RELIABILITY ANALYSIS OF SYSTEMS

Y.K. Tung
L.W. Mays
M.J. Cullinane, Jr.

1989
Book Chapter WWRC-89-21

In

Reliability Analysis of
Water Distribution Systems

Chapter 9

Y.K. Tung
Wyoming Water Research Center
University of Wyoming
Laramie, Wyoming

L.W. Mays
Center for Research in Water Resources
University of Texas
Austin, Texas

M.J. Cullinane, Jr.
Waterways Experiment Station
Vicksburg, Mississippi

CHAPTER 9

RELIABILITY ANALYSIS OF SYSTEMS

by

Y. K. Tung, Larry W. Mays and M. John Cullinane

9.1 SIMPLE SYSTEMS

Most systems are composed of several subsystems. The reliability of a system depends on how the components are interconnected. Several methods for computing system reliability are presented below.

9.1.1 Series Systems

The simplest type system is a series system in which every component must function if the system is to function (see Fig. 9.1.1). Considering the random variable of the time of failure as T_i for the i-th component, then for a system of n components, the system reliability over the period (0, t) is

$$R_s(t) = \prod_{i=1}^{n} P\left(T_i > t\right) = \prod_{i=1}^{n} R_i(t) \qquad (9.1.1)$$

where $R_i(t)$ is the reliability for the i-th component. For a system that has failure times exponentially distributed (with constant failure rates) so that the i-th component reliability is $e^{-\lambda_i t}$, then the system reliability is

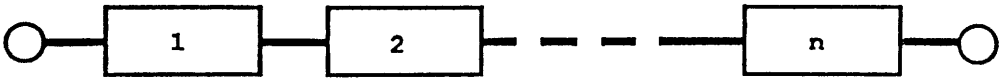


Figure 9.1.1 Components Arranged in Series

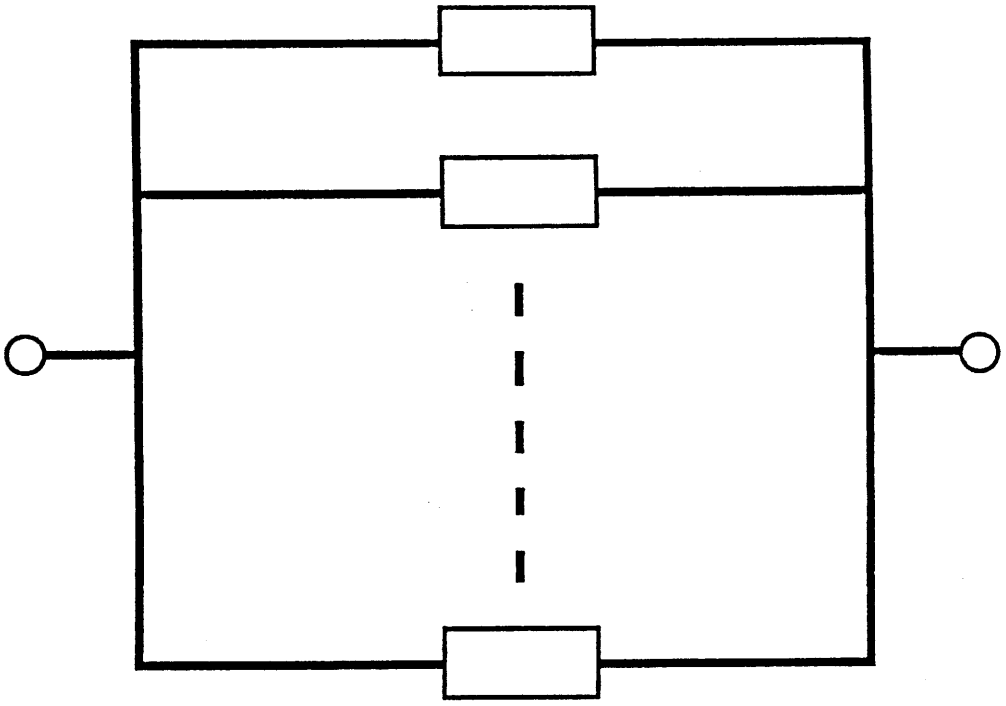


Figure 9.1.2 Components Arranged in Parallel

$$R_s(t) = \exp\left(-\sum_{i=1}^{n} \lambda_i t\right) \tag{9.1.2}$$

The MTTF is

$$\text{MTTF} = \int_0^{\infty} \exp\left(-\sum \lambda t\right) dt = \frac{1}{\sum_{i=1}^{n} \lambda_i} \tag{9.1.3}$$

Example

As an example of the series system, consider two different pumps in series, both of which must operate to pump the required quantity. The constant failure rates for the pumps are $\lambda_1 = 0.0003$ failures/hr and $\lambda_2 = 0.0002$ failures/hr. For a 2,000-hr mission time, the system reliability is

$$R_s(t) = e^{-(0.0003 + 0.0002)\,(2000)} = 0.90484 \tag{9.1.4}$$

and the MTTF is

$$\text{MTTF} = \frac{1}{0.0003 + 0.0002} = 2{,}000 \text{ hr} \tag{9.1.5}$$

9.1.2 Chain-Series Systems

A chain-series model is a series system such that if any one component fails, the system will fail. This model is based on the idea of a chain composed of n links where the chain will break if the applied stress X exceeds the strength Y of any one link. This model is also referred to as a weakest link model. The system reliability is then

$$R_s = \min_i \left\{R_i\right\} \tag{9.1.6}$$

The reliability for any one link by equation (9.1.3) is

$$R_i = P(X < Y_i) = \int_0^\infty f_{Y_i}(y)\, F_X(y)\, dy \qquad (9.1.7)$$

9.1.3 Parallel Systems

A parallel system is defined as one which will fail if and only if all units in the system fail or malfunction (see Fig. 9.1.2). The pure parallel system is one in which all components are initially activated, and any component can maintain the system operation. The system reliability is then expressed as

$$R_s(t) = 1 - \prod_{i=1}^{n} \left[1 - R_i(t)\right] \qquad (9.1.8)$$

For a system with exponentially distributed time to failure and a constant failure rate for each component of the system, the system reliability is

$$R_s(t) = 1 - \prod_{i=1}^{n} \left(1 - e^{-\lambda_i t}\right) \qquad (9.1.9)$$

and the MTTF for a system with identical components is

$$MTTF = \frac{1}{\lambda} \sum_{i=1}^{n} \frac{1}{i} \qquad (9.1.10)$$

Example

As an example of a parallel system, consider two identical pumps operating in a redundant configuration so that either pump could fail and the peak discharge could still be delivered. Both pumps have a failure rate of $\lambda = 0.0005$ and both pumps start operating at $t = 0$. The system reliability for a mission time of $t = 1{,}000$ hr is

$$R_s(t) = 1 - \left(1 - e^{-\lambda_1 t}\right)\left(1 - e^{-\lambda_2 t}\right)$$

$$= 2e^{-\lambda t} - e^{-2\lambda t}$$

$$= 2e^{-(0.0005)(1000)} - e^{-2(0.0005)(1000)}$$

$$= 1.2131 - 0.3679$$

$$= 0.8452 \qquad (9.1.11)$$

The MTTF is

$$\text{MTTF} = \frac{1}{\lambda}\left(\frac{1}{1} + \frac{1}{2}\right) = \frac{3}{2}\,\frac{1}{\lambda} = 1.5\left(\frac{1}{0.0005}\right) = 3{,}000 \text{ hr} \qquad (9.1.12)$$

9.1.4 Standby Redundancy

A standby-redundant system is a parallel system in which only one component or subsystem is in operation (see Fig. 9.1.3). If the operating component fails, then another component is operated. This type of system is different than the parallel network where all the components are operating because standby units do not operate. The system reliability for a system with n + 1 components in which one component is operating and n units are on standby until the operating unit fails, is given by

$$R_s(t) = \sum_{i=0}^{n} \frac{(\lambda t)^i e^{-\lambda t}}{i!} \qquad (9.1.13)$$

This assumes the following: the switching arrangement is perfect, the units are identical, the component failure rates are constant, the standby units are as good as new, and the unit failures are statistically independent. For n + 1 nonidentical components with different failure time density functions, the system reliability is

$$R_s(t) = \int_t^{\infty} f_{st}(t)\,dt \qquad (9.1.14)$$

where $f_{st}(t)$ is the standby-redundant system failure density given by

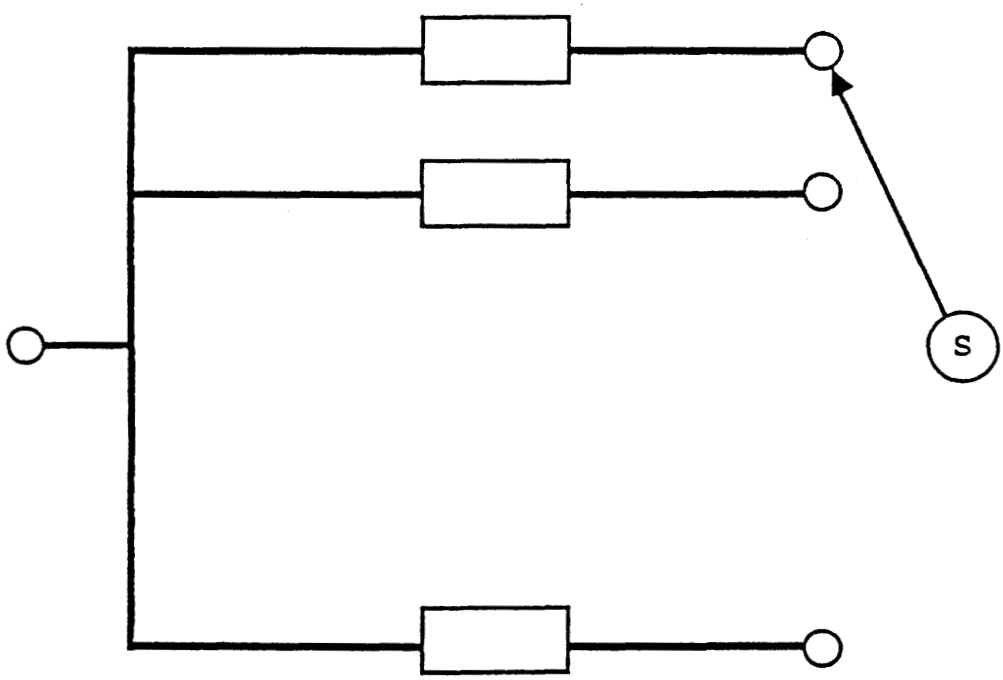


Figure 9.1.3 Standby-Redundancy System

$$f_{st}(t) = \int_0^t \int_0^{y_n} \cdots \int_0^{y_2} f_1(y_1) f_2(y_2 - y_1) \cdots f_{n+1}(t - y_n)\, dy_1\, dy_2 \cdots dy_n \quad (9.1.15)$$

Example

As an example of a standby-redundant system, assume an exponential failure distribution and consider two identical pumps, one operating and the second on standby, with identical failure rates of λ = 0.0005 failures/hr. The standby unit is as good as new at time t = 0. The system reliability for t = 1,000 hr is

$$R_{st}(t) = (1 + \lambda t)e^{-\lambda t} = (1 + 0.0005 \cdot 1000)e^{-(0.0005)(1000)} = 0.9098 \quad (9.1.16)$$

K-out-of-n Systems

A k-out-of-n system is a system in which a specified number k of n subsystems must be good for system success. The binomial distribution is used to define the system reliability for k-out-of-n of independent and identical units given by

$$R_{k/n} = \sum_{i=k}^{n} \binom{n}{i} R^i (1 - R)^{n-i} \quad (9.1.17)$$

where

$$\binom{n}{i} = \frac{n!}{i!(n - i)!}$$

For a constant failure rate the reliability is expressed as

$$R_{k/n}(t) = \sum_{i=k}^{n} \binom{n}{i} \left(e^{-\lambda t}\right)^i \left(1 - e^{-\lambda t}\right)^{n-i} \quad (9.1.18)$$

Example

As an example of a k-out-of-n system, consider a pumping system with three pumps, one of which is standby, all with constant failure rates

of $\lambda = 0.0005$ failures/hr. The system reliability for t = 1,000 hr, n = 3 and k = 2, is

$$R_{2/3}(t) = 3e^{-(2)\,(0.0005)\,(1000)} - 2e^{-(3)\,(0.0005)\,(1000)}$$

$$= 1.1036 - 0.4463$$

$$= 0.6573 \qquad (9.1.19)$$

9.2 COMPLEX SYSTEMS

As shown in the previous section, the reliability of series-parallel systems is generally straightforward. In most practical situations, such as water distribution systems have a nonseries-parallel configuration and the evaluation is much more difficult. There have been many techniques developed for system reliability evaluation. A great deal of work has been done on state enumeration methods (event-space methods), network reduction methods, and path enumeration methods. A brief summary is provided of each of these methods.

9.2.1 State-Enumeration Methods

This method lists all possible mutually exclusive states of the system. A state is defined by listing the successful and failed elements in the system. For a system with n elements or components, in general, there are 2^n states, so that a system with 10 components would have 1,024 states. The states which result in successful system operation are identified and the probability of occurrence of each successful state is computed. The last step is to sum all the successful state probabilities which give the system reliability. This method can be computationally infeasible for systems having a large number of components (Brown, 1971). The event-tree technique is a typical method that uses the approach.

Example

Consider a simple water distribution network consisting of five pipes and one loop, as shown in Fig. 9.2.1. Node 1 is the source node and nodes 3, 4, and 5 are demand nodes. The components of this network subject to possible failure are the five pipe sections. Within a given time period, each pipe section has an identical failure probability of 5% due to breakage or other causes that require it to be removed from service. The system reliability is defined as the probability that water can reach all three

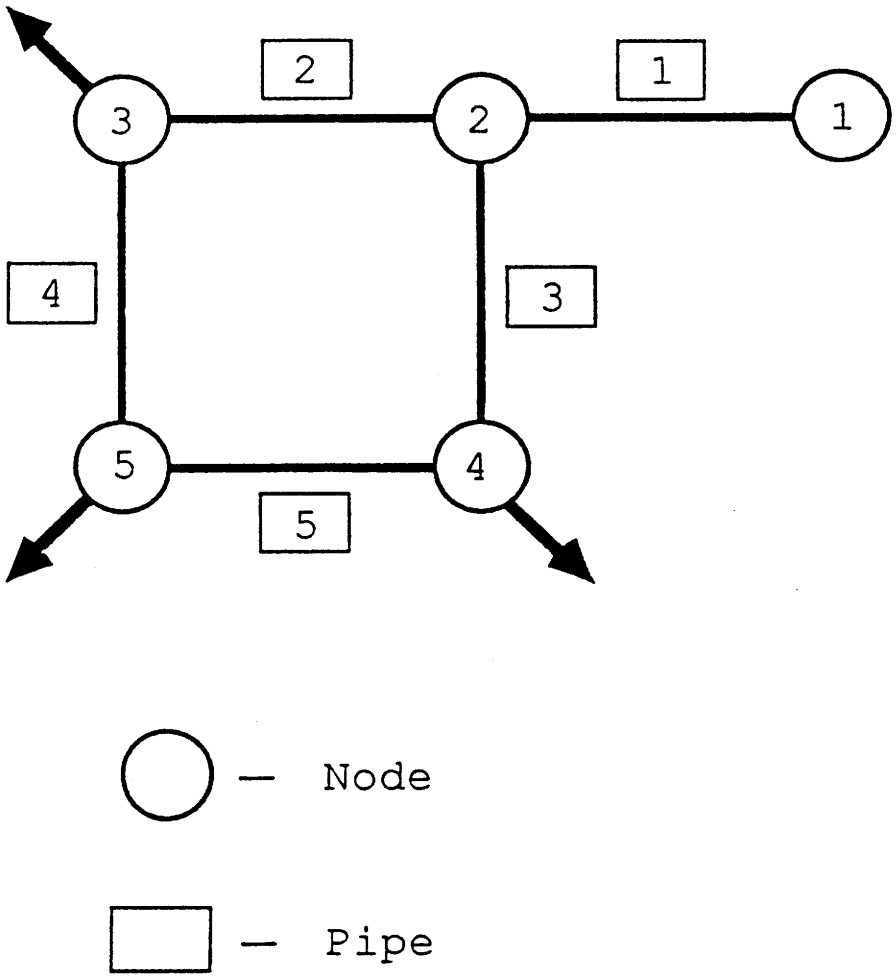


Figure 9.2.1 Simple Example Water Distribution Network

demand nodes from the source node. Furthermore, it is assumed that the states of serviceability of each pipe are independent.

Using the state-enumeration method for system reliability evaluation, the associated event tree can be constructed depicting all possible combinations of component states in the system, as shown in Fig. 9.2.2. Since each pipe has two possible states, i.e., failure (F) or nonfailure (N), the tree, if fully expanded, would have $2^5 = 32$ branches. However, knowing the role that each pipe component plays in the network connectivity, exhaustive enumeration of all possible states is not necessary.

For example, referring to Fig. 9.2.2, we realize that when pipe 1 fails, all demand nodes cannot receive water, indicating a system failure, regardless of the state of the remaining pipe sections. Therefore, branches in the event tree beyond this point do not have to be constructed. Applying some judgment in event-tree construction in this fashion can generally lead to a smaller tree. However, for a complex system, this may not be easy.

The system reliability can be obtained by summing up the probabilities associated with all of the nonfailure branches. In this example, the system reliability is

$$R_s = P\left\{\bigcup_{i=1}^{5} B_{[i]}\right\}$$

$$= \sum_{i=1}^{5} P\left(b_{[i]}\right)$$

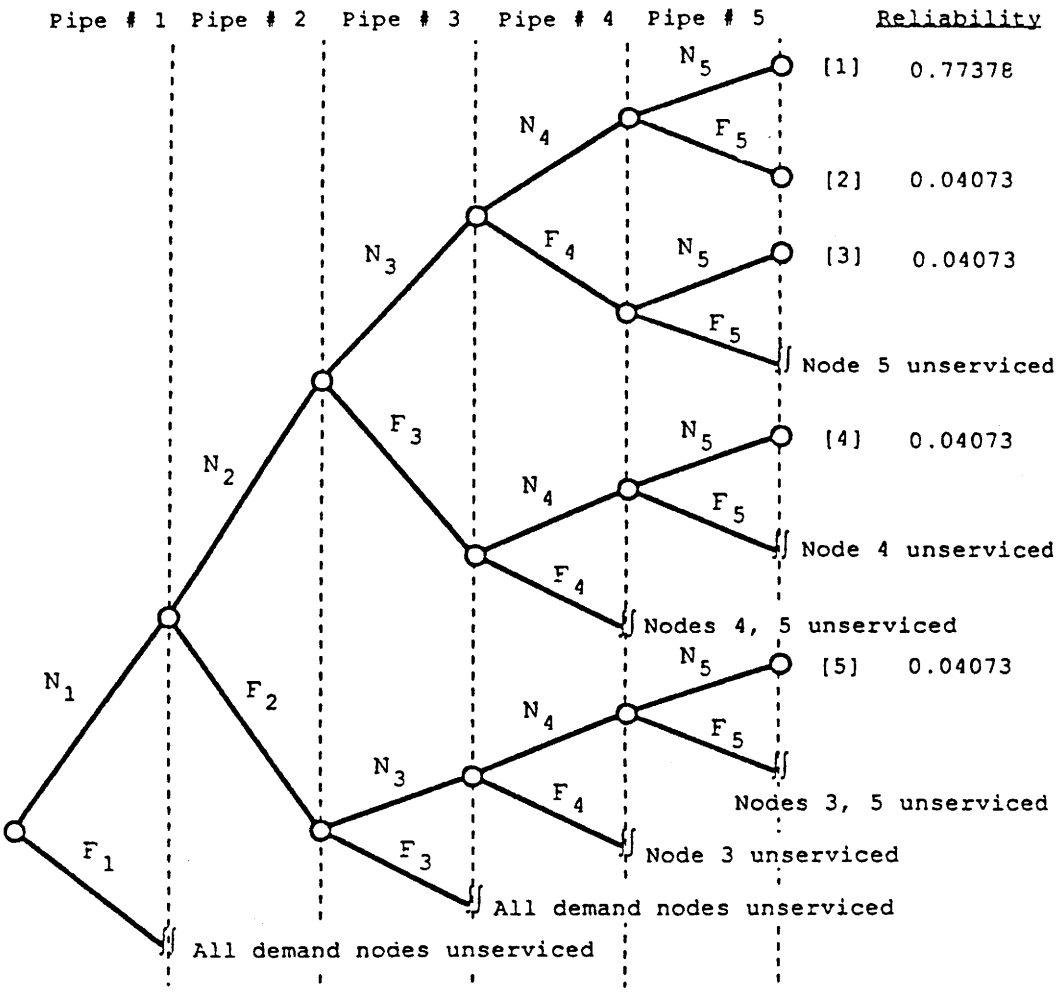
$$= 0.9367$$

where $P(B_{[i]})$ = the probability that the branch $B_{[i]}$ of the event tree. For example, the probability that branch $B_{[2]}$ occurs is

$$P\left(B_{[2]}\right) = P\left[N_1\right] \cdot P\left[N_2\right] \cdot P\left[N_3\right] \cdot P\left[N_4\right] \cdot P\left[F_5\right]$$

$$= (0.95)\,(0.95)\,(0.95)\,(0.95)\,(0.05)$$

$$= 0.04073$$



N_i = Non-failure of pipe i

F_i = Failure of pipe i

$\int\int$ = Branch associated with unserviceability of one or more demand nodes

[i] = The i-th branch indicating system reliability

Figure 9.2.2 Example Event Tree for State Enumeration Method

9.2.2 Network-Reduction Methods

These methods combine the series, parallel, and series-parallel subsystems until a nonseries-parallel system which cannot be further reduced is obtained. Factoring theorems are then used to obtain system reliability. A component A is selected, and two networks are obtained and generated when A is replaced by a short circuit (perfect competition) and an open circuit. If the two networks are simple series-parallel, they can be reduced; otherwise, the next block A must be selected and the procedure is repeated. Further discussions of network-reduction methods can be found in Moscowitz (1958), Buzacott (1970), Banerjee and Rajamani (1972), and Misra (1972).

In general, network-reduction methods are useful if the network system under investigation consists of a single-source node and a single-sink node. Because of the nature of a water distribution network that involves multiple source and sink nodes, the technique of network-reduction methods cannot be directly applied for system reliability evaluation.

9.2.3 Path-Enumeration Methods

Path-enumeration methods are very valuable tools for system reliability evaluation. The tie-set analysis and the cut-set analysis are the two well-known methods in which the former uses the minimum path concept while the latter uses the minimum cut-set concept. A path is a set of elements (components) which form a connection between input and output when traversed in a stated direction. A minimal path is one in which no node is traversed more than once in going along the path. The i-th minimal path will be denoted as T_i, i = 1,...,m. Assuming that any path is operable and the system performs adequately, then the system reliability is

$$R = P\left[\bigcup_{i=1}^{m} T_i\right] \tag{9.2.1}$$

where P [ ] represents probability that at least one of the m paths will be operable and $\cup$ denotes the union.

Example

Refer to the previous example with the simple water distribution network as shown in Fig. 9.2.1 The minimum tie-set (or path), based on the definition of system reliability given previously, for the example network are

$$T_1 = \{N_1 \cap N_2 \cap N_4 \cap N_5\}$$

$$T_2 = \{N_1 \cap N_3 \cap N_5 \cap N_4\}$$

where T_i = the i-th minimum tie-set and N_k = the nonfailure of the k-th pipe link in the network. The four minimum tie-sets are shown in Fig. 9.2.3. The system reliability, based on equation (9.2.1), is

$$\begin{aligned} R_s &= P(T_1 \cup T_2 \cup T_3 \cup T_4) \\ &= P(T_1) + P(T_2) + P(T_3) + P(T_4) \\ &\quad - [P(T_1 \cap T_2) + P(T_1 \cap T_3) + P(T_1 \cap T_4) \\ &\quad + P(T_2 \cap T_3) + P(T_2 \cap T_4) + P(T_3 \cap T_4)] \\ &\quad + [P(T_1 \cap T_2 \cap T_3) + P(T_1 \cap T_2 \cap T_4) + P(T_1 \cap T_3 \cap T_4) \\ &\quad + P(T_2 \cap T_3 \cap T_4)] - P(T_1 \cap T_2 \cap T_3 \cap T_4) \end{aligned}$$

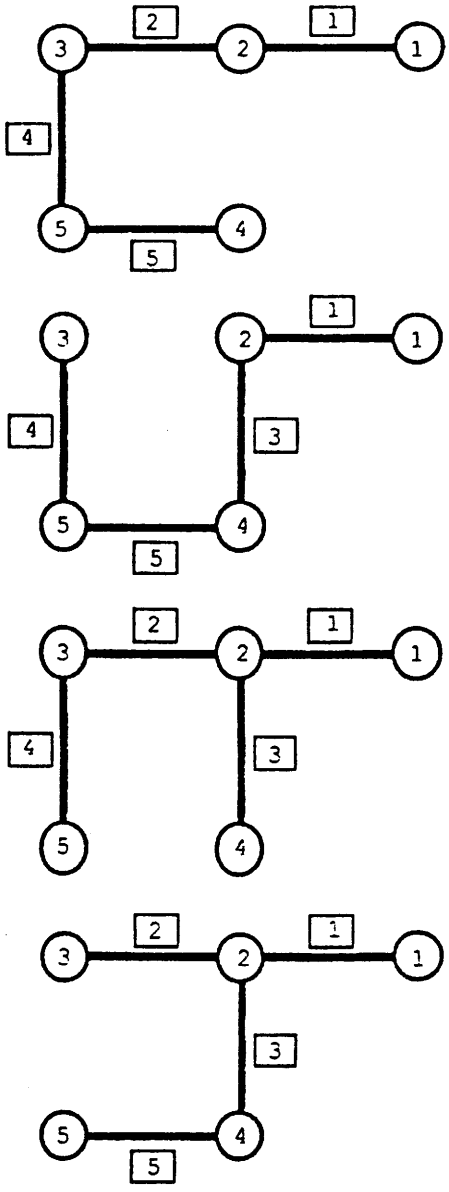
Since all pipes in the network behave independently, all minimum tie-sets (or paths) behave independently. In such circumstances, the probability of the joint occurrence of multiple independent events is simply the multiplication of the probability of the individual event. That is,

$$P(T_1) = P(N_1) \cdot P(N_2) \cdot P(N_4) \cdot P(N_5) = (0.95)^4 = 0.81451$$

Similarly,

$$P(T_2) = P(T_3) = P(T_4) = 0.81451$$

Note that, in this example, the intersections of more than two minimum tie-sets is the intersection of the nonfailure state of all five pipe sections, i.e., $N_1 \cap N_2 \cap N_3 \cap N_4 \cap N_5$. The system reliability can be reduced to



$T_1 = (N_1 \cap N_2 \cap N_4 \cap N_5)$

$T_2 = (N_1 \cap N_3 \cap N_4 \cap N_5)$

$T_3 = (N_1 \cap N_2 \cap N_3 \cap N_4)$

$T_4 = (N_1 \cap N_2 \cap N_3 \cap N_5)$

T_i = the i^{th} tie set

N_k = Non-failure state of pipe section k

Figure 9.2.3 The Four Minimum Tie-Sets (or Paths) for the Example Network

$$R_s = P(T_1) + P(T_2) + P(T_3) + P(T_4)$$
$$- 3P(N_1 \cap N_2 \cap N_3 \cap N_4 \cap N_5)$$
$$= 4\,(0.81451) - 3\,(0.95)^5$$
$$= 0.9367$$

A cut-set is defined as a set of elements which, if it fails, causes the system to fail regardless of the condition of the other elements in the system. A minimal cut is one in which there is no proper subset of elements whose failure alone will cause the system to fail. In other words, a minimal cut is such that if any component is removed from the set, the remaining elements collectively are no longer a cut-set. The minimal cut-sets are denoted as C_i, i = 1,...,m and $\overline{C}_i$ denotes the complement of C_i, i.e., the failure of all elements of the cut C_i. The system reliability is

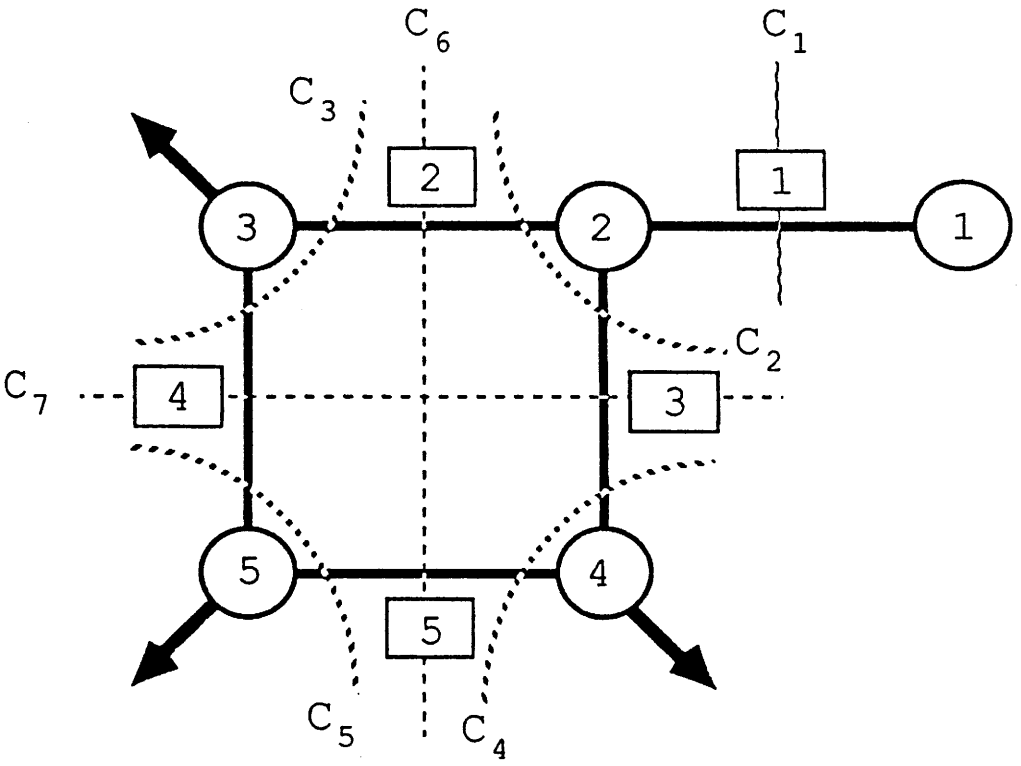
$$R_i = 1\text{-}P\left[\bigcup_{i=1}^{m} C_i\right] = P\left[\bigcap_{i=1}^{m} \overline{C}_i\right] \qquad (9.2.2)$$

Example

Again, refer to the previous simple water distribution network example. We now like to evaluate system reliability using the minimum cut-set method. Based on the system reliability as defined, the minimum cut-sets for the example network are

$$C_1 = \{F_1\} \qquad C_2 = \{F_2 \cap F_3\}$$
$$C_3 = \{F_2 \cap F_4\} \qquad C_4 = \{F_3 \cap F_4\}$$
$$C_5 = \{F_4 \cap F_5\} \qquad C_6 = \{F_2 \cap F_5\}$$
$$C_7 = \{F_3 \cap F_4\}$$

where C_i = the i-th cut-set and F_k = the failure state of pipe link k. The above seven cut-sets for the example network is shown in Fig. 9.2.4. The



C_i = the i^{th} cut set

Figure 9.2.4 Cut-Sets for the Example Water Distribution Network

system unreliability R is the probability of occurrence of the union of the cut-set, i.e.,

$$\overline{R}_s = P\left[\bigcup_{i=1}^{7} C_i\right]$$

The system reliability can be obtained by subtracting R_s from 1. However, the computation, in general, will be very cumbersome for finding the probability of the union of large numbers of events, even if they are independent. In this circumstance, it is computationally easier to compute the system reliability, by equation (9.2.2), as

$$R_s = P\left[\bigcup_{i=1}^{7} C_i\right] = P\left[\bigcap_{i=1}^{7} \overline{C}_i\right]$$

where the overbar "—" represents the complement of the event. Since all cut-sets behave independently, all their complements also behave independently. The probability of the intersection of a number of independent events, as described previously is

$$R_s = \prod_{i=1}^{7} P\left(\overline{C}_i\right)$$

where

$$P\left(\overline{C}_1\right) = 0.95,\ P\left(\overline{C}_2\right) = P\left(\overline{C}_3\right) = \ldots = P\left(\overline{C}_7\right) = 0.9975$$

Hence, the system reliability of the example network is

$$R_s = (0.95)\ (0.9975)^6 = 0.9360$$

A basic algorithm for the path-enumeration method can be stated as (Henley and Gandhi, 1975):

a. Find all minimal paths using the reliability graph. Several computer codes have been developed for this purpose which are discussed in a later section.

b. Find all required unions of the paths.

c. Give each path union a reliability expression in terms of module reliability.

d. Use the following equation expressing the system reliability in terms of module reliabilities.

$$R = \sum_{i=1}^{m} \prod_{1 \epsilon P_i} R_1 - \sum_{i=1}^{m} \sum_{j>1}^{m} \prod_{1 \epsilon P_i \cup P_j} R_1$$

$$+ \sum_{i=1}^{m} \sum_{j>1}^{m} \sum_{k>1}^{m} \prod_{1 \epsilon P_i \cup P_j \cup P_k} R_1 + \ldots + (-1)^{m-1} \prod_{\substack{m \\ 1 \epsilon \cup P_i \\ i=1}} R_1 \qquad (9.2.3)$$

where the members of the i-th path are denoted as $1 \epsilon P_i$, the union of the i-th and j-th paths are denoted by $1 \epsilon P_1 \cup P_j$, etc.

9.2.4 Conditional-Probability Approach

The approach starts with a selection of key elements (or components) whose states (operational or failure) would decompose the entire system into simple series and/or parallel subsystems for which the reliability and risk of subsystems can be easily evaluated. Then, the reliability of the entire system is obtained by combining the subsystems using the conditional probability rule as:

P (system success or failure) =
P (system success or failure if component X is good) • P (X is good)
+ P (system success or failure if component X is bad) • P (X is bad)

Except for a very simple and small system, a nested conditional-probability operation is inevitable. Efficient evaluation of system reliability of a complex system hinges entirely on a proper selection of key elements which generally would be a difficult task when one deals with a moderate or large water distribution network. The technique also cannot be easily adopted to computerization for problem solving.

Example

Using the conditional-probability approach for system reliability evaluation, first select pipe section 1 as the key element which decomposes the system into a simpler configuration, as shown in Fig. 9.2.5. After the entire system is decomposed into a simple-system configuration, the conditional probability of the decomposed systems can be easily evaluated. For example, the conditional system reliability, after imposing N_1 and F_3 for pipes 1 and 3, respectively, can be expressed as

$$R_{s\,|N_1, F_3} = P\left(N_2 \cap N_4 \cap N_5\right) = (0.95)^3 = 0.8574$$

where $R_{s\,|N_1, F_3}$ = conditional system reliability. Conditional system reliabilities for other imposed conditions are shown in Fig. 9.2.5 After the conditional system reliabilities for the decomposed systems are calculated, the reliability of the entire system can be combined using equation (9.2.5). For this particular example, the system reliability is

$$R_s = R_{s/N_1, F_3} \bullet P\left(N_1 \cap F_3\right) + R_{s/N_1, N_3, N_2} \bullet P\left(N_1 \cap N_3 \cap N_2\right)$$

$$+ R_{s/N_1, N_3, F_2} \bullet P\left(N_1 \cap N_3 \cap F_2\right)$$

$$= (0.8574)\,(0.95)\,(0.9975)\,(0.95)^3 + (0.9025)\,(0.95)^2\,(0.05)$$

$$= 0.9370$$

9.2.5 Review of System Reliability Evaluation Techniques for Complex Systems

Hwang, Tillman, and Lee (1981) presented a review of literature related to system reliability evaluation techniques for small to large complex systems. A large system was defined as one which was more than ten components and a moderate system as one which has more than six components and less than ten. Complex systems were defined as ones which could not be reduced to a series-parallel system.

Hwang, Tillman, and Lee (1981) concluded that for a large complex system, computer programs should be used that provide the minimum cut-sets and calculate the minimal cut approximation to system reliability. Minimal paths can be generated from minimum cuts. Based on minimum cut-sets, reliability approximations can then be obtained for large

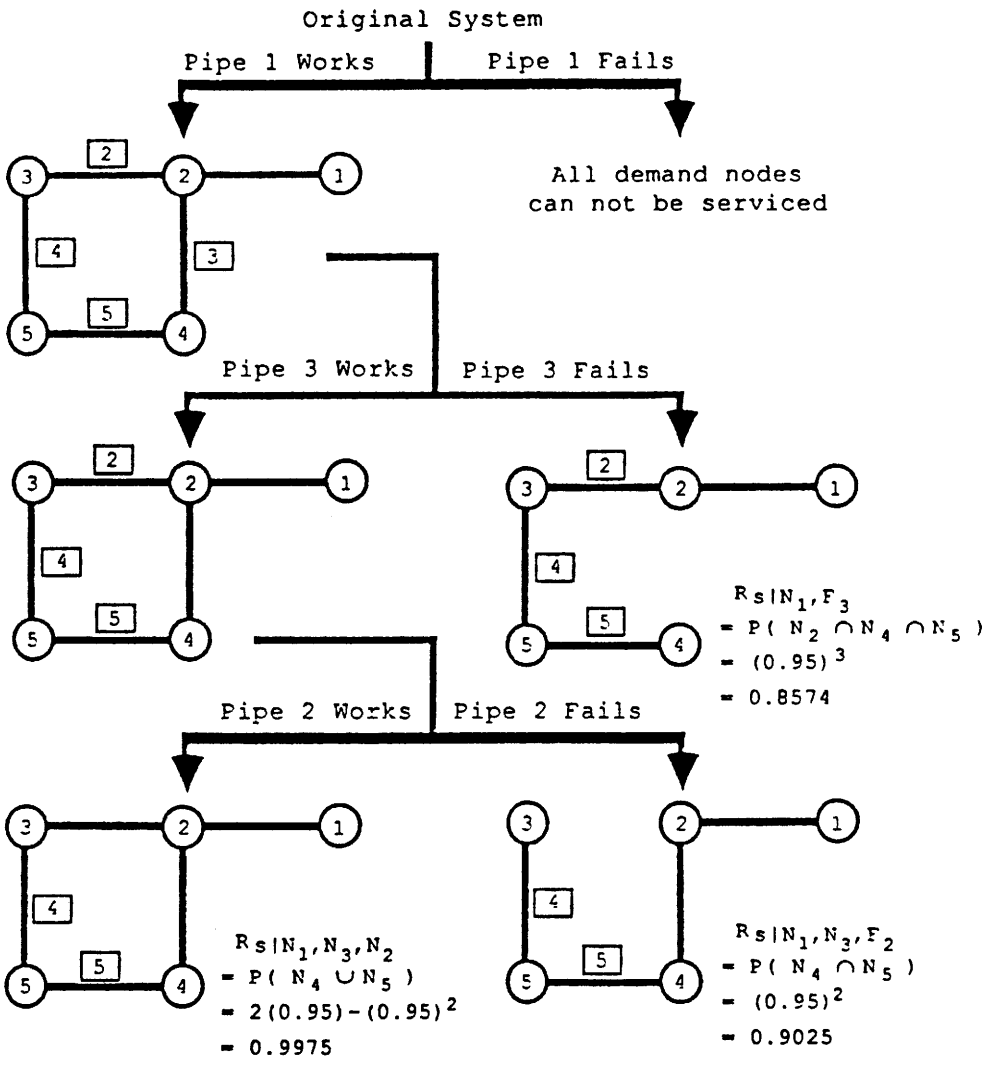


Figure 9.2.5 Illustration of Conditional Probability Method for System Reliability Evaluation

complex networks. Hwang, Tillman, and Lee also noted that Monte Carlo methods for system reliability evaluation can be used when component reliabilities are sampled by the Monte Carlo method. They also identified several miscellaneous approaches for evaluating complex systems including a moment method, a block diagram method, Bayesian decomposition, and decomposition by Boolean expression.

Hwang, Tillman, and Lee (1981) concluded that of all the evaluation techniques in the papers surveyed, only a few had limited success in solving some large complex system reliability problems and few techniques have been completely effective when applied to large system reliability problems. They suggested that a generally efficient graph partitioning technique for reliability evaluation of large, highly interconnected networks should be developed.

Since the 1981 paper of Hwang, Tillman, and Lee, several other system reliability evaluation techniques have been reported in the literature. Aggarwal, Chopra, and Bajwa (1982) presented a method that uses decomposition of a probabilistic graph using cut-sets. The method is applied to a simplified network with five nodes and seven links and only limited computational results are presented.

Bennetts (1982) presents a method for the analysis of reliability block diagrams using Boolean algebra techniques. The method is based on an analysis of path sets derived from reliability block diagrams. Boolean methods are applied to each path so that the component reliability parameters are considered to be Boolean variables rather than probabilistic variables and the whole problem is treated in a Boolean framework. Hagstrom (1983) presents a model using decomposition trees of a network based upon finding and analyzing triconnected components of the network.

Deuermeyer (1982) presented an interesting approach to network reliability analysis of flow networks that is based upon developing network functions. A network function specifies the maximum flow deliverable by the network while in a specific state. The maximum flow problem can be represented as a linear programming problem in which the objective is to maximize flow. The probability distribution of maximum flow can then be determined and used as an index of reliability.

Touey (1983) presented a new algorithm for computing network terminal reliability from a set of paths or cut-sets. This algorithm is based on selective generation of relevant states by way of methods for choosing and pruning branches of a binary tree. The author states that the method

is easy to implement and to understand, and has proven in practice to be more efficient than the fastest methods published.

9.2.6 Multistate Systems with Multistate Components

Hudson and Kapur (1982) present models for reliability analysis to systems which can have a range of states and all of its components can also have a range of multiple states. Such systems generally have various levels of operational performance so that the total system effectiveness measures reflect all the performance levels and their reliabilities. Binary system theory requires that each component, as well as the entire system, be considered either functioning or failed. Multistate approaches allow states of partial failure for both the system and its components. The advantage is that either standby or active redundancy can be considered. The methodology presented in Hudson and Kapur's paper is illustrated by a simple example of a domestic hot water system consisting of components representing a gas-fired subsystem, a solar collector-controller, two pumps, and a solar piping and storage subsystem.

This type of approach seems to be in the developmental stages and may be a little premature for application to water distribution systems. However, once the technology is developed, this should prove to be very promising. Earlier work on the multistate (discrete state) point of work was reported by Dhillon (1975), Murchland (1975), Barlow and Wu (1978), and El-Heweihi, Proschan, and Sethuraman (1978).

9.3 FAULT-TREE ANALYSIS

Fault-tree analysis has been proposed as a method for evaluating the reliability of systems. A fault tree is a logical diagram representing the consequences of the component failures (basic or primary failures) on system failure (top failure). Dhillon and Singh (1981) defined the advantages and disadvantages of the fault-tree analysis technique. Advantages include:

a. provides insight into the system behavior;

b. requires the reliability analyst to understand the system thoroughly and deal specifically with one particular failure at a time;

c. helps to ferret out failures deductively;

d. provides a visible and instructive tool to designers, users and management to justify design changes and trade-off studies;

e. provides options to perform quantitative or qualitative reliability analysis;

f. technique can handle complex systems;

g. commercial codes are available to perform the analysis.

Disadvantages include:

a. can be costly and time-consuming;

b. results can be difficult to check;

c. 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;

d. analytical solution for fault trees containing standbys and repairable components are difficult to obtain for the general case;

e. to include all types of common-cause failure requires considerable effort.

Another advantage not mentioned by Dhillon and Singh (1981) is that commercial codes are available to perform the analysis.

9.3.1 Fault-Tree Construction

Before constructing a fault tree, the analyst must thoroughly understand the system and its intended use. One must determine the higher order functional events and continue the fault-event analysis to determine their logical relationships with lower level events. Once this is accomplished, the fault tree can be constructed. A brief description of fault-tree construction is presented below. The basic concepts of fault-tree analysis are presented in Henley and Kumamoto (1981) and Dhillon and Singh (1981).

The major objective of fault-tree construction is to represent the system condition, which may cause system failure, in a symbolic manner. In other words, the fault tree consists of sequences of events that lead to system failure. There are actually two types of building blocks: gate symbols and event symbols.

Gate symbols connect events according to their casual relation such that they may have one or more input events but only one output event. Table 9.3.1 lists the various gate symbols (Henley and Kumamoto, 1981). The AND gate denotes that an output event occurs if, and only if, all the input events occur. The OR gate is an intermediate event which denotes that there is not output unless one, and only one, of the input events occur. The priority AND gate is logically equivalent to an AND gate with the exception that the input events must occur in a specific order. The inhibit gate produces output only when the conditional input is satisfied and is logically equivalent to an AND gate with two input events.

Event symbols are shown in Table 9.3.2. A fault event, denoted by a rectangular box, results from a combination of more basic faults acting through logic gates. A circle denotes a basic component failure that represents the limit of resolution of a fault tree. A diamond represents a fault event whose causes have not been fully developed. A house-shaped event denotes a fault event which is expected to occur. A triangle denotes a transfer IN or OUT and is used to avoid repeating sections of the fault tree.

There are two approaches, forward analysis and backward analysis, for analyzing causal relations. Forward analysis starts with a set of failure events and proceeds forward, looking for possible consequences resulting from the events. The backward analysis, which is used in fault-tree analysis, begins with a system hazard (failure) and traces backward, searching for possible causes of the hazard.

Henley and Kumamoto (1981) present heuristic guidelines for constructing fault trees which are summarized in Table 9.3.3 and Fig. 9.3.1, and are listed below:

a) Replace abstract events by less abstract events.

b) Classify an event into more elementary events.

c) Identify distinct causes for an event.

d) Couple trigger event with "no protection actions."

e) Find cooperative causes for an event.

f) Pinpoint component failure events.

g) Develop component failure using Fig. 9.3.1.

Table 9.3.1 Gate Symbols in Fault-Tree Analysis
(From Henley and Kumamoto, Reliability Engineering and Risk Assessment, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1981.)

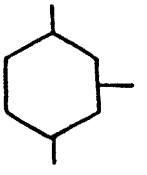
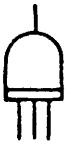
	GATE SYMBOL	GATE NAME	CAUSAL RELATION
1		AND GATE	OUTPUT EVENT OCCURS IF ALL INPUT EVENTS OCCUR SIMULTANEOUSLY.
2		OR GATE	OUTPUT EVENT OCCURS IF ANY ONE OF THE INPUT EVENTS OCCURS.
3		INHIBIT GATE	INPUT PRODUCES OUTPUT WHEN CONDITIONAL EVENT OCCURS.
4		PRIORITY AND GATE	OUTPUT EVENT OCCURS IF ALL INPUT EVENTS OCCUR IN THE ORDER FROM LEFT TO RIGHT.
5		EXCLUSIVE OR GATE	OUTPUT EVENT OCCURS IF ONE, BUT NOT BOTH, OF THE INPUT EVENTS OCCUR.
6		m OUT OF n GATE (VOTING OR SAMPLE GATE)	OUTPUT EVENT OCCURS IF m OUT OF n INPUT EVENTS OCCUR.

Table 9.3.2 Event Symbols in Fault-Tree Analysis
(From Henley and Kumamoto, Reliability Engineering and Risk Assessment, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1981.)

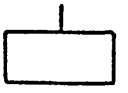
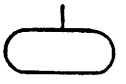
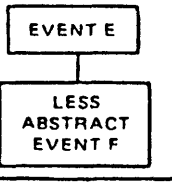
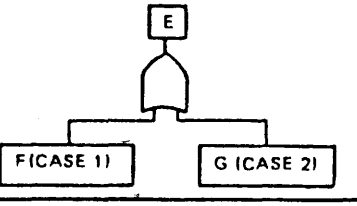
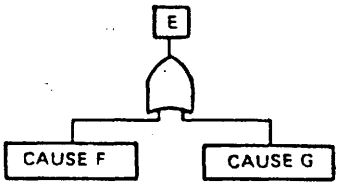
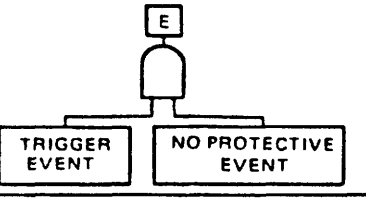
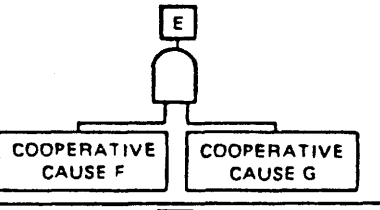
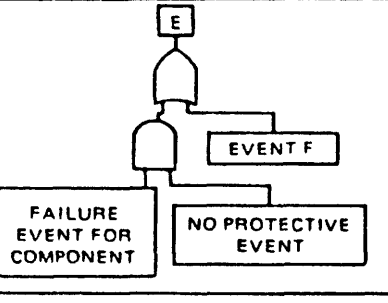
	EVENT SYMBOL	MEANING OF SYMBOLS
1	 CIRCLE	BASIC EVENT WITH SUFFICIENT DATA
2	 DIAMOND	UNDEVELOPED EVENT
3	 RECTANGLE	EVENT REPRESENTED BY A GATE
4	 OVAL	CONDITIONAL EVENT USED WITH INHIBIT GATE
5	 HOUSE	HOUSE EVENT. EITHER OCCURRING OR NOT OCCURRING
6	 TRAINGLES	TRANSFER SYMBOL

Table 9.3.3 Heuristic Guidelines for Fault-Tree Construction

(From Henley and Kumamoto, Reliability Engineering and Risk Assessment, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1981.)

	DEVELOPMENT POLICY	CORRESPONDING PART OF FAULT TREE
1	EQUIVALENT BUT LESS ABSTRACT EVENT F	
2	CLASSIFICATION OF EVENT E	
3	DISTINCT CAUSES FOR EVENT E	
4	TRIGGER VERSUS NO PROTECTIVE EVENT	
5	COOPERATIVE CAUSE	
6	PINPOINT A COMPONENT FAILURE EVENT	

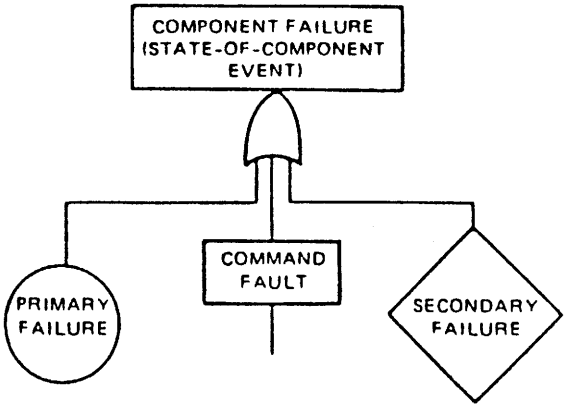


Figure 9.3.1 Development of a Component Failure
(From Henley and Kumamoto, Reliability Engineering and Risk Assessment, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1981.)

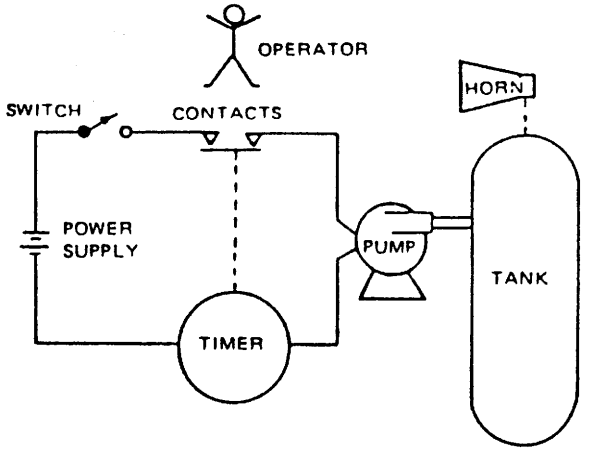


Figure 9.3.2 Schematic Diagram for an Example Pumping System
(From Henley and Kumamoto, Reliability Engineering and Risk Assessment, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1981.)

An example of a fault-tree construction is given for the system in Fig. 9.3.2. In this pumping system, the tank is filled in 10 min. and empties in 50, having a cycle time of 60 min. After the switch is closed, the time is set to open the contacts in 10 min. If the mechanism fails, then the horn sounds and the operator opens the switch to prevent pressure tank rupture. The fault tree for the pumping system is shown in Fig. 9.3.3.

9.3.3 Evaluation of Fault Trees

The basic steps used to evaluate fault trees include:

a) Construct the fault tree.

b) Determine the minimal cut-sets.

c) Develop primary event information.

d) Develop cut-set information.

e) Develop top event information.

In order to evaluate the fault tree, one should always start from the minimal cut-sets which, in essence, are critical paths. Basically, the fault-tree evaluation comprises two distinct processes: (a) the determination of the logical combination of events that cause top event failure expressed in minimal cut-sets; and (b) the numerical evaluation of the expression.

Cut-sets are collections of basic events such that if all these basic events occur, then the top event is guaranteed to occur. The path-set is a dual concept to the cut-set in that it is a collection of basic events. If none of the events in the set occur, then the top event is guaranteed not to occur. As one could imagine, a large system has an enormous number of failure modes. A minimal cut-set is one that if any basic event is removed from the set, the remaining events collectively are no longer a cut-set. By the use of minimum cut-sets, the number of cut-sets and basic events are reduced in order to simplify the analysis. Several computer codes are available for generating cut-sets, including MOCUS (Fussell, Henry, and Marshall, 1974) which was developed to obtain minimal cut-sets from fault trees.

The system availability, $A_s(t)$, is the probability that the top event does not exist at time t, which is the probability of the systems operating successfully when the top event is an OR combination of all system hazards. System unavailability, $U_s(t)$, is the probability that the top event exists at time t, which is either the probability of system failure or the

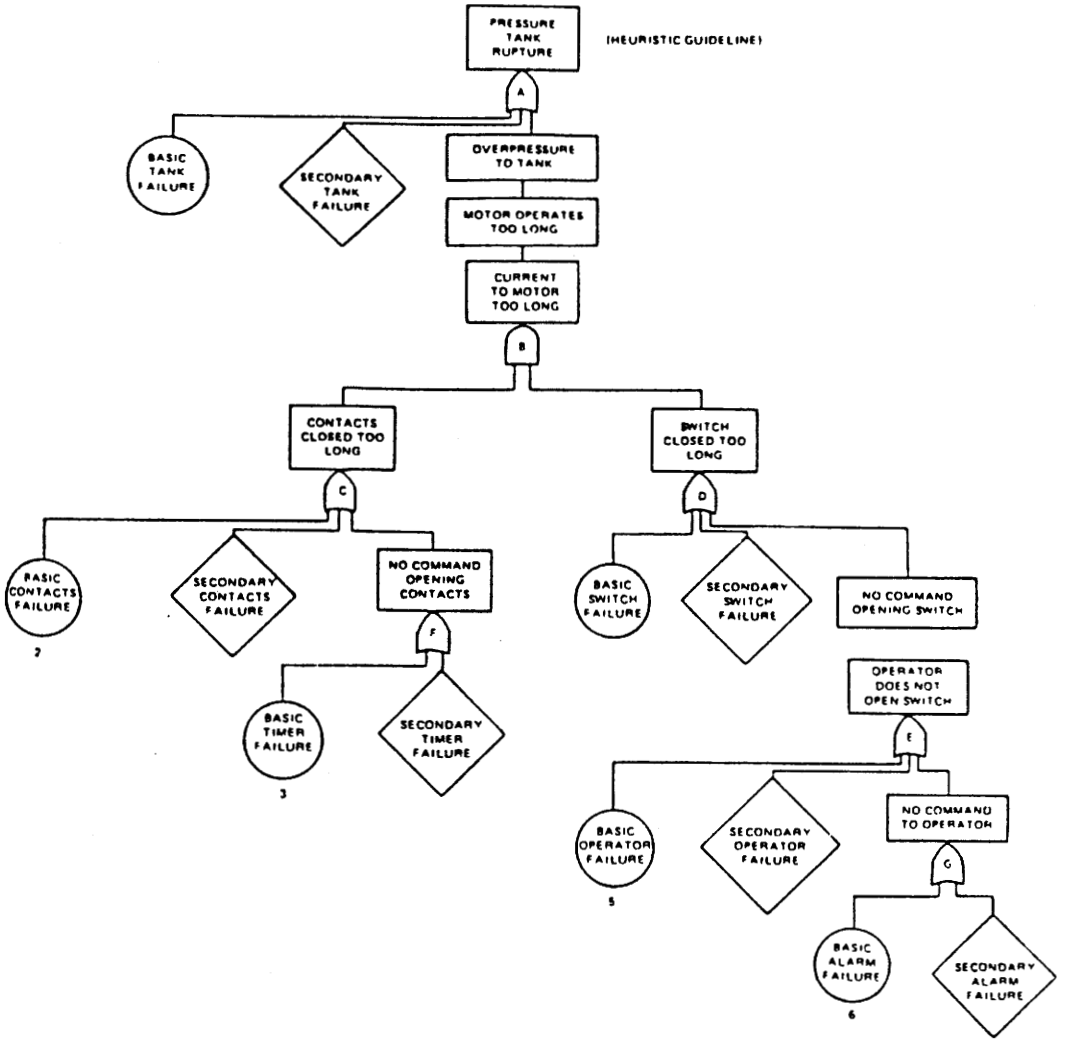


Figure 9.3.3 Fault Tree for the Example Pumping System
(From Henley and Kumamoto, Reliability Engineering and Risk Assessment, Prentice-Hall, Inc., Englewood Cliffs, N.J., 1981.)

probability of a particular system hazard at time t. The system availability and system unavailability are complementary, i.e.,

$$A_s(t) + U_s(t) = 1 \tag{9.3.1}$$

System reliability $R_S(t)$ is the probability that the top event does not occur over time interval (0,t). System reliability requires continuation of the nonexistence of the top event and the following holds

$$R_s(t) \leq A_s(t) \tag{9.3.2}$$

The system unreliability $F_S(t)$ is the probability that the top event occurs before time t and is complementary to the system reliability

$$R_s(t) + F_s(t) = 1 \tag{9.3.3}$$

and

$$F_s(t) \geq U_s(t) \tag{9.3.4}$$

The system failure density $f_S(t)$ is defined as

$$f_s(t) = \frac{dF_s(t)}{dt} \tag{9.3.5}$$

System conditional failure intensity $w_S(t)$ is the probability that the top event occurs per unit time at time t given that it does not exist at time t. The system unconditional failure intensity, $W_S(dt)$, is the probability that the top event occurs per unit time at time t. The expected number of top events during time interval (t, t + dt) is

$$W_s(t, t + dt) = \int_t^{t+dt} w_s(t)\,dt \tag{9.3.6}$$

The mean time to first failure is the expected length of time to the first occurrence of the top event and is given by

$$MTTF_s = \int_0^\infty t f_s(t)\,dt \tag{9.3.7}$$

Considering independent basic events $B_1 \ldots B_n$, the probability of a cut-set occurrence at time t, U*(t) is obtained from the intersection of the basic events as

$$U^*(t) = P(B_i \cap B_2 \cap \ldots \cap B_n) = \prod_{j=1}^{n} U_j(t) \tag{9.3.8}$$

where n is the number of cut-set members and $U_j(t)$ is the probability of the j-th basic event existing at time t. A cut-set occurrence is when all basic events in the cut-set are occurring. The asterisk (*) is used to denote that the quantity is a cut-set. The notation U(t) refers to a component unavailability, U*(t) refers to the cut-set unavailability.

The probability of occurrence of a cut-set per unit time at time t, given no cut-set failure at time t, is denoted as $\lambda^*(t)$. The probability that the cut-set occurs during the time interval (t, t + dt) is

$$\lambda^*(t)\,dt = P[C^*(t, t + dt) \mid \bar{C}^*(t)] = \frac{P[C^*(t, t + dt)]}{P[\bar{C}^*(t)]} \tag{9.3.9}$$

where

$C^*(t, t + dt)$ = occurrence of the cut-set during (t, t + dt)
$C^*(t)$ = the nonexistence of the cut-set failure at time t.

Henley and Kumamoto (1981) show that the numerator is W*(t)dt, so that

$$\lambda^*(t)\,dt = \frac{\sum_{j=1}^{n} w_j(t)\,dt \prod_{\substack{k=1 \\ k \neq j}} U(t)}{1 - U^*(t)} \tag{9.3.10}$$

Each term in the summation is the probability of the j-th basic event during (t, t + dt) with the remaining basic event existing at time t. The denominator is the probability of the nonexistence of the cut-set failure at time t.

The term W*(t) is the expected number of times the cut-set occurs per unit time at time t, defined as

$$W^*(t) = \sum_{j=1}^{n} w_j(t) \prod_{\substack{k=1 \\ k \neq j}} U_k(t) \qquad (9.3.11)$$

so that

$$\lambda^*(t) = \frac{W^*(t)}{[1 - U^*(t)]} \qquad (9.3.12)$$

Similar expressions hold for the unconditional repair intensity, i.e. v*(t)

$$v^*(t) = \sum_{j=1}^{n} v_j(t) \prod_{\substack{k=1 \\ k \neq j}}^{n} \left[1 - U_k(t)\right] \qquad (9.3.13)$$

and the conditional repair intensity u*(t),

$$u^*(t) = \frac{v^*(t)}{U^*(t)} \qquad (9.3.14)$$

The values of the expected number of failures W*(0,t) and the expected number of repairs V*(0,t) are

$$W^*(0,t) = \int_0^t w^*(h)dh \qquad (9.3.15)$$

$$V^*(0,t) = \int_0^t v^*(h)dh \qquad (9.3.16)$$

Henley and Kumamoto (1981) show that the system unavailability can be determined using

$$U_s(t) = \sum_{i=1}^{N_c} U_i^*(t) - \sum_{i=2}^{N_c} \sum_{j=1}^{i-1} \prod_{i,j} U(t) + \ldots$$

$$+ (-1)^{m-1} \sum_{1 \le i_1 < i_2 < \ldots < i_m \le N_c} \prod_{i_1 \ldots i_m} U(t)$$

$$+ \ldots + (-1)^{N_c - 1} \prod_{i_1 \ldots i_{N_c}} U(t) \qquad (9.3.17)$$

where

Π = product of U(t) for the basic events in cut-sets i_1 or i_2 ... or i_m

N_c = total number of minimal cuts

The lower and upper bounds for $Q_s(t)$ can be written as (Henley and Kumamoto, 1981)

$$\sum_{i=1}^{N_c} U_i^*(t) - \sum_{i=2}^{N_c} \sum_{j=1}^{i-1} \prod_{i,j} U(t) \le U_s(t) \le \sum_{i=1}^{N_c} U_i^*(t) \qquad (9.3.18)$$

where Π refers to the product of cut-sets i or j.

The expected number of times the top event occurs at time t, per unit time, is $w_s(t)$. Let e_i be the event that the i-th cut-set failure occurs at time t to t + dt so that $P(e_i) = W_i^*(t)dt$. For the top event to occur in time (t, t + dt), none of the cut-set failures can exist at time t and one or more must fail during the time t to t + dt, so that

$$w_s(t)dt = P\left(A \bigcup_{i=1}^{N_c} e_i\right) \qquad (9.3.19)$$

where

$$A \bigcup_{i=1}^{N_c} e_i \text{ is } A \bigcap \left(\bigcup_{i=1}^{N_c} e_i \right)$$

$\left(\bigcup_{i=1}^{N_c} e_i \right)$ = the event that one or more of the cut-set failures occur at time t

A = the event of none of the cut-set failures existing at time t

This can be reduced to (Henley and Kumamoto, 1981):

$$w_s(t) = w_s^{(1)}(t) - w_s^{(2)}(t) \tag{9.3.20}$$

where

$w_s^{(1)}(t)$ = contribution from the event that one or more cut-sets fail during time (t, t + dt).

$w_s^{(2)}(t)$ = those cases in which one or more cut-sets fail during (t, t + dt), while the other cut-sets that have already failed to time t, have not been repaired.

Computer programs have been developed to compute system parameters (unavailability, availability, expected number of failures and repairs, and conditional failure and repair intensities) given minimal cut- or path-sets of large complicated fault trees. KITT-1 (Vesely and Narum, 1970) applies the above concepts of kinetic tree theory. The program handles independent basic events which are either repairable or nonrepairable and have constant failure rates and constant repair rates u. Another version of the program, KITT-2, allows for time-varying failure and repair rates. A later version called KITT-1T (Ong and Henley, 1980) is a modified version of KITT-1 to include time delays provided by storage tanks and component (standby) redundancy.

9.4 APPLICATION AND COMPARISON OF METHODS

To demonstrate the applicability of the various techniques described in sections 9.2 and 9.3 for evaluating the reliability of a complex system, a simple water distribution network as shown in Fig. 9.4.1 is used. The distribution system involves eight pipe sections of equal length and four demand points (nodes 3, 4, 6, and 7). The system service reliability is defined as the probability that demands for all users are met. The example considers the connectivity of pipes from source to users and ignores the level of hydraulic pressure required. All pipe sections are assumed to

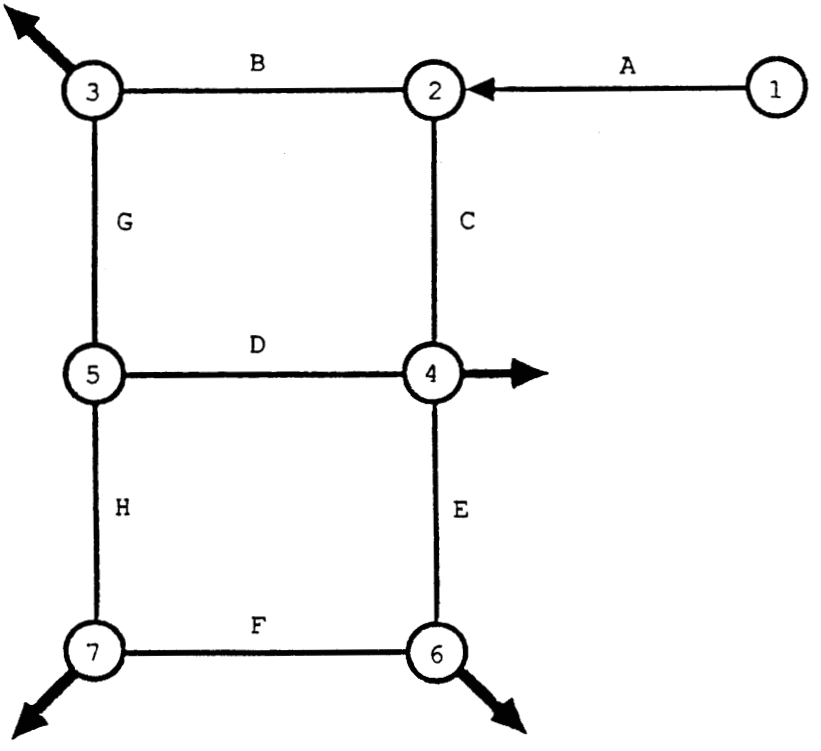


Figure 9.4.1 Example Water Distribution Network

behave independently and all have the same probability of failure of 5 percent. Using the various methods described, the service reliability of the entire system is shown in Table 9.4.1. As can be seen, the five methods considered yield practically the same system service reliability. Results obtained from the fault-tree analysis and event-tree analysis can be regarded as the true reliability. Results from the cut-set analysis is obtained by first-order approximation in that the system reliability is approximated by using only the first term of the right-hand side of equation (9.3.3). However, the result is very close to the true one. Computationally, first-order approximation of the cut-set analysis is much simpler than the other four methods considered.

Table 9.4.1 Comparison of Total System Service Reliability by Different Methods

Method	Reliability
Cut-set	0.9341
Tie-set	0.9352
Conditional Probability	0.9319
Event tree	0.9355
Fault tree	0.9354

REFERENCES

Aggarwal, K. K., Y. C. Chopra and J. S. Bajwa, "Reliability Evaluation by Network Decomposition," *Institute of Electrical and Electronics Engineers Transactions on Reliability*, Vol. R-3, No. 4, October 1982.

Banerjee, S. K. and K. Rajamani, "Parametric Representation of Probability in Two Dimension - A New Approach in System Reliability Evaluation," *Institute of Electrical and Electronics Engineers Transactions on Reliability*, Vol. R-12, p.56, 1972.

Barlow, R. E. and A.S. Wu, "Coherent System with Multistate Components," *Mathematics of Operation Research*, Vol. 3, pp. 275-281, 1978.

Bennetts, R. G., "Analysis of Reliability Block Diagrams by Bookean Techniques," *Institute of Electrical and Electronics Engineers Transactions on Reliability*, Vol. R-3, No. 2, June 1982.

Brown, D. B., "A Computerized Algorithm for Determing the Reliability of Redundant Configurations," *Institute of Electrical and Electronics Engineers Transaction Reliability*, Vol. R-20, p. 102, 1971.

Buzacott, J.A., "Network Approaches to Finding the Reliability of Repairable Systems," *Institute of Electrical and Electronics Engineers Transaction Reliability*, Vol. R-19, p. 140, 1970.

Deuermeyer, B. L., "A New Approach for Network Reliability Analysis," *Institute of Electrical and Electronics Engineers Transactions on Reliability*, Vol. R-3, No. 4, pp. 350-354, October 1982.

Dhillon, B. S., "The Analysis of the Reliability of Multistate Device Networks," Ph.D. Dissertation, University of Windsor, Windsor, Ontario, Canada, 1975.

Dhillon, B. S. and C. Singh, Engineering Reliability: New Techniques and Applications, John Wiley & Sons, New York, 1981.

El-Neweihi, E., F. Proschan and J. Sethuraman, "Multistate Coherent Systems," *Journal of Applied Probability*, Vol. 15, pp. 675-688, 1978.

Fussell, J. B., E.B. Henry and N.H. Marshall, "MOCUS - A Computer Program to Obtain Minimal Cut-Sets from Fault Trees," ANCR - 1156, 1974.

Hagstrom, J. N., "Using the Decomposition - Tree of a Network in Reliability Computation," *Institute of Electrical and Electronics Engineers Transactions on Reliability*, Vol. R-3, No. 1, April 1983.

Henley, E. J. and S.L. Gandhi "Process Reliability Analysis," *American Institute of Chemical Engineering Journal*, Vol. 21, No. 4, pp. 677-686, July 1975.

Henley, E.J. and H. Kumamoto, Reliability Engineering and Risk Assessment, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1981.

Hudson, J. C. and K.C. Kapur, "Reliability Theory for Multistate Systems with Multistate Components," *Microelectronics and Reliability,*" Vol. 22, No. 1, pp. 1-7, 1982.

Hwang, C. L., F.A. Tillman and M.H. Lee, "System Reliability Evaluation Techniques for Complex/Large Systems - A Review," *Institute of Electrical and Electronics Engineers Transactions on Reliability*, Vol. R-30, No. 5, December 1981.

Misra, K. B., "Reliability Optimization of a Series Parallel System," *Institute of Electrical and Electronics Engineers Transaction Reliability,* Vol. R-21, p. 230, 1972.

Moscowitz, F., "The Analysis of Redundancy Networks," *AIEE Transaction (Commun. Electron.),* Vol. 77, p. 627, 1958.

Murchland, J. D., "Fundamental Concepts and Relations for Reliability Analysis of Multistate System," Reliability and Fault-Tree Analysis, Theoretical and Applied Aspects of System Reliability and Safety Assessment, SIAM, Philadelphia, 1975.

Ong, J.O.Y. and E.J. Henley, "Users Manual for Code KITT-IT," Chemical Engineering Department, University of Houston, Texas, 1980.

Touey, J., "A Pruned Tree Approach to Reliability Computation," *Institute of Electrical and Electronics Engineers Transactions on Reliability,* Vol. R-32, No. 2, pp. 170-174, June 1983.

Vesely, W. E. and R.E. Narum, "PREP and KITT: Computer Codes for Automatic Evaluation of Fault Trees," Idaho Nuclear Corps., IN1349, 1970.