume that all of the basic events are statistically independent.

From (4.55) the single component steady-state unavailability is

$$\bar{A} = \frac{\lambda}{\lambda+\mu} = \frac{0.001}{0.051} \cong 0.02$$

In the case of an OR gate output event GT1, the unavailability from (4.53) is

$$\bar{A}_s \cong 0.04$$

From (4.57),

$$\lambda_{ss} = (\lambda_1 + \lambda_2) \prod_{i=1}^{2} \frac{\mu_i}{\mu_i + \lambda_i}$$

$$= 0.0019 \text{ failure/hour}$$

TEXAS A&M UNIVERSITY LIBRARY

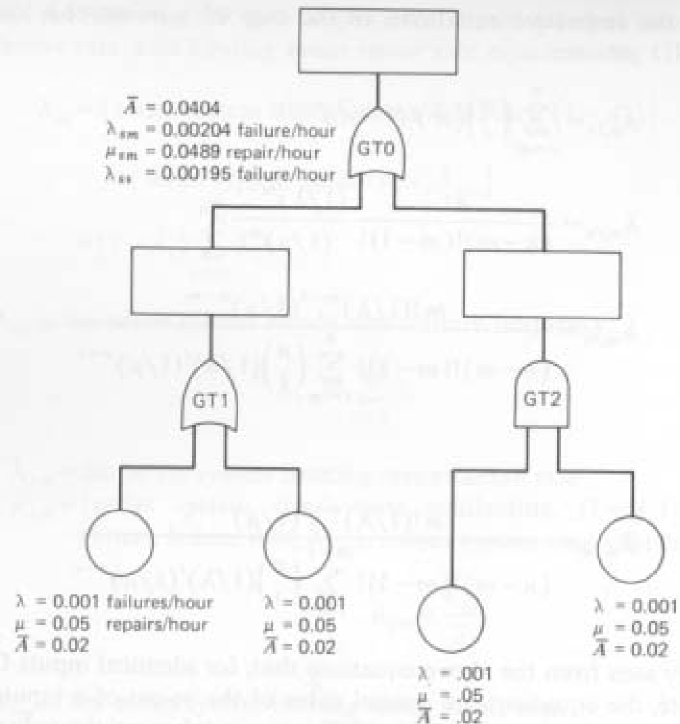


Figure 4.19 A hypothetical fault tree.

Equation 4.58 yields

$$\lambda_{sm} = 0.002 \text{ failure/hour}$$

The limiting mean repair rate $\hat{\mu}_{sm}$ is obtained from (4.59)

$$\hat{\mu}_{sm} = \frac{\left(\sum_{i=1}^{2} \lambda_i\right)\left(\prod_{i=1}^{2} \frac{\mu_i}{\mu_i + \lambda_i}\right)}{1 - \prod_{i=1}^{2} \mu_i/(\lambda_i + \mu_i)}$$

$$= 0.0475 \text{ repair/hour}$$

Similarly, for the AND gate output event, GT2, and top event OR gate GT0, the following information was calculated from (4.60), (4.61), (4.62), (4.63), (4.56), (4.57), (4.58), and (4.59), respectively. In the case of an AND

gate GT2,

$$\bar{A}_p = 0.0004$$

$$\lambda_{ps} = 0.00004 \text{ failure/hour}$$

$$\hat{\lambda}_{pm} = 0.000041 \text{ failure/hour}$$

and

$$\hat{\mu}_{pm} = 0.01 \text{ repair/hour}$$

Similarly, in the case of the top event OR gate, GT0

$$\bar{A}_s = 0.0404$$

$$\lambda_{ss} = 0.00195 \text{ failure/hour}$$

$$\hat{\lambda}_{sm} = 0.00204 \text{ failure/hour}$$

and

$$\hat{\mu}_{sm} = 0.0489 \text{ repair/hour}$$

4.11 LAMBDA TAU METHOD

This is another method that takes into consideration the repair of the basic components. The Lambda Tau technique requires redundant-free expressions from the fault tree diagram. In other words the basic events of the tree must not be repeated events. In many cases it may be obtained by Boolean substitution reduction techniques. However, this method incorporates many other restrictions. The Lambda Tau method calculations for an AND gate are based on the coexistence of all failures, and the calculations for an OR gate are based upon at least one failure among n number of possible failures. The basic formulas for the AND and OR gate parameters are derived in flow research references 124 and 65. The main restrictions of this technique are (a) τ/T is small, where τ is repair time of a component in question, where T is the time interval of interest; (b) the basic event failure rates are very small; (c) the product of the failure rate and repair time is very small (i.e., must be less than 1); (d) the product of the failure rate and the mission time is very small (i.e., must be less than 1 preferably 0.1); (e) the failures and repair rates are constant; and (f) failures occur independently.

The basic formulas for reliability of the AND (AND Priority) OR gates are derived in reference 126. AND and OR gate parameter formulas are presented in the following sections.

4.11.1 AND Gate (Coexistence of All Failures)

The general formula of the probability, P_{AND}, that n failures coexist in a small time interval, dt for the first time can be obtained:

$$P_{\text{AND}} = \prod_{i=1}^{n} \lambda_i \left[\prod_{i=2}^{n} \tau_n + \tau_1 \tau_3 \cdots \tau_n + \cdots \tau_1 \tau_2 \cdots \tau_{n-1} \right] t \tag{4.68}$$

where n is the number of components and λ_i is the constant failure rate of the ith component.

The AND gate output event hazard rate (failure rate) and repair time equations are given by

$$\lambda_{\text{AND}} = \prod_{i=1}^{n} \lambda_i \left[\prod_{i=2}^{n} \tau_i + \prod_{\substack{i=1 \\ i \neq \text{even}}}^{n} \tau_i + \cdots \prod_{i=1}^{n-1} \tau_i \right] \tag{4.69}$$

and

$$\tau_{\text{AND}} = \frac{1}{\sum_{i=1}^{n} \tau_i} \tag{4.70}$$

It is emphasized that (4.68), (4.69), and (4.70) are only valid for assumptions outlined in the earlier section

4.11.2 OR Gate (At Least One Failure Among n Possible Failures)

This gate represents a system with n components connected in a series configuration. The probability that one or more failures occur is

$$P_{\text{OR}}(t) = 1 - e^{(\sum_{i=1}^{n} \lambda_i)t} \tag{4.71}$$

The OR gate output event failure rate and repair time are

$$\lambda_{\text{OR}} = \sum_{i=1}^{n} \lambda_i \tag{4.72}$$

and

$$\tau_{\text{OR}} = \frac{\sum_{i=1}^{n} \lambda_i \tau_i}{\sum_{i=1}^{n} \lambda_i} \tag{4.73}$$

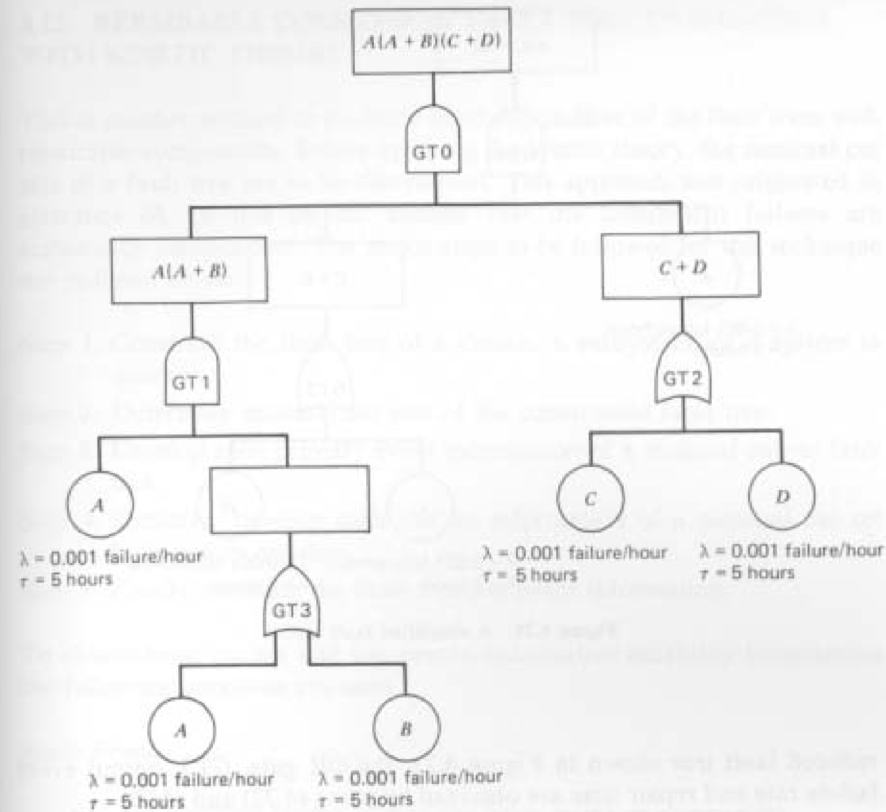


Figure 4.20 A fault tree containing repeated events.

As for the AND gate output event formulas, these equations are only valid under the assumptions outlined in the sections earlier.

Example 9. A fault tree containing a repeated event is shown in Figure 4.20. Assume the occurrence of basic fault events is statistically independent; then obtain the top event quantitative measures of the Lambda Tau technique.

As it can be realized from the fault tree that the repeated event A has to be eliminated before we can apply the Lambda Tau technique to compute quantitative reliability measures.

The output event expression of the gate, $GT1$, can be simplified by applying the following Boolean identity:

$$A(A+B) = A \tag{4.74}$$

Therefore the simplified fault tree of Figure 4.20 becomes as shown in Figure 4.21. To determine the top event quantitative measures of the

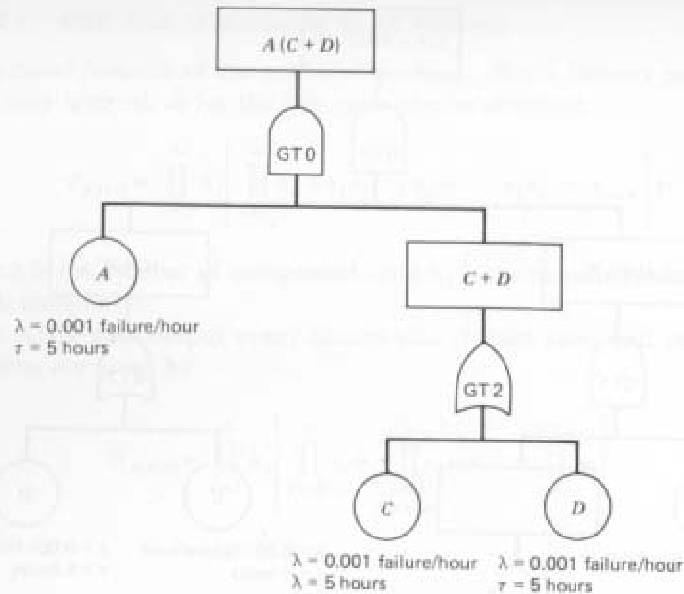


Figure 4.21 A simplified fault tree.

reduced fault tree shown in Figure 4.21, the OR gate, $GT2$, output event failure rate and repair time are obtained by using (4.72) and (4.73)

$$\lambda_{GT2}=2\lambda=0.002 \text{ failure/hour} \tag{4.75}$$

$$\tau_{GT2}=\tau=5 \text{ hours} \tag{4.76}$$

To obtain the quantitative measures of the top event, failure rate and repair time, use expressions (4.69) and (4.70), respectively:

$$\lambda_{GT0}=\lambda_A\lambda_{GT2}(\tau_A+\tau_{GT2})=0.00002 \text{ failure/hour} \tag{4.77}$$

$$\tau_{GT0}=\frac{\tau_{GT2}\tau_A}{\tau_{GT2}+\tau_A}=2.5 \text{ hours} \tag{4.78}$$

For a 100-hour mission, the top event probability that n failures coexist in time interval dt for the first time is

$$\begin{aligned} P_{GT0}&=\lambda_{GT0}t \\ &=0.00002\times 100=0.002/\text{mission} \end{aligned} \tag{4.79}$$

where λ_{GT0} is obtained from (4.77).

4.12 REPAIRABLE COMPONENT FAULT TREE EVALUATION WITH KINETIC THEORY

This is another method to evaluate reliability indices of the fault trees with repairable components. Before applying the kinetic theory, the minimal cut sets of a fault tree are to be determined. This approach was originated in reference 68. In this section assume that the component failures are statistically independent. The major steps to be followed for this technique are outlined below:

Step 1. Construct the fault tree of a device, a subsystem, or a system in question.

Step 2. Determine minimal cut sets of the constructed fault tree.

Step 3. Develop each primary event information of a minimal cut set fault tree.

Step 4. Similarly, develop each cut set information of a minimal cut set fault tree in question.

Step 5. Finally, evaluate the fault tree top event information.

To obtain basic cut set and top events quantitative reliability information the following notations are used.

Basic Events.

$\lambda=$ the constant failure rate of the basic event or component
$\mu=$ the constant repair rate of the basic event or component
$t=$ mission time
$F(t)=$ probability of a component failed condition at time t
$F_f(t)=$ probability that a component has its first failure by time t
$W=$ probability that a component fails or a basic fault event occurs in time interval $[t, t+\Delta t]$
$W_f=$ probability that a component has its first failure in time interval $[t, t+\Delta t]$

Cut-Sets.

$\lambda'(t)=$ the cut set failure rate at time t
$\mu'(t)=$ the cut set repair rate at time t

Top Event.

$\lambda_T(t)=$ the top event failure rate at time t
$\mu_T(t)=$ the top event repair rate at time t

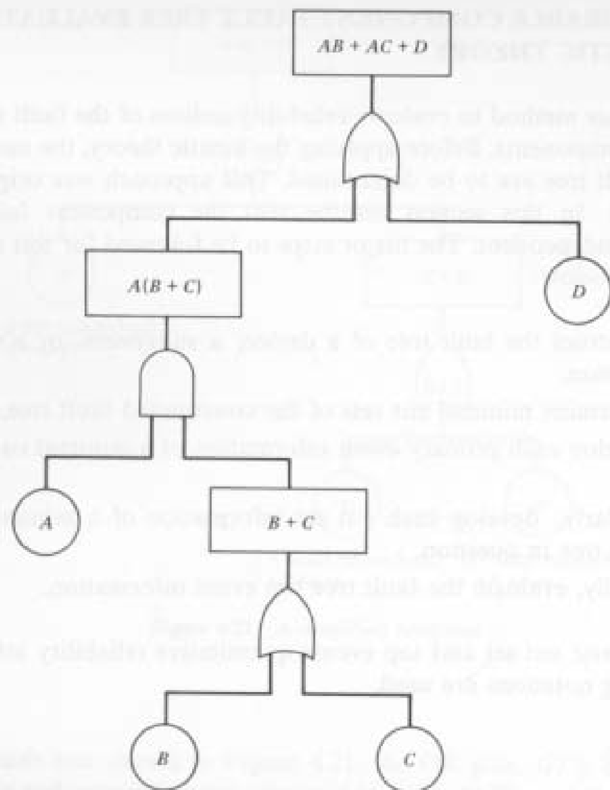


Figure 4.22 A hypothetical fault tree.

In a detailed form the kinetic tree theory is described in reference 69. Here we simply deal with the practical aspect of this theory, with assumptions that the basic failure rate, and repair rates are constant and the failures are statistically independent [130]. To demonstrate the practicality of this approach, the following hypothetical example is presented in Figure 4.22.

Example 10. For the fault tree shown in Figure 4.22, it is necessary to obtain the top event unavailability and failure and repair rate information. For the fault tree shown we develop the required information [130] for the basic events, cut-sets, and top event. One should note here that the constructed fault tree has no repeated events.

BASIC FAILURE EVENT INFORMATION. Assume that a repairable component has constant failure and repair rates; therefore, by applying the Markov process concept we obtain the following differential-difference equations

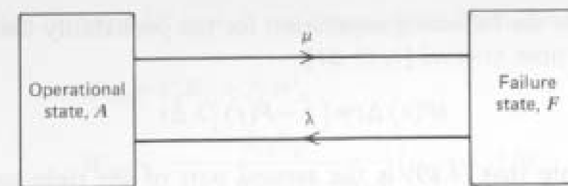


Figure 4.23 A single component state space diagram.

for the component operational and failure states as shown in Figure 4.23.

$$A(t+\Delta t)=(1-\lambda\,\Delta t)A(t)+\mu\,\Delta t\,F(t) \tag{4.80}$$

$$F(t+\Delta t)=(1-\mu\,\Delta t)F(t)+\lambda\,\Delta t\,A(t) \tag{4.81}$$

In the limiting case the above equations become

$$\frac{dA(t)}{dt}=-\lambda A(t)+\mu F(t) \tag{4.82}$$

$$\frac{dF(t)}{dt}=-\mu F(t)+\lambda A(t) \tag{4.83}$$

At $A(0)=1$, other initial condition probabilities are equal to zero, where $A(t)$ is the component availability at time t and $F(t)$ is the component unavailability at time t. By solving the above differential equations we get

$$A(t)=\frac{\mu}{\lambda+\mu}+\frac{\lambda}{\lambda+\mu}e^{-(\lambda+\mu)t} \tag{4.84}$$

$$F(t)=\frac{\lambda}{\lambda+\mu}-\frac{\lambda}{\lambda+\mu}e^{-(\lambda+\mu)t} \tag{4.85}$$

For large t, (4.85) becomes

$$F=\frac{\lambda}{\lambda+\mu} \tag{4.86}$$

To obtain the failure probability at time t, set $\mu=0$ in (4.85):

$$F_f(t)=1-e^{-\lambda t} \tag{4.87}$$

For small λt the above equation may be approximated to

$$F_f(t)\simeq\lambda t \tag{4.88}$$

Now, we define the following expression for the probability that a component fails in a time interval $[t, t+\Delta t]$:

$$W(t)\Delta t = [1-F(t)]\lambda\,\Delta t \tag{4.89}$$

One should note that (4.89) is the second part of the right-hand side of (4.81). By substituting (4.85) into (4.89) for large t we get

$$W = W(t)\Delta t = \frac{\mu}{\lambda+\mu}(\lambda\,\Delta t) \tag{4.90}$$

Similarly, for a nonrepairable component (i.e., $\mu=0$) substitute (4.87) into (4.89) for small λt; we get

$$W_f = W_f(t)\cdot\Delta t = \lambda\,\Delta t \tag{4.91}$$

CUT SET INFORMATION. To demonstrate how to obtain the cut set information we will use the fault tree example shown in Figure 4.22. The top event expression of Figure 4.22 is composed of the following cut sets:

$$\text{Top event} = AB + AC + D \tag{4.92}$$

Now, consider the cut set AB in (4.92). Here, we are interested to find the probability of first failure in time interval $[t, t+\Delta t]$.

There are two possibilities to encounter failure of cut set, AB, in a small interval Δt (here we assume that only one failure occurs in a small time Δt):

1. A is in failed state and B fails in Δt
2. B is in failed state and A fails in Δt

Thus we define, W_{AB}, as the probability of first failure of the cut set AB in the time interval $[t, t+\Delta t]$. Therefore,

$$W_{AB} = F_A W_B + F_B W_A \tag{4.93}$$

In the case of repairable events A and B substitute (4.86) and (4.90) into (4.93):

$$W_{AB} = \frac{\lambda_A}{(\lambda_A+\mu_A)}\cdot\frac{\lambda_B\mu_B}{(\lambda_B+\mu_B)}\cdot\Delta t + \frac{\lambda_B}{(\lambda_B+\mu_B)}\cdot\frac{\lambda_A}{(\lambda_A+\mu_A)}\mu_A\cdot\Delta t \tag{4.94}$$

$$= \frac{\lambda_A\lambda_B}{(\lambda_A+\mu_A)(\lambda_B+\mu_B)}\{\mu_B+\mu_A\}\Delta t \tag{4.95}$$

Similarly, for cut sets AC and D we obtain the following expressions:

$$W_{AC} = F_A W_C + F_C W_A \tag{4.96}$$

$$W_{AC} = \frac{\lambda_A\lambda_C}{(\lambda_A+\mu_A)(\lambda_C+\mu_C)}\{\mu_C+\mu_A\}\Delta t \tag{4.97}$$

and

$$W_D = W_D \tag{4.98}$$

$$W_D = \frac{\lambda_D\mu_D}{(\lambda_D+\mu_D)}\cdot\Delta t \tag{4.99}$$

To determine probability that the cut sets AB, AC, and D are in failed state one should multiply the individual event probabilities for the statistically independent events. Thus, by utilizing (4.86), we obtain

$$F_{AB} = F_A F_B = \frac{\lambda_A\lambda_B}{(\lambda_A+\mu_A)(\lambda_B+\mu_B)} \tag{4.100}$$

$$F_{AC} = F_A F_C = \frac{\lambda_A\lambda_C}{(\lambda_A+\mu_A)(\lambda_C+\mu_C)} \tag{4.101}$$

$$F_D = \frac{\lambda_D}{\lambda_D+\mu_D} \tag{4.102}$$

Suppose, if event B of the cut set AB is not repaired, then we will denote with a small alphabetic letter, b. Therefore one may rewrite (4.93) as

$$W_{Ab} = F_A W_b + F_b W_A \tag{4.103}$$

In the case of repairable and nonrepairable events A and b, respectively, substitute equations (4.91), (4.90), (4.86), and (4.88) into (4.103) to obtain

$$W_{Ab} = \frac{\lambda_A}{\lambda_A+\mu_A}\cdot(\lambda_b\Delta t) + (\lambda_b t)\frac{\mu_A\lambda_A}{\mu_A+\lambda_A}\Delta t \tag{4.104}$$

Hence,

$$W_{Ab} = \frac{\lambda_A\lambda_b}{\lambda_A+\mu_A}(1+t\mu_A)\Delta t \tag{4.105}$$

To obtain cut set failure rate we use (4.89)

$$\lambda'(t) = \frac{W(t)}{1-F(t)} \tag{4.106}$$

Similarly, the cut set repair rate is obtained by using equation (4.107):

$$\mu'(t)=\frac{W(t)}{F(t)} \tag{4.107}$$

Since

$$W=W(t)\,dt \tag{4.108}$$

Now consider the cut set AB, since W_{AB} is known from (4.95) therefore, we substitute (4.95) into (4.108) to get

$$W_{AB}(t)=\frac{\lambda_A\lambda_B}{(\lambda_A+\mu_A)(\lambda_B+\mu_B)}\{\mu_A+\mu_B\} \tag{4.109}$$

To obtain cut set AB repair rate, substitute (4.100) and (4.109) into (4.107) to get

$$\mu'_{AB}=\mu_A+\mu_B \tag{4.110}$$

Similarly, to obtain cut set failure rate, substitute (4.100) and (4.109) into (4.106) to get

$$\lambda'_{AB}=\frac{\lambda_A\lambda_B(\mu_A+\mu_B)}{\lambda_A\mu_B+\mu_A\lambda_B+\mu_A\mu_B} \tag{4.111}$$

In similar fashion, one can obtain the failure and repair rates for cut sets AC and D as follows:

$$\lambda'_{AC}=\frac{\lambda_A\lambda_C(\mu_A+\mu_C)}{\lambda_A\mu_C+\mu_A\lambda_C+\mu_A\mu_C} \tag{4.112}$$

$$\lambda'_D=\lambda_D \tag{4.113}$$

and

$$\mu'_{AC}=(\mu_A+\mu_C) \tag{4.114}$$

$$\mu'_D=\mu_D \tag{4.115}$$

TOP EVENT INFORMATION. To obtain the top event probability information, one has to take advantage of the union of the minimal cut sets, since the occurrence of any one of the cut sets will cause the top event to occur.

The probability of the union of the top events is given by

$$\begin{aligned}P(T_1+T_2+\cdots+T_n)=&[P(T_1)+P(T_2)+\cdots+P(T_n)] && \leftarrow n \text{ terms}\\ &-\Big[P(T_1T_2)+P(T_1T_3)+\cdots+P\Big(\underset{i\neq j}{T_i\ T_j}\Big)\Big] && \leftarrow\tbinom{n}{2}\text{ terms}\\ &+\Big[P(T_1T_2T_3)+P(T_1T_2T_4)+\cdots+P\Big(\underset{i\neq j\neq k}{T_iT_jT_k}\Big)\Big] && \tbinom{n}{3}\text{ terms}\\ &\cdots(1)^{n-1}[P(T_1T_2\cdots T_n)] && \leftarrow\tbinom{n}{n}\text{ term}\end{aligned} \tag{4.116}$$

Consider now the following top event minimal cut set expression of Figure 4.22:

$$T=AB+AC+D \tag{4.117}$$

The probability expression of the above expression becomes

$$\begin{aligned}F(AB+AC+D)=&F(AB)+F(AC)+F(D)-F(ABC)-F(ABD)\\ &-F(ACD)+F(ABCD)\end{aligned} \tag{4.117}$$

For statistically independent events

$$\begin{aligned}F_{TOP}=F(AB+AC+D)=&F_AF_B+F_AF_C+F_D-F_AF_BF_C-F_AF_BF_D\\ &-F_AF_CF_D+F_AF_BF_CF_D\end{aligned} \tag{4.118}$$

Now consider (4.117); it contains event A, which is common to both cut sets AB and AC. The occurrence of this common event A will cause the simultaneous failure of cut sets AB and AC, if the component A fails in interval $[t, t+\Delta t]$.

The probability expression of this intersection is given by:

$$W_{ABC}=W_AF_BF_C \tag{4.119}$$

Therefore by substituting (4.86) and (4.90) into the above expression we get

$$W_{ABC}=\frac{\lambda_A\lambda_B\lambda_C\mu_A}{(\lambda_A+\mu_A)(\lambda_B+\mu_B)(\lambda_C+\mu_C)}\cdot\Delta t \tag{4.120}$$

When obtaining, W_{TOP}, one should be careful that it is composed of two states:

1. All cut sets are operating at time t.
2. A cut set fails in a time interval $[t, t+\Delta t]$.

Thus we write an expression for W_{TOP} as follows:

$$W_{TOP}=W_{AB}(1-F_C)(1-F_D)+W_{AC}(1-F_B)(1-F_D)$$
$$+W_D(1-F_AF_B)(1-F_AF_C)$$
$$-W_{ABC}(1-F_D) \tag{4.121}$$

The term $W_D(1-F_AF_B)(1-F_AF_C)$ of (4.121) becomes in simplified form

$$W_D(1-F_AF_B-F_AF_C-F_AF_BF_C)$$

The top event failure and repair rates, λ_{TOP} and μ_{TOP}, for Figure 4.22 may be obtained by substituting (4.121) and (4.118) into the following expressions:

$$\lambda_{TOP}=\frac{W_{TOP}}{\Delta t(1-F_{TOP})} \tag{4.122}$$

and

$$\mu_{TOP}=\frac{W_{TOP}}{(\Delta t)F_{TOP}} \tag{4.123}$$

4.13 ADVANTAGES AND DISADVANTAGES OF THE FAULT TREE TECHNIQUE

Like any other technique, the fault tree technique has its advantages and disadvantages:

Advantages.

1. It provides insight into the system behavior.
2. It requires the reliability analyst to understand the system thoroughly and deal specifically with one particular failure at a time.
3. It helps to ferret out failures deductively.
4. It provides a visibility tool to designers, users, and management to justify design changes and trade-off studies.
5. It provides options to perform quantitative or qualitative reliability analysis.
6. This technique can handle complex systems more easily.

Disadvantages.

1. This is a costly and time-consuming technique.
2. Its results are difficult to check.
3. This technique normally considers that the system components are in either working or failed state. Therefore, the partial failure states of components are difficult to handle.
4. Analytical solutions for fault trees containing stand-bys and repairable priority gates are difficult to obtain for the general case.
5. To include all types of common-cause failures it requires a considerable effort.

4.14 COMMON-CAUSE FAILURES

As the field of reliability engineering is becoming a recognized discipline in engineering so is the awareness of associated problems such as common-cause failures, which were overlooked some years ago. In recent years the common-cause failures have received widespread attention for reliability analysis of redundant components, units or systems, because the assumption of statistical-independent failure of redundant units is easily violated in practice [93]. It may easily be verified from reference 116. This paper reports frequency of common-cause failure in the U. S. power reactor industry: "Of 379 components failures or groups of failures arising from independent causes, 78 involved common-cause failures of two or more components."

A common-cause failure is defined in reference 105 as any instance where multiple units or components fail due to a single cause. Some of the common-cause failures may occur due to:

1. *Equipment design deficiency.* This includes those failures that may have been overlooked during the design phase of the equipment or system, and may be due to the interdependence between electrical and mechanical subsystems or components of a redundant system.
2. *Operations and maintenance errors.* These errors may occur due to improper adjustment or calibration, carelessness, improper maintenance, etc.
3. *External normal environment.* This includes causes such as dust, dirt, humidity, temperature, moisture, and vibration. These may be the normal extremes of the operating environment.
4. *External catastrophe.* This includes natural external phenomena such as flood, earthquake, fire, and tornado. The occurrence of any one of these events may affect the redundant system at a plant.

5. *Common manufacturer.* The redundant equipment or component procured from the same manufacturer may have the same design or fabrication errors. For example, the fabrication errors may occur due to use of wrong material, wiring a circuit board backward, poor soldering, etc.
6. *Common external power source.* A common-cause failure may occur due to the common external power source of the redundant equipment, subsystem, or unit.
7. *Functional deficiency.* This may occur due to inappropriate instrumentation or inadequacy of designed protective action.

There are several examples of common-cause failures in nuclear power systems [114]. Some spring loaded relays in a parallel configuration fail simultaneously due to a common cause. Furthermore, due to a maintenance error of incorrectly disengaging the clutches, two motorized valves are placed in a failed state. In addition, a steam line rupture causing multiple circuit board failures is another example. The common cause is the steam line rupture in this case. In some cases instead of triggering a complete redundant system failure (simultaneous failure), which is the extreme case, the common cause may produce a less severe but *common*, degradation of the redundant unit. This will increase the joint probability of failure of the system units. It may be due to harsh accident environment. In this degradation state, the redundant unit may fail at a time later than the first unit failure. Because of the common morose environment, the second unit failure is *dependent* and *coupled* to the first unit failure.

Although the existence of common-cause failures has been recognized for a long time, no concrete steps were taken to represent them systematically until the late 1960s. Most of the literature on the subject is presented in bibliography on common-cause failures [93].

Some of the newly established theory and models to analyze common-cause are presented in this section.

4.14.1 Common-Cause Failure Analysis of Reliability Networks

In this section we present a newly developed method [88, 101] to analyze active identical units with statistically independent and dependent (common-cause) failures. However, this method may be extended to other reliability models and probability densities. To develop this method, it was assumed that each unit has a certain amount of common-cause failures.

Since from past experience [101] it is known that the common-cause failures occur in real life, the parameter α is introduced into the newly developed formulas to include common-cause failures [88]. The parameter α can be obtained from the operating experience data of the redundant

system or equipment

$$\alpha \equiv \text{fraction of unit failures that are common cause}$$

The above parameter can be considered a point estimate of the conditional probability that a unit failure is common cause. A unit failure rate λ can be considered to have two mutually exclusive components, λ_1 and λ_2, that is,

$$\lambda = \lambda_1 + \lambda_2 \tag{4.124}$$

where λ_1 = the unit independent mode constant failure rate.
λ_2 = the redundant system or unit constant common-cause failure rate

Since

$$\alpha = \frac{\lambda_2}{\lambda} \tag{4.125}$$

$$\therefore \lambda_2 = \alpha\lambda \tag{4.126}$$

and λ_1 can be obtained from (4.124) by substituting (4.126)

$$\therefore \lambda_1 = (1-\alpha)\lambda \tag{4.127}$$

The system reliability, hazard rate, and MTTF formulas as well as the graphical plots are developed for a parallel, *k*-out-of-*n*, series, and a bridge network as discussed in the following sections.

A Parallel Network. The modified identical units parallel network is shown in Figure 4.24. It is simply a parallel network with a unit in series. The parallel stage (i.e., labeled "1") of Figure 4.24 represents all the independent failures for any n unit system. The series unit stage labeled "2" in Figure 4.24 represents all the common-cause failures of the system.

The common-cause failure probability hypothetical unit is connected in series with the independent failure mode units. A failure of the hypothetical series unit (i.e., the common-cause failure) will cause the system failure. It is assumed that all the common-cause failures are completely coupled. The system reliability R_p of the Figure 4.24 can be written as

$$R_p = \{1 - (1 - R_1)^n\} R_2 \tag{4.128}$$

where n = the number of identical units
R_1 = the unit's independent failure mode reliability
R_2 = the system common failure mode reliability

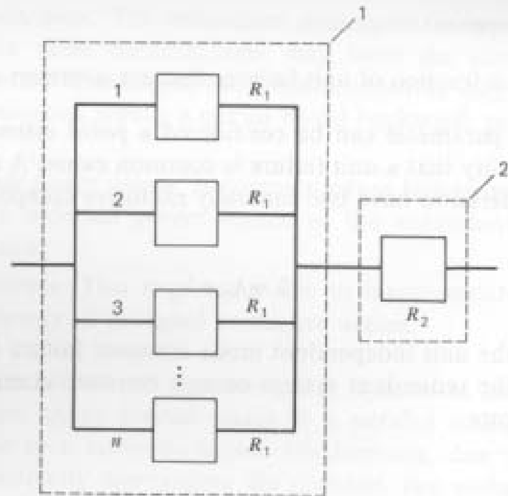


Figure 4.24 A modified identical units parallel network.

For constant failure rates λ_1 and λ_2 from (4.126) and (4.127) and for reliabilities R_1 and R_2, the (4.128) can be rewritten as

$$R_p(t) = \{1-(1-e^{-(1-\alpha)\lambda t})^n\}e^{-\alpha\lambda t} \tag{4.129}$$

where t is the time.

The reliability plots of (4.129) are shown for $n=2,3,4$, in Figures 4.25, 4.26, and 4.27, respectively. These plots clearly show the effect of common-

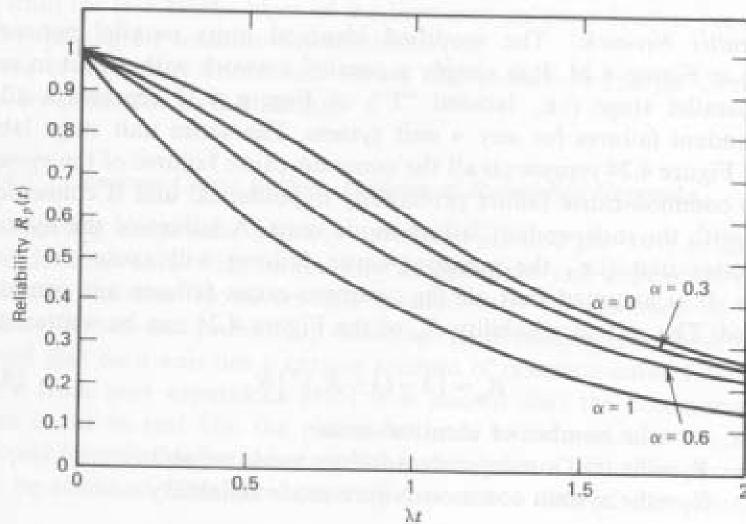


Figure 4.25 A two-parallel-units reliability plot.

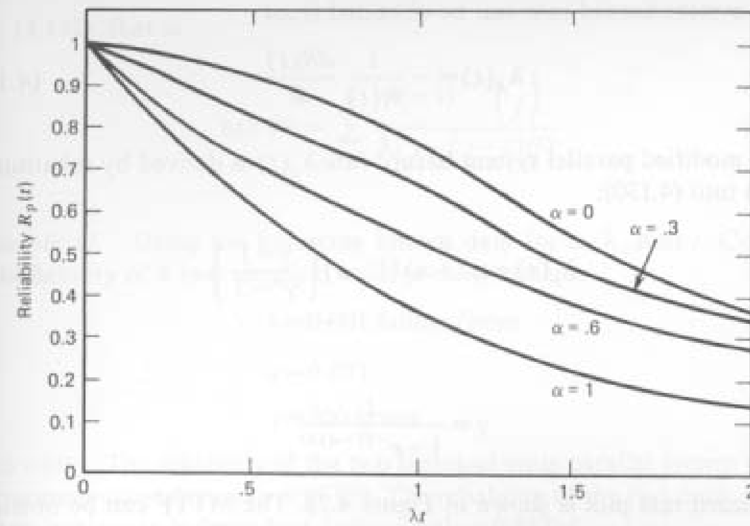


Figure 4.26 A three-parallel-units reliability plot.

cause failure on the parallel system. As the value of α increases, the reliability of the parallel system decreases.

The parameter α takes values from zero to one. At $\alpha=0$, the modified parallel network simply acts as an ordinary parallel network; however, at $\alpha=1$ the modified redundant parallel system just acts as a single unit. What it means is that all the system failures are common-cause failures.

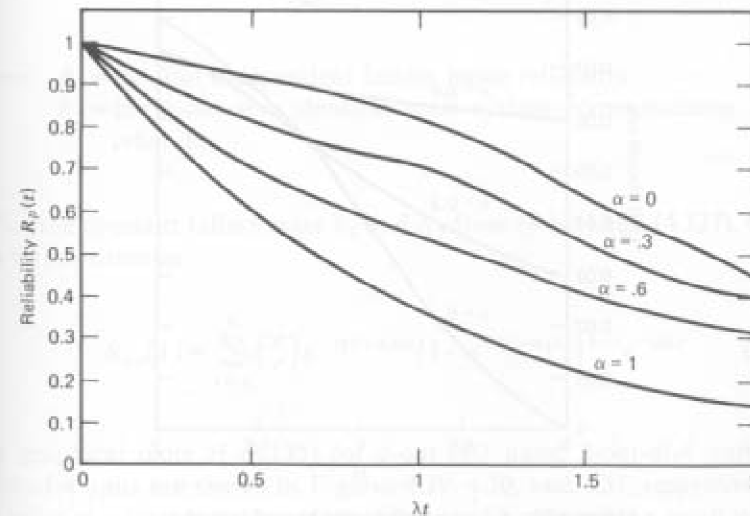


Figure 4.27 A four-parallel-units reliability plot.

The system hazard rate can be obtained from

$$\lambda_p(t) = -\frac{1}{R(t)}\frac{dR(t)}{dt} \tag{4.130}$$

The modified parallel system hazard rate $\lambda_p(t)$ is derived by substituting (4.129) into (4.130):

$$\lambda_p(t) = \alpha\lambda + n\lambda(1-\alpha)\left\{\frac{\gamma-1}{\gamma^n-1}\right\} \tag{4.131}$$

where

$$\gamma = \frac{1}{1-e^{-(1-\alpha)\lambda t}}$$

The hazard rate plot is shown in Figure 4.28. The MTTF can be obtained from

$$\text{MTTF} = \int_0^\infty R(t)\,dt \tag{4.132}$$

The modified parallel system MTTF is obtained by substituting (4.129)

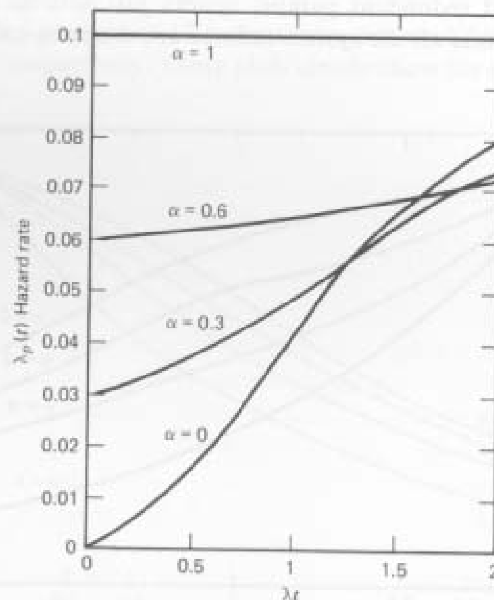


Figure 4.28 A four-parallel-units hazard rate plot.

into (4.132), that is,

$$\text{MTTF} = \sum_{j=1}^{n} \frac{(-1)^{j+1}\binom{n}{j}}{\lambda\{j-(j-1)\beta\}} \tag{4.133}$$

Example 11. Using the following known data for α, λ, and t. Compute the reliability of a two identical units parallel system:

$$\lambda = 0.001 \text{ failure/hour}$$

$$\alpha = 0.071$$

$$t = 200 \text{ hours}$$

SOLUTION. The reliability of the two identical units parallel system subject to common-cause failures = 0.95769. The reliability of the two units parallel system subject to independent failures only = 0.96714.

k-out-of-n System. The modified identical units k-out-of-n system has a hypothetical unit for the common-cause failure connected in series with the independent failure mode k-out-of-n units. The series-connected hypothetical unit represents the system or unit common-cause failures. A failure associated with this hypothetical unit will cause the overall system failure. The modified k-out-of-n identical units system reliability, R_{kn}, can be obtained from

$$R_{kn} = \left\{\sum_{r=k}^{n}\binom{n}{r}R_1^r(1-R_1)^{n-r}\right\}R_2 \tag{4.134}$$

where R_1 = the unit independent failure mode reliability
R_2 = the k-out-of-n identical units system common-cause failure reliability

For the constant failure rates λ_1 and λ_2 from (4.126) and (4.127), (4.134) can be rewritten as

$$R_{kn}(t) = \sum_{r=k}^{n}\binom{n}{r}e^{-r(1-\alpha)\lambda t}\{1-e^{-(1-\alpha)\lambda t}\}^{n-r}e^{-\alpha\lambda t} \tag{4.135}$$

The graphical plots of (4.135) for 2-out-of-3 units, 2-out-of-4 units, and 3-out-of-4 units are shown in Figures 4.29, 4.30, and 4.31, respectively. As the value of α increases, the system reliability decreases for a small value of λt, as can be verified from Figures 4.29, 4.30, and 4.31.

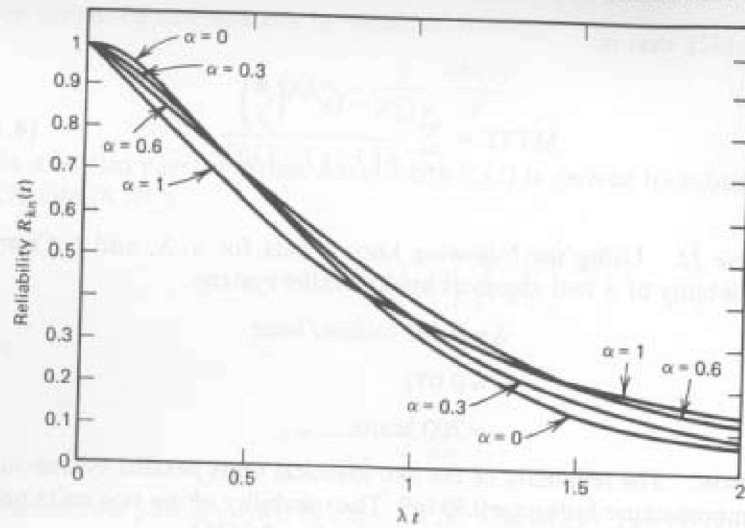


Figure 4.29 A 2-out-of-n units reliability plot.

The k-out-of-n system hazard rate $\lambda_{kn}(t)$ and MTTF can be obtained by substituting (4.135) into (4.130) and (4.132), respectively, that is,

$$\lambda_{kn}(t) = -\frac{\left\{ \sum_{r=k}^{n} \binom{n}{r} [(r\alpha - r - \alpha)\lambda]\theta[\eta^{(n-r)}] + \theta\lambda(n-r)(1-\alpha)\eta^{(n-r-1)}(1-\eta) \right\}}{\sum_{r=k}^{n} \binom{n}{r} \theta\eta^{(n-r)}} \tag{4.136}$$

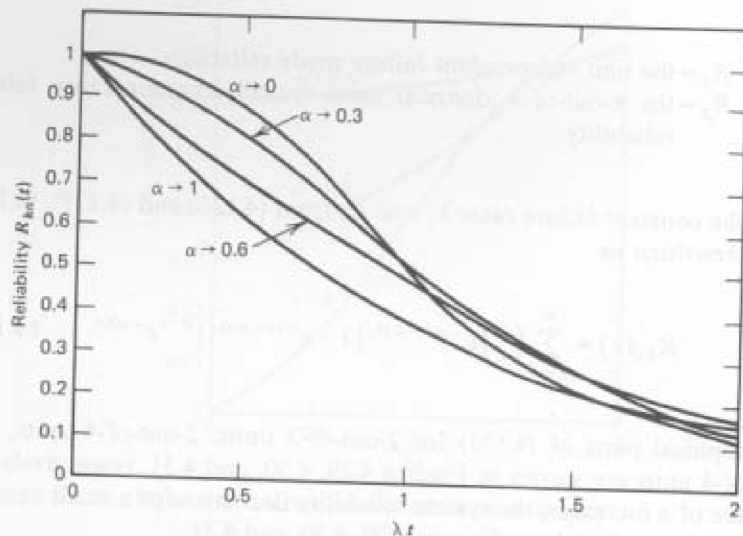


Figure 4.30 A 2-out-of-4 units reliability plot.

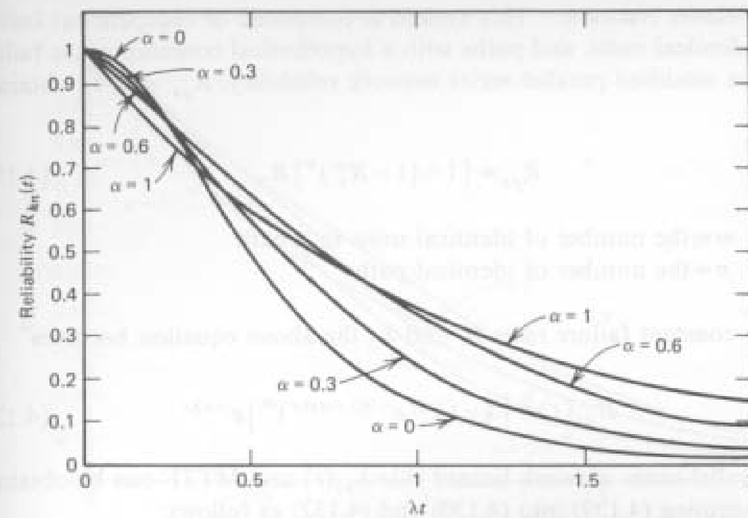


Figure 4.31 A 3-out-of-4 units reliability plot.

where

$$\eta = \{1 - e^{-(1-\beta)\lambda t}\}$$

$$\theta = e^{(r\alpha - r - \alpha)\lambda t}$$

and

$$\mathrm{MTTF} = \sum_{r=k}^{n} \binom{n}{r} \left[\frac{1}{r - r\alpha + \alpha} - \frac{(n-r)}{(r - r\alpha + 1)\lambda} + \frac{(n-r)(n-r-1)}{2!(r - r\alpha - \alpha + 2)\lambda} - \frac{(n-r)(n-r-1)(n-r-2)}{3!} \frac{1}{(r + 3 - r\alpha - 2\alpha)\lambda} + \cdots \right] \tag{4.137}$$

Example 12. For the following given hypothetical values of λ, t, and α calculate the system reliability of a 2-out-of-3 units system:

$$\lambda = 0.0005 \text{ failure/hour}$$

$$\alpha = 0.3$$

$$t = 200 \text{ hours}$$

From (4.135) the reliability of a system with common-cause failures was in the order of 0.95772 as compared with the system reliability, 0.97455, with no common cause failures.

Parallel-Series Network. This system is composed of independent failure mode, identical units, and paths with a hypothetical common-cause failure unit. The modified parallel-series network reliability, R_{ps}, can be obtained from

$$R_{ps}=\{1-(1-R_1^m)^n\}R_2 \tag{4.138}$$

where m = the number of identical units in a path
n = the number of identical paths

For the constant failure rates λ_1 and λ_2 the above equation becomes

$$R_{ps}(t)=\left[1-(1-e^{-n(1-\alpha)\lambda t})^m\right]e^{-\alpha\lambda t} \tag{4.139}$$

The parallel-series network hazard rate $\lambda_{ps}(t)$ and MTTF can be obtained by substituting (4.139) into (4.130) and (4.132) as follows:

$$\lambda_{ps}(t)=\alpha\lambda+mn(1-\alpha)\lambda\frac{(\gamma-1)}{(\gamma^m-1)} \tag{4.140}$$

where $\lambda=1/[1-e^{-n(1-\gamma)\lambda t}]$ and

$$\text{MTTF}=\frac{\sum_{j=1}^{n}\binom{m}{j}(-1)^{j+1}}{\{\lambda\alpha+n\lambda(j-\alpha j)\}} \tag{4.141}$$

A Bridge Network. This system is composed of an independent failure mode identical units bridge network in series with a hypothetical common-cause failure unit for the bridge structure. If the hypothetical common-cause failure unit fails, the overall system fails. The modified bridge network reliability [127] can be obtained from

$$R_b=\{1-2(1-R_1)^5+5(1-R_1)^4-2(1-R_1)^3-2(1-R_1)^2\}R_2 \tag{4.142}$$

where R_b is the reliability of the bridge network subject to common-cause failures.

For the constant failure rates λ_1 and λ_2 from (4.126) and (4.127), (4.142) can be rewritten as

$$R_b(t)=\left[1-2(1-e^{-At})^5+5(1-e^{-At})^4-2(1-e^{-At})^3 -2(1-e^{At})^2\right]e^{-\beta\lambda t} \tag{4.143}$$

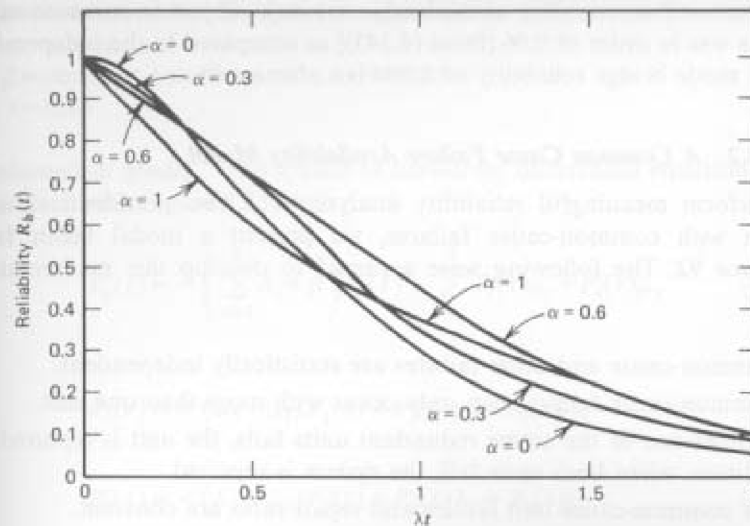


Figure 4.32 A bridge network reliability plot.

where $A=(1-\alpha)\lambda$. The reliability plots of (4.143) are shown in Figure 4.32 for the varying values of parameter α. For the small value of λt, the bridge network reliability decreases as the value of parameter α increases.

The bridge network hazard rate, $\lambda_b(t)$ and the MTTF can be obtained by substituting (4.143) into (4.130) and (4.132), respectively:

$$\lambda_b(t)=\beta\lambda+A(-8\pi^5+25\pi^4-24\pi^3+4\pi^2+4\pi) + \frac{-2\pi^5+5\pi^4-2\pi^3-2\pi^2}{1-2\pi^5+5\pi^4-2\pi^3-2\pi^2} \tag{4.144}$$

where $\pi=(1-e^{-At})$ and

$$\text{MTTF}=\frac{2}{(2-\alpha)\lambda}+\frac{2}{(3-2\alpha)\lambda}+\frac{5}{(4-3\alpha)\lambda}+\frac{2}{(5-4\alpha)\lambda} \tag{4.145}$$

Example 13. Suppose an identical units bridge network has the following known values for its parameter λ and α. Calculate the bridge reliability for 200 hours, that is,

$$\lambda=0.0005 \text{ failure/hour}$$

$$\alpha=0.3$$

$$t=200 \text{ hours}$$

SOLUTION. The reliability of the bridge network subject to common-cause failures was in order of 0.96 [from (4.143)] as compared to the independent failure mode bridge reliability of 0.984 (i.e., for $\alpha=0$).

4.14.2 A Common Cause Failure Availability Model

To perform meaningful reliability analysis of a two nonidentical units system with common-cause failures, we present a model taken from reference 92. The following were assumed to develop this mathematical model:

1. Common-cause and other failures are statistically independent.
2. Common-cause failures can only occur with more than one unit.
3. If either one of the active redundant units fails, the unit is repaired. In addition, when both units fail, the system is repaired.
4. The common-cause unit failure and repair rates are constant.

When both units are failed, repair is dependent on the following three cases:

Case 1. The failed component replacements, repair facilities, and skilled craftsmen are available to repair both units.

Case 2. The failed component replacements, repair facilities, and skilled craftsmen are available to repair one unit only.

Case 3. Neither (2) or (3) is applicable due to nonavailability of the failed components replacements, tools, or skilled craftsmen. Furthermore, it may be queuing at a repair facility.

In Case 1 both units can be repaired simultaneously; however, in Case 2 only one unit can be repaired at a time. For the last and final case (3) the units can only be repaired at the availability of the craftsmen replacements for failed components.

The following notations and abbreviations were used to formulate this availability model:

$P_0(t)$ = probability at time t, both units are operational
$P_1(t)$ = probability at time t, the unit 1 has failed and unit 2 is operational
$P_2(t)$ = probability at time t, the unit 2 has failed and unit 1 is operational
$P_3(t)$ = probability at time t, the units 1 and 2 have failed
$P_4(t)$ = probability at time t, the failed component replacements and repairmen are available to repair both units
λ_i = constant failure rate of units 1 and 2, respectively, for $i=1,2$
μ_i = constant repair rate of units 1 and 2, respectively, for $i=1,2$
μ_3 = constant repair rate of units 1 and 2

α = constant rate of repairmen availability and components replacements
β = constant common-cause failure rate
t = time

Mathematical Model. The system of first-order differential equations [129] associated with Figure 4.33 are

$$P_0'(t)=-\left(\sum_{i=1}^{2}\lambda_i+\beta\right)P_0(t)+\sum_{i=1}^{3}P_i(t)\mu_i+P_4(t)\mu_3 \tag{4.146}$$

$$P_1'(t)=-(\lambda_2+\mu_1)P_1(t)+P_3(t)\mu_2+P_0(t)\lambda_1 \tag{4.147}$$

$$P_2'(t)=-(\lambda_1+\mu_2)P_2(t)+P_0(t)\lambda_2+P_3(t)\mu_1 \tag{4.148}$$

$$P_3'(t)=-\left(\sum_{i=1}^{3}\mu_i+\alpha\right)P_3(t)+\sum_{i=1}^{2}P_i(t)\lambda_{(3-i)}+P_0(t)\beta \tag{4.149}$$

$$P_4'(t)=-\mu_3P_4(t)+P_3(t)\alpha \tag{4.150}$$

At $P_0(0)=1$ other initial condition probabilities are equal to zero, where the prime represents differentiation with respect to time t.

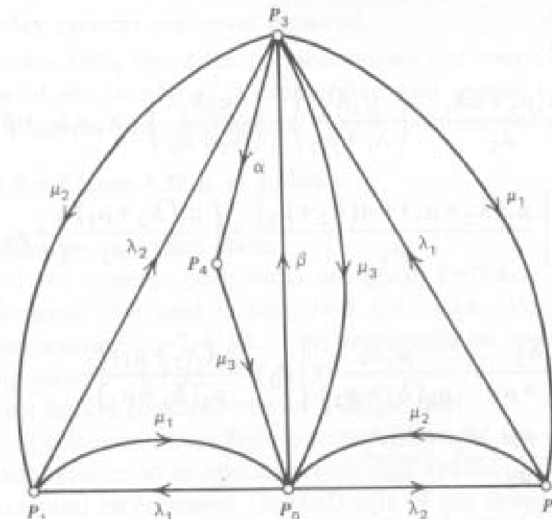


Figure 4.33 A common-cause failure availability model.

The following steady-state equations obtained from (4.146)–(4.150) by setting the derivatives with respect to time t equal to zero:

$$-\left(\sum_{i=1}^{2}\lambda_i+\beta\right)P_0+\sum_{i=1}^{3}P_i\mu_i+P_4\mu_3=0 \tag{4.151}$$

$$-(\lambda_2+\mu_1)P_1+P_3\mu_2+P_0\lambda_1=0 \tag{4.152}$$

$$-(\lambda_1+\mu_2)P_2+P_0\lambda_2+P_3\mu_1=0 \tag{4.153}$$

$$-\left(\sum_{i=1}^{3}\mu_i+\alpha\right)P_3+\sum_{i=1}^{2}P_i\lambda_{(3-i)}+P_0\beta=0 \tag{4.154}$$

$$-\mu_3P_4+P_3\alpha=0 \tag{4.155}$$

$$\sum_{i=0}^{4}P_i-1=0 \tag{4.156}$$

Solving the above system of simultaneous equations yields

$$P_0=\left[\theta\left\{1+\frac{\mu_1(\lambda_2+\mu_1)}{\mu_2(\lambda_1+\lambda_1+\mu_2)}+\frac{\lambda_2+\mu_1}{\mu_2}+\frac{\alpha(\lambda_2+\mu_1)}{\mu_2\mu_3}\right\}+\frac{\lambda_2}{\lambda_1+\mu_2}-\frac{\mu_1\lambda_1}{(\lambda_1+\mu_2)\mu_2}-\frac{\lambda_1}{\mu_2}-\frac{\alpha\lambda_1}{\mu_2\mu_3}+1\right]^{-1} \tag{4.157}$$

where

$$\theta=\frac{P_1}{P_0}$$

$$(P_1/P_0)=\left[\frac{\lambda_1\mu_3+\alpha\lambda_1}{\mu_2}-\left(\frac{\mu_2\lambda_2}{\lambda_1+\mu_2}\right)+\left(\frac{\mu_1\lambda_1}{\lambda_1+\mu_2}\right)+\lambda_1+\lambda_2+\beta\right]\times\left[\frac{\mu_3(\lambda_2+\mu_1)+\alpha(\lambda_2+\mu_1)}{\mu_2}+\left(\frac{\mu_1(\lambda_2+\mu_1)}{\lambda_1+\mu_2}\right)+\mu_1\right]^{-1} \tag{4.158}$$

$$P_1=\theta P_0 \tag{4.159}$$

$$P_2=\left[\frac{\lambda_2}{\lambda_1+\mu_2}-\frac{\mu_1\lambda_1}{\mu_2(\lambda_1+\mu_2)}\right]P_0+\frac{\mu_1(\lambda_2+\mu_1)P_1}{\mu_2(\lambda_1+\mu_2)} \tag{4.160}$$

$$P_3=\frac{(\lambda_2+\mu_1)P_1}{\mu_2}-\frac{\lambda_1P_0}{\mu_2} \tag{4.161}$$

$$P_4=\frac{\alpha P_1(\lambda_2+\mu_1)}{\mu_2\mu_3}-\frac{\alpha\lambda_1}{\mu_2\mu_3}P_0 \tag{4.162}$$

The steady-state system availability can be obtained from

$$\text{system availability}=\sum_{i=0}^{2}P_i \tag{4.163}$$

4.14.3 A 1-Out-Of-N: G System With Duplex Elements

This model incorporates stand-by duplex unit replacements and common-cause failures [91]. When the operational duplex system (contains two statistically identical units) fails, it is replaced by one of the $(N-1)$ standby duplex systems. Furthermore, this model incorporates a possibility (i.e., to replace the failed system) that the repairmen or special repair tools may be available or, alternatively, not available at the time of the operational system failure. This type of situation occurs at a nuclear plant where a duplex system is replaced only when both units fail.

The following were assumed to develop this model:

1. A duplex system has two statistically identical units. All but one of the duplex systems are cold standbys (units cannot fail).
2. Common-cause and other failures are statistically independent.
3. Operational system is replaced only when both units fail.
4. Operational units are independently identically distributed (i.i.d.), except for common-cause failures.
5. A failed system is restored as good as new.
6. Cold standby systems; standby units cannot fail.
7. Failed duplex systems are never repaired.
8. When a system fails, two different possibilities are considered to replace it with one of the standbys: (a) repairmen and special repair tools are available; (b) repairmen and special repair tools are not available.

The notation for Figure 4.34 is as follows:

n = total number of system states
i = state of the system: both units are good, $i=0,4,8,\ldots,(n-2)$; one unit is good, one unit is bad, $i=1,5,9,\ldots,(n-1)$; both units are bad, no waiting, $i=2,6,10,\ldots,n$; repairmen or special repair tool waiting state, $i=3,7,11,\ldots,(n-3)$
λ = constant failure (hazard) rate of a single unit
β = constant common-cause failure (hazard) rate of the duplex system
α = constant repairmen or special repair tool availability (hazard) rate
μ_j = constant and replacement (hazard) rate of the failed duplex system when repairmen and special repair tools are available (for $j=1$); or not available (for $j=2$)

[library stamp in margin, illegible]

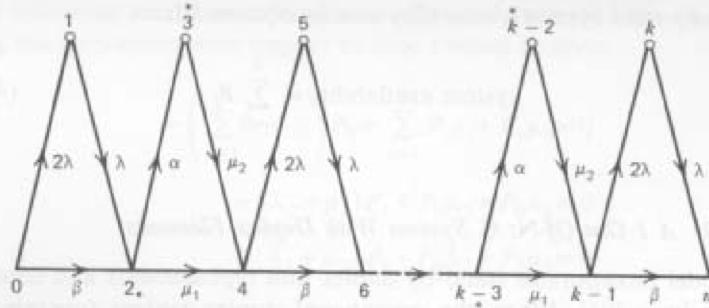


Figure 4.34 Transition diagram of system. The star denotes down states.

The equations for the Figure 4.34 model [129] are:

$$P_0'(t) = -(2\lambda+\beta)P_0(t) \tag{4.164}$$

$$P_k'(t) = P_{k-1}(t)2\lambda - P_k(t)\lambda \tag{4.165}$$

$$P_{k-3}'(t) = P_{k-5}(t)\beta + \lambda P_{k-4}(t) - (\mu_1+\alpha)P_{k-3}(t) \tag{4.166}$$

$$P_{k-2}'(t) = P_{k-3}(t)\alpha - \mu_2 P_{k-2}(t) \tag{4.167}$$

$$P_{k-1}'(t) = P_{k-3}(t)\mu_1 + \mu_2 P_{k-2}(t) - (2\lambda+\beta)P_{k-1}(t) \tag{4.168}$$

$$\vdots$$

$$P_n'(t) = P_k(t)\lambda + P_{k-1}(t)\beta \tag{4.169}$$

The above equations are valid for $k = 5, 9, 13, \ldots, (n-1)$.

$$P_i(t) = 1 \quad \text{for } i = 0$$
$$= 0 \quad \text{for all other } i$$

The prime denotes differentiation with respect to time t.

$$n \equiv (4N-2) \quad \text{for } N \geqslant 2 \tag{4.170}$$

The Laplace transforms of the end result are

$$P_0(s) = \frac{1}{s+2\lambda+\beta} \tag{4.171}$$

$$P_k(s) = \frac{P_{k-1}(s)2\lambda}{s+\lambda} \tag{4.172}$$

$$P_{k-2}(s) = \frac{P_{k-3}(s)\alpha}{s+\mu_2} \tag{4.173}$$

$$P_{k-3}(s) = \frac{P_{k-5}(s)\beta + P_{k-4}(s)\lambda}{s+\mu_1+\alpha} \tag{4.174}$$

$$P_{k-1}(s) = \frac{P_{k-3}(s)\mu_1 + P_{k-2}(s)\mu_2}{s+2\lambda+\beta} \tag{4.175}$$

$$\vdots$$

$$P_n(s) = \frac{P_k(s)\lambda + P_{k-1}(s)\beta}{s} \tag{4.176}$$

To obtain the time domain solution, one should transform (4.171)–(4.176) for the known value of N.

4.14.4 A 4-Unit Redundant System with Common-Cause Failures

This mathematical model represents a 4-identical-unit system with common-cause failures [87] where system repair times are arbitrarily distributed. Therefore, the supplementary variable technique [123, 125, 126] is used to develop equations for the model.

The following were assumed to develop this mathematical model:

1. Common-cause and other failures are statistically-independent.
2. Common-cause failures can only occur with more than one unit.
3. Units are repaired only when the system fails. A failed system is restored to like-new.
4. System repair times are arbitrarily distributed.

The transition diagram is shown in Figure 4.35.

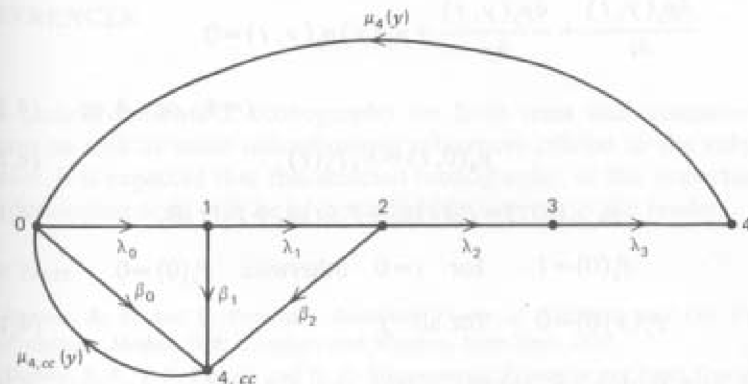


Figure 4.35 Transition diagram of system.

The following notation was used to develop model equations

i = state of the unfailed system: number of failed units, $i=0,1,2,3$

j = state of the failed system, $j=4$ means failure not due to a common cause; $j=4$, cc means failure due to a common-cause

$P_i(t)$ = probability that system is in unfailed state i, at time t

$p_j(y,t)$ = probability density (with respect to repair time) that the failed system is in state j and has an elapsed repair time of y

$\mu_j(y)$, $q_j(y)$ = repair rate (a hazard rate) and pdf of repair time when system is in state j and has an elapsed repair time of y

β_i = constant common-cause failure rate of the system when in state i; $\beta_3=0$

λ_i = constant failure rate of a unit, for other than common-cause failures, when the system is in state i; $i=0,1,2,3$

s = Laplace transform variable

The equations for the model are

$$\frac{dP_0(t)}{dt}+(\lambda_0+\beta_0)P_0(t) = \int_0^\infty p_4(y,t)\mu_4(y)\,dy+\int_0^\infty p_{4,cc}(y,t)\mu_{4,cc}(y)\,dy \tag{4.177}$$

$$\frac{dP_i(t)}{dt}+(\lambda_i+\beta_i)P_i(t)-\lambda_{i-1}P_{i-1}(t)=0 \qquad i=1,2,3 \qquad \beta_3=0 \tag{4.178}$$

$$\frac{\partial p_j(y,t)}{\partial t}+\frac{\partial p_j(y,t)}{\partial y}+\mu_j(y)p_j(y,t)=0 \qquad j=4 \text{ or } 4,\text{cc} \tag{4.179}$$

$$p_4(0,t)=\lambda_3P_3(t) \tag{4.180}$$

$$p_{4,cc}(0,t)=P_0(t)\beta_0+P_1(t)\beta_1+P_2(t)\beta_2 \tag{4.181}$$

$$P_i(0)=1 \quad \text{for } i=0 \quad \text{otherwise } P_i(0)=0$$

$$p_j(y,0)=0 \quad \text{for all } j \tag{4.182}$$

Solving and setting up, similar to the above equations are presented in reference 125.

The Laplace transforms of the solution are

$$P_0(s)=\left[s+\lambda_0+\beta_0-\left(\beta_0+\frac{\beta_1}{A_1}+\frac{\beta_2}{A_2}\right)G_{4,cc}(s)-\frac{G_4(s)}{A_3}\right]^{-1} \tag{4.183}$$

$$G_j(s)\equiv\int_0^\infty \exp(-sy)q_j(y)\,dy \qquad \text{for } j=4 \text{ or } 4,\text{cc}$$

$$A_1\equiv\frac{s+\lambda_1+\beta_1}{\lambda_0}$$

$$A_2\equiv\frac{A_1(s+\lambda_2+\beta_2)}{\lambda_1}$$

$$A_3\equiv\frac{A_2(s+\lambda_3)}{\lambda_2}$$

$$P_i(s)=\frac{P_0(s)}{A_i} \qquad \text{for } i=1,2,3 \tag{4.184}$$

$$P_4(s)=\frac{\lambda_3P_3(s)[1-G_4(s)]}{s} \tag{4.185}$$

$$P_{4,cc}(s)=\left[\sum_{i=0}^{2}\beta_iP_i(s)\right]\frac{1-G_{4,cc}(s)}{s} \tag{4.186}$$

To obtain time domain solution of the above equations, one should substitute the Laplace transform of the repair times density functions for $G_4(s)$ and $G_{4,cc}(s)$ and then take inverse Laplace transforms of (4.183)–(4.186).

REFERENCES

This section presents a bibliography on fault trees and common-cause failures as well as some miscellaneous references related to the subject of interest. It is expected that this selected bibliography, in this important and fast developing area, will be of considerable interest to the readers.

Fault Trees

1. Barlow, R. E. and F. Proschan, *Statistical Theory of Reliability and Life Testing—Probability Models*, Holt, Rinehart and Winston, New York, 1975.
2. Barlow, R. E., J. B. Fussell, and N. D. Singpurwalla, *Reliability and Fault Tree Analysis*. SIAM, Philadelphia, 1975.

3. Green, A. E. and A. J. Bourne, *Reliability Technology*. Wiley-Interscience, London, 1972.
4. Aggarwal, K. K., "Comments on 'On the Analysis of Fault Trees,'" *IEEE Trans. Reliab.*, **R-25**, 126–127 (1976).
5. Apostolakis, G. and Y. T. Lee, "Methods for the Estimation of Confidence Bounds for the Top-Event Unavailability of Fault Trees," *Nucl. Eng. Design*, **41**, 411–419 (1977).
6. Barlow, R. E. and H. E. Lambert, "Introduction to Fault Trees Analysis." In: *Reliability and Fault Tree Analysis*, SIAM, Philadelphia, 1975, pp. 7–37.
7. Bass, L., H. W. Wynholds, and W. R. Poterfield, "Fault Tree Graphics," *Proceedings of the Annual Reliability Maintainability Symposium*, IEEE, New York, 1975, pp. 292–297.
8. Bazovsky, I., "Fault Trees, Block Diagrams and Markov Graphs," *Proceedings of the Annual Reliability Maintainability Symposium*, IEEE, New York, 1977, pp. 134–141.
9. Bengiamin, N. N., B. A. Brown, and K. F. Schenk, "An Efficient Algorithm for Reducing the Complexity of Computation in Fault Tree Analysis," *IEEE Trans. Nucl. Sci.* NS-23, pp. 1442–1446 (1976).
10. Bennetts, R. G., "On the Analysis of Fault Trees," *IEEE Trans. Reliab.* **R-24** (3), 175–185 (1975).
11. Browning, R. L., "Analyzing Industrial Risks," *Chem. Eng.*, **76**, 109–114 (Oct. 1969).
12. Burdick, G. R., "COMCAN—A Computer Code for Common-Cause Analysis," *IEEE Trans. Reliab.*, **R-26**, 100–102 (1977).
13. Carnino, A., "Safety Analysis Using Fault Trees," *NATO Advanced Study Institute on Generic Techniques of System Reliability Assessment*, Nordhoff, Leiden, Netherlands, 1974.
14. Chatterjee, P., "A Method to Reduce the Cost of Analysis," In: *Reliability and Fault Tree Analysis*, SIAM, Philadelphia, 1975, pp. 101–129.
15. Crosetti, P. A., "Fault Tree Analysis with Probability Evaluation," *IEEE Trans. Nucl. Sco.*, **18**, 465–471 (1971).
16. Crosetti, P. A. and R. A. Bruce, "Commercial Application of Fault Tree Analysis," *Proceedings of the Annual Reliability Maintainability Symposium*, IEEE, New York, 1970.
17. Cummings, G. E., "Application of the Fault Tree Technique to a Nuclear Reactor Containment System," In: *Reliability and Fault Tree Analysis*, SIAM, Philadelphia, 1975.
18. Danzeisen, R. N., J. A. Mateyka, and D. W. Weiss, "A Reliability and Safety Analysis of Automotive Vehicles," *Proceedings of the Symposium on Reliability*, 1971, p. 150–151. IEEE, New York.
19. Dhillon, B. S. " A Modification of Fault Tree AND Gate," *Microelectron. Reliab.*, **15**, 625–626 (1976).
20. Dhillon, B. S. and C. Singh, "On Fault Trees and Other Reliability Evaluation Methods," *Microelectron. Reliab.*, **19** (1/2), 57–64 (1979).
21. Dhillon, B. S. and C. Singh, "Bibliography of Literature on Fault Trees," *Microelectron. Reliab.*, **17**, 501–503 (1978).
22. Dhillon, B. S., C. L. Proctor, and A. Kothari, On repairable component fault tree, *Proceedings of the Annual Reliability and Maintainability Symposium*, (1979). IEEE, New York.
23. Eagle, K. H., "Fault Tree and Reliability Analysis Comparison," *Proceedings of the Symposium on Reliability*, (1969). IEEE, New York.
24. Evans, R. A., "Fault-Trees and Cause-Consequence Charts," *IEEE Trans. Reliab.*, **23**, 1 (1974).
25. Fleming, K. N., G. W. Hannaman, "Common Cause Failure Considerations in Predicting HTGR Cooling System Reliability," *IEEE Trans. Reliab.*, **R-25**, 171–177 (1976).
26. Fussell, J. B., "Fault Tree Analysis—Concepts and Techniques," *Proceedings of the NATO Advanced Study Institute on Generic Techniques of System Reliability Assessment*, Nordhoff, Leiden, Netherlands, 1975

27. Fussell, J. B., "Fault Tree Analysis—Concepts and Techniques," *Proceedings of the NATO Advanced Study Institute on Generic Techniques of System Reliability Assessment*, Nordhoff, Leiden, Netherlands, 1975.
28. Fussell, J. B., "Computer Aided Fault Tree Construction for Electrical System." In: *Reliability and Fault Tree Analysis*, SIAM, Philadelphia, 1975.
29. Fussell, J. B., "A Formal Methodology for Fault Tree Construction," *Nucl. Sci. Engng*, **52**, 421–432 (1973).
30. Fussell, J. B., "How to Hand-Calculate System Reliability Characteristics," *IEEE Trans. Reliab.*, **R-24**, 169–174 (1975).
31. Fussell, J. B., E. F. Aber, and R. G. Rahl, "On the Quantitative Analysis of Property—AND Failure Logic," *IEEE Trans. Reliab.*, **R-26**, 324–326 (1977).
32. Fussell, J. B., G. J. Powers, and R. G. Bennetts, "Fault Trees—A State of the Art Discussion," *IEEE Trans. Reliab.*, **R-23**, 51–55 (1974).
33. Fussell, J. B. and W. E. Vesely, "A New Methodology for Obtaining Cut Sets for Fault-Trees," *Trans. Am. Nucl. Soc.*, **15**, 262–263 (1972).
34. Garribba, S., "Efficient Construction of Minimal Cut Set from Fault Trees," *IEEE Trans. Reliab.*, **R-26**, 88–94 (1977).
35. Garrick, B. J., "Principles of Unified Systems Safety Analysis," *Nucl. Eng. Design*, **13**, 245–321 (1970).
36. Gopal, K. and J. S. Gupta, "On the Analysis of Fault Trees—Some Comments," *IEEE Trans. Reliab.*, **R-26**, 14–15 (April 1977).
37. Haasl, D. F., "Advanced Concepts in Fault Tree Analysis," *System Safety Symposium*, (1965). (Available from the University of Washington Library, Seattle.)
38. Hannum, W. H., F. X. Gavigan, D. E. Emon, "Reliability and Safety Analysis Methodology in the Nuclear Programs of ERDA," *IEEE Trans. Reliab.*, **R-25**, 140–146 (1976).
39. Henley, E. J., "Systems Analysis by Sequential Fault Trees," *Microelectronics and Reliab.*, **15**, 247–248 (1976).
40. Henser, F. W., "Reliability Analysis of Reactor Systems," *Proceedings of the Annual Symposium on Reliability*, 1970, pp. 135–145. IEEE, New York.
41. Hiltz, P. A., "The Fundamentals of Fault-Tree Analysis," Government-Industry Data Exchange Program (GIDEP), Report No. 347.40.00.00-F1-38 (C2300). Available from the GIDEP Operations Center, Corona, CA 91720, 1965.
42. Human, C. L., "The Graphical FMECA", *Proceedings of the Annual Reliability and Maintainability Symposium*, IEEE, New York, 1975, pp. 298–303.
43. Lambert, H. E., "Measures of Importance of Events and Cut Sets in Fault Trees," In: *Reliability and Fault Tree Analysis*, SIAM, Philadelphia, 1975, pp. 77–101.
44. Lambert, H. E. and G. Yadigaroglu, "Fault Trees for Diagnosis of System Fault Conditions," *Nucl. Sci. Eng.*, **62**, 20–34 (1977).
45. Lapp, S. A. and G. J. Powers, "Computer-Aided Synthesis of Fault Trees," *IEEE Trans. Reliab.*, **R-26**, 2–13 (1977).
46. Levine, S. and W. E. Vesely, "Important Event-Tree and Fault-Tree Considerations in the Reactor Safety Study," *IEEE Trans. Reliab.*, **R-25**, 132–139 (1976).
47. Michels, J. M., "Computer Evaluation of the Safety Fault Tree Model," System Safety Symposium, (1965). (Available from the University of Washington Library, Seattle.)
48. Murchland, J. D., "Comments on 'A Time Dependent Methodology for Fault Tree Evaluation,'" *Nucl. Eng. Design*, **22**, 167–172 (1972).
49. Nagel, P. M., "A Monte Carlo Method to Compute Fault Tree Probabilities," *System Safety Symposium*, (1965). (Available from University of Washington Library, Seattle.) 1965.
50. Neilsen, D. S., O. Platz, and B. Runge, "A Cause Consequence Chart of a Redundant Protection System," *IEEE Trans. Reliab.*, **R-24**, (April 1975). pp 8–13.

51. Neogy, R., "Fault Trees in Ocean Systems," *Proceedings of the American Reliability and Maintainability Symposium*, IEEE, New York, 1975, pp. 280–285.
52. Neuman, C. P. and N. M. Bonhomme, "Evaluation of Maintenance Policies using Markov Chains and Fault Tree Analysis," *IEEE Trans. Reliab.*, **24**, (1975). pp 37–44.
53. Nieuwhof, G. W. E., "An Introduction to Fault Tree Analysis with Emphasis on Failure Rate Evaluation," *Microelectron. Reliab.*, **14**, 105–119 (1975).
54. Nieuwhof, G. W. E., "Unavailability Logic Tree Analysis," *Third Annual Reliability and Energy Conference on Power Apparatus, Montreal*, IEEE, New York, 1976, pp. 79–83.
55. Phibbs, E. and S. H. Kuwamoto, "An Efficient Map Method for Processing Multistate Logic Trees," *IEEE Trans. Reliab.*, **R-21**, (1972). pp. 93–98.
56. Powers, G. J. and F. C. Tompkins, "Fault Tree Synthesis for Chemical Processes," *Amer. Inst. Chem. Eng. J.*, **20**, 376–387 (1974).
57. Powers, G. J., F. C. Tompkins, and S. A. Lapp, "A Safety Simulation Language for Chemical Processes: A Procedure for Fault Tree Synthesis," In: *Reliability and Fault Tree Analysis*, SIAM, Philadelphia, 1975.
58. Roush, S. L. and F. J. Schilagi, "Fault Tree Approach to Organization Design," *Proceedings of the Annual Reliability Maintainability Symposium*, IEEE, New York, 1971.
59. Rubel, P., "BONSAI: Cultivating th Logic Tree for Reactor Safety," *Proceedings of the Annual Reliability and Maintainability Symposium*, (Available from the IEEE). 1975.
60. Rubel, P., "Tiger in the Fault Tree Jungle," *Proceedings of the Seventh Annual Modelling Simulation Conference*, Pittsburgh, Instrument Society of America, 1975, pp. 1071–1086. 400 Stanwix St., Pittsburgh, Pennsylvania 15222, USA.
61. Reactor Safety Study, WASH-1400 (NUREG-75) National Technical Information Service, Springfield, VA, 22161, (October 1976).
62. Salvatori, R., "Systematic Approach to Safety Design and Evaluation," *IEEE Trans. Nucl. Sci.*, **18**, (February 1971).
63. Sarver, S. J., "Reliability Evaluation of a Containment for Cooler System," *Proceedings of the Annual Reliability and Maintainability Symposium*, IEEE, New York, 1975, pp. 154–162.
64. Schneeweiss, W. G., "Calculating the Probability of Boolean Expression Being 1," *IEEE Trans. Reliab.*, **26**, (1977).
65. Schroder, R. J., "Fault Tree for Reliability Analysis," *Proceedings of the Annual Symposium Reliability*, IEEE, New York, 1970.
66. Semanderes, S. N., "Elraft, a Computer Program for Efficient Logic Reduction Analysis of Fault Trees," *IEEE Trans. Nucl. Sci.*, **18**, (February 1971).
67. Shooman, M. L., "The Equivalence of Reliability Diagrams and Fault-Tree Analysis," *IEEE Trans. Reliab.*, **R-19**, 74–75 (1970).
68. Vesely, W. E., "A Time-Dependent Methodology for Fault Tree Evaluation," *Nucl. Eng. Design*, **13**, 337–360. (April, 1970).
69. Vesely, W. F., "Reliability and Fault-Tree Applications at the NRTS," *IEEE Trans. Nucl. Sci.*, **18**, 472–480 (February 1971).
70. Virolainen, R., "Unreliability of a Complex System with Parallel Redundancy and Repair," *Nucl. Eng. Design*, **40**, 431–441 (1977).
71. Wheeler, D. B. et al., "Fault Tree Analysis Using Bit Manipulation," *IEEE Trans. Reliab.* **R-26**, 95–99 (June 1977).
72. Worrell, R. B., "Using the Set Equation Transformation System in Fault Tree Analysis," In: *Reliability and Fault Tree Analysis*, SIAM, Philadelphia, 1975.
73. Wynholds, H. W. and R. Poterfield, "Fault-Tree Graphics," In: *Reliability and Fault Tree Analysis*, SIAM, Philadelphia, 1975.
74. Young, J., "Using the Fault Tree Analysis Technique," In: *Reliability and Fault Tree Analysis*, SIAM, Philadelphia, 1975.

Common-Cause Failures

75. Apostolakis, G. E., "The Effect of a Certain Class of Potential Common-Mode Failures on the Reliability of Redundant Systems," *Nucl. Eng. Design*, **36**, 123–133 (1976).
76. Apostolakis, G. E., "On a Certain Class of Potential Common-Mode Failures," *Trans. Am. Nucl. Soc.*, **22**, 476–477 (1975).
77. Apostolakis, G. E., "On the Reliability of Redundant Systems," *Trans. Am. Nucl. Soc.*, **22**, 477–478 (1975).
78. Barlow, R. T., R. A. Hill, D. C. McIntine, and J. F. O'Brien, "Probabilistic Evaluation of Failure Modes Leading to the Mispositioning of Certain ECCS Motor Operated Valves in Westinghouse NSS," *IEEE Trans. Power Appar. Syst.*, **PAS-97**, 358–361 (March/April 1978).
79. Billington, R., T. K. P. Medicherla, and M. S. Sachdev, "Common-Cause Outages in Multiple Circuit Transmission Lines," *IEEE Trans. Reliability*, **27**, 128–131 (1978).
80. Burdick, G. R., "COMCAN—A Computer Code for Common-Cause Analysis," *IEEE Trans. Reliab.*, **R-26**, 100–102 (1977).
81. Cain, D. G., "Closing the Loop Summary-Equipment Qualification," *Proceedings of the 1977 Environmental Technology Conference*. Institute of the Environmental Sciences, IL, 60058, pp. 434–437. (1977).
82. Cate, C. L., D. P. Wagner and J. B. Fussell, "A Computer Aided Approach to Qualitative and Quantitative Common-Cause Failure Analysis for Complex Systems," *Proceedings of the Eighth Pittsburgh Modelling and Simulation Conference*, Instrument Society of America, Pittsburgh, 1977, pp. 25–29.
83. Chelapati, C. V., and R. P. Kennedy, "Probabilistic Assessment of Aircraft Hazard for Nuclear Plants," *Nucl. Eng. Design*, **19**, 333–364 (1972).
84. Chu, B. B. and D. P. Gaver, "A Stochastic Modelling for Common-Mode Failures of Repairable Redundant Systems," *Conference Proceedings*, Edited by J. B. Fussell and G. R. Burdick, SIAM, Philadelphia, 1977.
85. Dhillon, B. S., "A k-out-of-N Three-state Devices System with Common-cause Failures," *Microelectron. Reliab.*, **18**, 447–448 (1978).
86. Dhillon, B. S., "A Modification to Fault Tree "AND" Gate," *Microelectron. Reliab.*, **15**, 625–626 (1976).
87. Dhillon, B. S., "A 4-Unit Redundant System with Common-Cause Failures," *IEEE Trans. Reliab.*, **R-26**, 373–374 (1977).
88. Dhillon, B. S. and C. L. Proctor, "Common-Mode Failure Analysis of Reliability Networks," *Proceedings of the Annual Reliability and Maintainability Symposium*, IEEE, New York, 1977, pp. 404–408.
89. Dhillon, B. S., "Effects of Weibull Hazard Rate on Common-Cause Analysis of Reliability Networks," *Microelectron. Reliability*, **17**, 59–65 (1978).
90. Dhillon, B. S., "Optimal Maintenance Policy for Systems with Common-Cause Failures," *Proceedings of the Ninth Pittsburgh Modelling and Simulation Conference*, Instrument Society of America, Pittsburgh, 1978.
91. Dhillon, B. S., "A 1-out-of-N: G system with Duplex Elements," *IEEE Trans. Reliab.* (in press).
92. Dhillon, B. S., "A Common-Cause Failure Availability Model," *Microelectron. Reliability*, **17**, 583–584 (1978).
93. Dhillon, B. S., "ON Common-Cause Failures—Bibliography," *Microelectron. Reliability*, **18**, 533–534 (1978).
94. Dhillon, B. S., "A 4-Unit Redundant System with Common-Cause Failures," *IEEE Trans. Reliability*, **R-28**, 267 pp. (June 1979).
95. Dhillon, B. S., A. Sambhi, and M. R. Khan, "Common Cause Failure Analysis of a Three-State Device System," *Microelectron. Reliab.*, **19**, 345–348 (1979).

96. Ditto, S. J., "Failures of Systems Designed for High Reliability," *Nucl. Safety*, **8**, 35–37 (Fall 1966).
97. Epler, E. P., "Common-Mode Failure Considerations in the Design of Systems for Protection and Control," *Nucl. Safety*, **11**, 323–327 (Jan.–Feb. 1969).
98. Epler, E. P., "The ORR Emergency Cooling Failures," *Nucl. Safety*, **11**, 323–327 (July–Aug. 1970).
99. Epler, E. P., "Diversity and Periodic Testing in Defense Against Common-Mode Failures," Edited by J. B. Fussell and G. R. Burdick, *Conference Proceedings*, Society for Industrial and Applied Mathematics, Philadelphia, PA 19103, 1977.
100. Evans, R. A., "Statistical Independence and Common-Mode Failures," *IEEE Trans. Reliab.*, **R-24**, 289 (1975).
101. Fleming, K. N., "A Redundant Model for Common Mode Failures in Redundant Safety Systems," *Proceedings of the Sixth Pittsburgh Annual Modelling and Simulation Conference*, Instrument Society of America, Pittsburgh, 1975, pp. 579–581
102. Fleming, K. N., and G. W. Hannaman, "Common Cause Failure Considerations in Predicting HTGR Cooling System Reliability," *IEEE Trans. Reliab.*, **R-25**, 171–177 (1976).
103. Gachot, B., "A Probabilistic Approach to Design for the ECCS of a PWR," *Proceedings of the Annual Reliability and Maintainability Symposium*, 1977, pp. 332–342.
104. Gangloff, W. C., "Common-Mode Failure Analysis is "in"," *Electron. World*, 30–33 (Oct. 1972).
105. Gangloff, W. C., "Common Mode Failure Analysis," *IEEE Trans. Power Apparatus Systems*, **94**, 27–30 (Feb. 1975).
106. Gangloff, W. C. and T. Franke, "An Engineering Approach to Common-Mode Failure Analysis," *Conference on the Development and Application of Reliability Techniques to Nuclear Plants, Liverpool, England* (April 1974). University of Liverpool.
107. Garrick, B. J., W. C. Gekler, and H. P. Pomrehn, "Some Aspects of Protective Systems in Nuclear Power Plants," *IEEE Trans. Nucl. Sci.*, **NS-12**, 22–30 (Dec. 1975).
108. Hayden, K. C., "Common-Mode Failure Mechanisms in Redundant Systems Important to Reactor Safety," *Nucl. Safety*, **17**, 686–693 (1976).
109. Houghton, W. J., V. Joksimovic, and D. E. Emon, "Methods of Probabilistic Safety Analysis for Gas-Cooled Reactors," *Trans. Amer. Nucl. Soc.*, **21**, 210–217 (1975).
110. Jacobs, I. M., "The Common-Mode Failure Study Discipline," *IEEE Trans. Nucl. Sci.*, **NS-17**, 594–598 (1970).
111. Levine, S. and W. E. Vesely, "Important Event-Tree and Fault-Tree Considerations in the Reactor Safety Study," *IEEE Trans. Reliab.*, **R-25**, 132–139 (1976).
112. Leverenz, F. L., E. T. Rumble, and E. Erdmann, "A Dependent-Event Model for Fault Trees," *Trans. Amer. Nucl. Soc.*, **21**, 212–213 (1975).
113. Rankin, J. P., "Sneak-Circuit Analysis," *Nucl. Safety*, **14**, 461–469, (Sept.–Oct. 1973).
114. *Reactor Safety Study*, WASH-1400 (NUREG-75/014)(Oct. 1975), National Technical Information Service, Springfield, VA 22161.
115. Rubel, P., "Tiger in the Fault Tree Jungle," *Proceedings of the Seventh Annual Pittsburgh Modelling and Simulation Conference*, Pittsburgh, Instrument Society of America, 1976, pp. 1071–1082.
116. Taylor, J. R., "A Study of Failure Causes Based on U.S. Power Reactor Abnormal Occurrence Reports," *Reliab. Nucl. Power Plants*, IAEA-SM-195/16 (1975).
117. Vesely, W. E., "Estimating Common-Cause Failure Probabilities in Reliability and Risk Analysis: Marshal-Olkin Specialization," Edited by J. B. Fussell and G. R. Burdick, Society for Industrial and Applied Mathematics, Philadelphia, PA 19103, 1977.

118. Wagner, D. P., C. L. Cate, and J. B. Fussell, "Common-Cause Failure Analysis Methodology for Complex Systems," Edited by J. B. Fussell and G. R. Burdick, *Conference Proceedings*, Society for Industrial and Applied Mathematics, 33 South 17 St., Philadelphia Pennsylvania 19013 U.S.A.
119. Wall, I. B., "Probabilistic Assessment of Flooding for Nuclear Power Plants," *Nucl. Safety*, **15**, 399–408 (1974).
120. Wall, I. B., "Probabilistic Assessment of Aircraft Risk for Nuclear Power Plants," *Nucl. Safety*, **15**, 276–284 (1974).
121. Wilson, J. R. and R. J. Crump, "Computer-Aided Common-Cause Analysis of an LMFBR System," *Trans. Amer. Nucl. Soc.*, **22**, 474–475 (1975).
122. Worrell, R. B. and G. R. Burdick, "Qualitative Analysis in Reliability and Safety Studies," *IEEE Trans. Reliab.*, **R-25**, 164–169 (1976).

Miscellaneous

123. Cox, D. R., "The Analysis of Non-Markovian Stochastic Process by Supplementary Variables," *Proc. Camb. Phil. Soc.*, **51**, 433–441 (1955).
124. *Flow Research Report*, "Risk Analysis Using the Fault Tree Technique," Flow Research, Inc., 1973.
125. Garg, R. C., "Dependability of a Complex System Having Two Types of Components," *IEEE Trans. Reliab.*, **R-12**, 11–15 (Sept. 1963).
126. Gaver, D. P., "Time to Failure and Availability of Paralleled Systems with Repair," *IEEE Trans. Reliab.*, **R-12**, 30–38 (June 1963).
127. Lipp, J. P., "Topology of Switching Elements vs. Reliability," *Trans. IRE Reliab. Quality Control* (June 1957).
128. Ross, S. M., "On the Calculation of Asymptotic System Reliability Characteristics," *Reliability and Fault Tree Analysis*, SIAM, Philadelphia, 1975, pp. 331–350.
129. Shooman, M. L., *Probabilistic Reliability: An Engineering Approach*, McGraw-Hill, New York, 1968.
130. Wolfe, W. A., "Fault Trees Revisited," *Microelectron. Reliab.*, **17**, (1978).