

Subject: Introduction to Fault Tree Analysis
Author: Jørn Vatn
Date: 2001-09-27
Rev: 1

1. Introduction

1.1 History

The fault tree technique was introduced in 1962 at the Bell Telephone Laboratories, in connection with a safety evaluation of the launching system for the intercontinental Minuteman missile. The Boeing Company improved the technique and introduced computer programs for both qualitative and quantitative fault tree analysis. Today fault tree analysis is by far the most commonly used technique of risk and reliability studies. Fault tree analysis has particularly been used with success to analyse safety systems in nuclear power stations, e.g. during the Reactor Safety Study, WASH-1400 (1974). The Fault tree analysis technique is described in e.g. the IEC standard 1025 (1990).

1.2 The fault tree technique

A fault tree is a logic diagram that displays the interrelationships between a potential critical event (accident) in a system and the reasons for this event. The reasons may be environmental conditions, human errors, normal events (events which are expected to occur during the life span of the system) and specific component failures. A properly constructed fault tree provides a good illustration of the various combinations of failures and other events which can lead to a specified critical event. The fault tree is easy to explain to engineers without prior experience of fault tree analysis.

An advantage with a fault tree analysis is that the analyst is forced to understand the failure possibilities of the system, to a detailed level. A lot of system weaknesses may thus be revealed and corrected during the fault tree construction.

A fault tree is a *static* picture of the combinations of failures and events which can cause the TOP event to occur. Fault tree analysis is thus not a suitable technique for analysing dynamic systems, like switching systems, phased mission systems and systems subject to complex maintenance strategies.

A fault tree analysis may be qualitative, quantitative or both, depending on the objectives of the analysis. Possible results from the analysis may e.g. be:

- A listing of the possible combinations of environmental factors, human errors, normal events and component failures that can result in a critical event in the system.
- The probability that the critical event will occur during a specified time interval.

The analysis of a system by the fault tree technique is normally carried out in five steps:

1. Definition of the problem and the boundary conditions.
2. Construction of the fault tree.
3. Identification of minimal cut and/or path sets.
4. Qualitative analysis of the fault tree.
5. Quantitative analysis of the fault tree.

Fault tree analysis is thoroughly described in the literature, see references in e.g., Høyland and Rausand (1994).

2. Fault tree construction

2.1 Fault tree diagram, symbols and logic

A fault tree is a logic diagram that displays the connections between a potential system failure (TOP event) and the reasons for this event. The reasons (Basic events) may be environmental conditions, human errors, normal events and component failures. The graphical symbols used to illustrate these connections are called “logic gates”. The output from a logic gate is determined by the input events.

The graphical layout of the fault tree symbols are dependent on what standard we choose to follow. The table below shows the most commonly used fault tree symbols together with a brief description of their interpretation. (Fault tree symbols as shown in Table 1 are according to LINEX 1139).

2.2 Definition of the Problem and the Boundary Conditions

This activity consists of:

- Definition of the critical event (the accident) to be analysed.
- Definition of the boundary conditions for the analysis.

The critical event (accident) to be analysed is normally called the TOP event. It is very important that the TOP event is given a clear and unambiguous definition. If not, the analysis will often be of limited value. As an example, the event description “Fire in the plant” is far too general and vague. The description of the TOP event should always answer the questions: **What, where** and **when**.

What: Describes what type of critical event (accident) is occurring, e.g. fire.

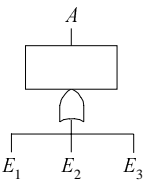
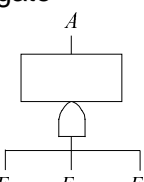
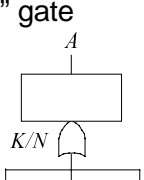
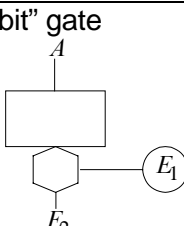
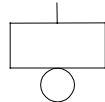
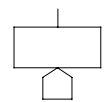
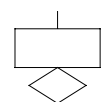



Where: Describes where the critical event occurs, e.g. in the process oxidation reactor.

When: Describes when the critical event occurs, e.g. during normal operation.

A more precise TOP event description is thus: “Fire in the process oxidation reactor during normal operation”.

To get a consistent analysis, it is important that the *boundary conditions* for the analysis are carefully defined. By boundary conditions we mean:

Table 1 Fault tree symbols.

	SYMBOL	DESCRIPTION
LOGIC GATES	<p>“OR” gate</p> 	The OR-gate indicates that the output event A occurs if any of the input events E_i occurs.
	<p>“AND” gate</p> 	The AND-gate indicates that the output event A occurs only when all the input events E_i occurs simultaneously.
	<p>“KooN” gate</p> 	The KooN-gate indicates that the output event A occurs if K or more of the input events E_i occurs.
	<p>“Inhibit” gate</p> 	The INHIBIT gate indicates that the output event A occurs if both the conditional event E_1 and the input event E_2 occur.
INPUT EVENTS	<p>“BASIC” event</p> 	The Basic event represents a basic equipment fault or failure that requires no further development into more basic faults or failures.
	<p>“HOUSE” event</p> 	The House event represents a condition or an event which is TRUE (ON) or FALSE (OFF) (not true).
	<p>“UNDEVELOPED” event</p> 	The Undeveloped event represents a fault event that is not examined further because information is unavailable or because its consequence is insignificant.
DESCRIPTION OF STATE	<p>“COMMENT rectangle</p> 	The Comment rectangle is for supplementary information.
TRANSFER SYMBOLS	<p>“TRANSFER” down</p>  <p>“TRANSFER” up</p> 	The Transfer down symbol indicates that the fault tree is developed further at the occurrence of the corresponding Transfer up symbol.

- **The physical boundaries of the system.** What parts of the system are to be included in the analysis, and what parts are not?

- **The initial conditions.** What is the operational state of the system when the TOP event is occurring? Is the system running on full/reduced capacity? Which valves are open/closed, which pumps are functioning etc.?
- **Boundary conditions with respect to external stresses.** What type of external stresses should be included in the analysis? By external stresses we here mean stresses from war, sabotage, earthquake, lightning etc.
- **The level of resolution.** How far down in detail should we go to identify potential reasons for a failed state? Should we as an example be satisfied when we have identified the reason to be a “valve failure”, or should we break it further down to failures in the valve housing, valve stem, actuator etc.? When determining the required level of resolution, we should remember that the detail in the fault tree should be comparable to the detail of the information available.

2.3 Construction of the Fault Tree

The fault tree construction always starts with the TOP event. We must thereafter carefully try to identify all fault events which are the immediate, necessary and sufficient causes that result in the TOP event. These causes are connected to the TOP event via a logic gate. It is important that the first level of causes under the TOP event is developed in a structured way. This first level is often referred to as the TOP structure of the fault tree. The TOP structure causes are often taken to be failures in the prime modules of the system, or in the prime functions of the system. We then proceed, level by level, until all fault events have been developed to the required level of resolution. The analysis is in other words deductive and is carried out by repeated asking “What are the reasons for...?”

Rules for fault tree construction

- **Description of the fault events.** Each of the Basic events must be carefully described (what, where, when) in a “rectangle”.
- **Evaluation of the fault events.** Component failures may be divided in three groups: primary failures, secondary failures and command faults.
 - A primary failure is a failure caused by natural ageing of the component. The primary failure occurs under conditions within the design envelope of the component. A repair action is necessary to return the component to a functioning state.
 - A secondary failure is a failure caused by excessive stresses outside the design envelope of the component. A repair action is necessary to return the component to a functioning state.
 - A command fault is a failure caused by an improper control signal or noise. A repair action is usually not required to return the component to a functioning state. Command faults are often referred to as transient failures.
 - The “normal” Basic events in a fault tree are primary failures identifying the equipment which is responsible for the failure. Secondary failures and command faults are intermediate events which require a further investigation to identify the prime reasons.

When evaluating a fault event, we ask the question “can this fault be a primary failure?”. If the answer is “yes”, we classify the fault event as a “normal” Basic event. If the answer is “no”, we classify the fault event as either an intermediate event which has to be further developed, or as a “secondary” Basic event. The “secondary” Basic event is often called an “Undeveloped”

event and represents a fault event that is not examined further because information is unavailable or because its consequence is insignificant.

- **The gates shall be completed.** All inputs to a specific gate should be completely defined and described before proceeding to the next gate. The fault tree should be completed in levels, and each level should be completed before beginning the next level.

3. Identification of Minimal Cut- and Path Sets

A fault tree provides valuable information about possible combinations of fault events which can result in a critical failure (TOP event) of the system. Such a combination of fault events is called a cut set.

*A **cut set** in a fault tree is a set of Basic events whose (simultaneous) occurrence ensures that the TOP event occurs. A cut set is said to be **minimal** if the set cannot be reduced without losing its status as a cut set.*

*A **path set** in a fault tree is a set of Basic events whose non-occurrence (simultaneously) ensures that the TOP event does not occur. A path set is said to be **minimal** if the set cannot be reduced without losing its status as a path set.*

For small and simple fault trees, it is feasible to identify the minimal cut- and path sets by inspection without any formal procedure/algorithm. For large or complex fault trees we need an efficient algorithm. The MOCUS algorithm (*Method for obtaining cut sets*) is described in standard FTA textbooks, and an efficient improvement of the algorithm is described by Vatn (1993).

4. Qualitative Evaluation of the Fault Tree

4.1 Conditions for Qualitative Evaluation of the Fault Tree

A qualitative evaluation of the fault tree may be carried out on the basis of the minimal cut sets. The importance of a cut set depends obviously on the number of Basic events in the cut set. The number of different Basic events in a minimal cut set is called the *order* of the cut set. A cut set of order one is usually more critical than a cut set of order two, or higher. When we have a cut set with only one Basic event, the TOP event will occur as soon as this Basic event occurs. When a cut set has two Basic events, both of these have to occur at the same time to cause the TOP event to occur.

Another important factor is the type of Basic events in a minimal cut set. We may rank the criticality of the various cut sets according to the following ranking of the Basic events:

1. Human error
2. Failure of active equipment
3. Failure of passive equipment

The ranking is based on the assumption that human errors occur more frequently than active equipment failures, and that active equipment is more failure-prone than passive equipment (an active or running pump is for example more exposed to failures than a passive standby pump).

4.2 Ranking of critical minimal cut sets

Based on this ranking, we get the ranking of the criticality of minimal cut sets of order two as shown in Table 2.

Table 2 Criticality ranking of minimal cut sets of order two.

Rank	Basic event no. 1 (type)	Basic event no. 2 (type)
1	Human error	Human error
2	Human error	Active equipment failure
3	Human error	Passive equipment failure
4	Active equipment failure	Active equipment failure
5	Active equipment failure	Passive equipment failure
6	Passive equipment failure	Passive equipment failure

5. Quantitative Analysis of the Fault Tree

5.1 Important system reliability measures

When reliability data for each of the Basic events is available, it is possible to carry out a quantitative evaluation of the fault tree. Different system reliability measures may be of interest. In Table 3 some important system reliability measures are listed.

Table 3 System reliability measures

Reliability Measure	Description
$Q_0(t)$	The probability that the TOP event occurs at time t .
$R_0(t)$	The probability that the TOP event does not occur in $[0, t)$.
MTTF	Mean time to first system failure.
Freq distr.	Distribution of TOP event frequency.
$Freq(TOP)$	Frequency of the TOP event.
$E(\#failures)$	Expected number of failures within a time period.

5.2 $Q_0(t)$ - The probability that the TOP event occurs at time t .

$Q_0(t)$ is the probability that the TOP event is occurring at time t . If the state of each component¹⁾ in the fault tree is known at time t , then the state of the TOP event can also be determined regardless of what has happened up to time t . Hence $Q_0(t)$ is uniquely determined by the $q_i(t)$'s. If all components have failure data of the category¹⁾ *on demand probability*, the $q_i(t)$'s are constant with respect to the time, hence $Q_0(t)$ is also time invariant. If at least one component in each minimal cut set has data of the category *repairable unit* or *non-repairable unit*, the corresponding $q_i(t)$'s will increase from $q_i(0) = 0$ to some asymptotic value $q_i(\infty) \leq 1$ implying $Q_0(t)$ to increase from $Q_0(0) = 0$ to $Q_0(\infty) \leq 1$.

It makes no sense to obtain values for $Q_0(t)$ when components with failure data of category *frequency* is used. Components with failure data of category *frequency* are assumed to function at time t with probability one (*duration* of occurrence equals zero). Thus minimal cut sets with such components are also assumed to function at time t with probability one.

5.3 $R_0(t)$ - The probability that the TOP event does not occur in $[0, t)$.

$R_0(t)$ is the probability that the TOP event has *not* occurred in the time period from 0 to t , i.e. the probability that the system has survived up to time t .

¹⁾ We will use the term *component* instead of *input event* because it is natural to think about the occurrence of an input event as a component failure. In other situations, e.g. when the input event represent a *human error*, this is not natural.

²⁾ The failure data categories are defined in Section 6.

In opposition to $Q_0(t)$, $R_0(t)$ does depend on what has happened up to time t , and not only the situation at time t . We will illustrate this by considering a system with two components A and B in parallel. This corresponds to two components connected with an AND-gate. The TOP event is occurring if both A and B are occurring at time t , hence

$$Q_0(t) = q_A(t) \cdot q_B(t)$$

To determine whether the TOP event does occur one or several times up to time t , it is not sufficient to know that both components have failed one or several times up to time t . This because the TOP event will *not* occur if one of the component is functioning while the other is repaired.

As a special case, when *all* components have failure data of category *non-repairable unit*, we have

$$R_0(t) = 1 - Q_0(t)$$

Generally Monte Carlo techniques or use of numerical integration is required to calculate $R_0(t)$.

5.4 MTTF - Mean time to first system failure.

MTTF is the mean time to the *first* failure of the TOP event. The MTTF is always greater or equal to the mean time *between* failures, MTBF. This is because all components are assumed to function at time t , but this assumption can not be made when the system has been restored after a system failure.

Generally Monte Carlo techniques is required to calculate MTTF.

5.5 Freq(TOP)/E(# failures)/Freq distr.

The frequency of the TOP event is the expected number of occurrences of the TOP event in a period of time, for example:

$$Freq(TOP) = 2 \text{ occurrences per year.}$$

Note that the number of occurrences of the TOP event, say X , in a given period of time, is a *random number*. We may be interested in obtaining the *distribution* of X as well as the *expected value* of X , $E(X)$. Thus the notation $Freq(TOP)$ is not always clear, in some situations we mean the distribution of X , in other situations we mean $E(X)$. The distribution of X is determined by the probabilities $P(X=0)$, $P(X=1)$, $P(X=2)$ etc., and the expected value of X is given by:

$$E(X) = \sum_{i=0}^{\infty} i \cdot P(X = i) \quad (1)$$

If the times between consecutive occurrences of the TOP event are *exponentially* distributed, then the number of failures X , in a unit period of time will be *Poisson* distributed with parameter $\lambda = 1/E(X)$ and the distribution of X is given by:

$$P(X = i) = \frac{\lambda^i}{i!} e^{-\lambda} \quad (2)$$

A common situation when the frequency of the TOP event applies, is when one and only one component in each minimal cut set has failure data of category *frequency*. As an example, consider a system with two components A and B in parallel. Component A has data of failure category *frequency*, say f_A , and component B has failure data of category *on demand probability*, say q_B . We then have:

$$Freq(TOP) = f_A \cdot q_B \quad (3)$$

This will be a typical situation when A is an undesired event and B is a barrier. Please refer to the Hand Calculation Method in Section 7.5 for further discussion of this situation.

5.6 Notations for describing reliability measures

We will end this chapter by giving an overview of the notation used when describing reliability measures. The overview is given in Table 4.

Table 4 Summary of notation

Notation	Description
$Q_0(t)$	P(the TOP event occurs at time t).
$\tilde{Q}_j(t)$	P(cut set j occurs at time t)
$R_0(t)$	P(the TOP event does not occur in $[0, t)$).
MTTF	Mean time to first system failure.
$Freq(TOP)$	Frequency of the TOP event.
$E(\#fail.)$	Expected number of failures within a time period.
$A_{0,av}(t)$	Average system availability in $[0, t)$.
$q_i(t)$	P(i 'th component is not functioning at time t).
λ_i	Failure rate, i 'th component, i.e. expected number of failures of i 'th component per hours.
f_i	Frequency of i 'th input event, i.e. expected number of occurrences of i 'th input event per hours.
τ_i	Mean time to repair, MTTR, for i 'th component (in hours).
\tilde{t}	Length of test interval for components periodically tested (in hours).
$I^B(j t)$	Birnbaum's Measure of Reliability Importance
$I^{VF}(j t)$	Vesely-Fussell's Measure of Reliability Importance.
$I^P(j t)$	Improvement Potential Reliability Measure
$I^{CR}(j t)$	Criticality Importance Reliability Measure
$I^O(j)$	Order of smallest cut set
$B_0(j)$	Birnbaum's Measure of Structural Importance.
$I^{CI}(j)$	Cut set importance of cut set j

6. Input Data to the Fault Tree

6.1 Category of failure data for input events

The crucial factors in the quantitative evaluation of the fault tree are the reliability data for the input events. The following five different categories of failure data for input events are often relevant:

- Frequency
- On demand probability
- Test interval
- Repairable unit
- Non repairable unit

In Table 5, the different categories are listed:

Table 5 Category of failure data for Input events

Category of failure data		Reliability Parameters
Code	Description	
1	House event	ON/OFF
2	Frequency	f = Frequency ¹⁾
3	On demand probability	q = Probability
4	Test interval	t* = Test interval ²⁾ , τ = Repair time ²⁾ and λ = Failure rate ³⁾
5	Repairable unit	τ = Repair time ²⁾ and λ = Failure rate ³⁾
6	Non repairable unit	λ = Failure rate ³⁾

1) Expected number of occurrences per hour.

2) To be specified in hours.

3) Expected number of failures per hour.

6.2 Frequency

This category is used to describe events occurring now and then, but with no duration. Thus the *probability* that the event is occurring at time t , $q_i(t) = 0$.

Note! If there is a *duration* of the event, the event should be described as a *repairable unit*, where the failure rate equals the frequency of the event, and the repair time equals the duration.

6.3 On demand probability

This category is usually used to describe components which is *not* activated during normal operation. The component is demanded only now and then. The reliability data represents the probability that the component is not able to perform its function upon request. In safety systems, the *operator* is often modelled by an *on demand probability*, for example: *Operator fails to activate manual shut-down system*.

6.4 Test interval

This category is used to describe components which are tested periodically with test interval t^* . A failure may occur anywhere in the test interval. The failure will, however, not be detected until the test is carried out or the component is needed. This is a typical situation for many types of detectors, process sensors and safety valves. The probability $q_i(t)$ in this situation often referred to as the mean fractional dead-time, MFDT. The reliability parameters entered are the failure rate λ , the test interval t^* (in hours) and the repair time τ . The MFDT may be approximated by the formula:

$$q_i(t) \approx \frac{\lambda t^*}{2} + \frac{\tau}{t^*} \quad (4)$$

Note that this formula only is valid if we have *independent* testing of each component. If components are tested *simultaneously*, or if we have *staggered* testing, this formula will not be correct.

6.5 Repairable unit

The component is repaired when a failure occurs. If the failure rate is denoted λ and the mean time to repair (MTTR) is denoted τ , and $q_i(t)$ may be calculated by the formula:

$$q_i(t) = \frac{\lambda \tau}{1 + \lambda \tau} \left(1 - e^{-\frac{(1 + \lambda \tau)t}{\tau}} \right) \quad (5)$$

Note that by letting t tend to infinity, we obtain the well-known approximation:

$$q_i(t) = \frac{MTTR}{MTTR + MTTF} \quad (6)$$

where

$$MTTF = \frac{1}{\lambda} \quad (7)$$

6.6 Non repairable unit

The component is not repaired when a failure occurs. If the failure rate of the component is denoted by λ , then:

$$q_i(t) = 1 - e^{-\lambda t} \quad (8)$$

7. TOP Event Calculations

7.1 Methods for calculation of different reliability measures

7.2 $Q_0(t)$ - The TOP Event Probability

The probability of the TOP event is denoted by

$$Q_0(t) = P(\text{"The TOP event is occurring at time } t\text{"})$$

For a given point in time t , the value of $Q_0(t)$ of course depends on the structure of the fault tree and of the probabilities of occurrence of the input events at time t .

7.2.1 Upper Bound Approximation for $Q_0(t)$

The following formula provides an upper bound for $Q_0(t)$, and is usually a satisfactory approximation to $Q_0(t)$.

Let the minimal cut sets of the tree be denoted K_1, K_2, \dots, K_k . By the assumption of independence of input events, the probability that all input events in the minimal cut set K_j occur, is

$$\tilde{Q}_j(t) = \prod_{i \in K_j} q_i(t) \quad (9)$$

If the cut sets were disjoint, then they would be stochastically independent and we would have

$$Q_0(t) = 1 - \prod_{j=1}^k (1 - \tilde{Q}_j(t)) \quad (10)$$

In general, however, the minimal cut sets are not disjoint. In this case it may be shown that we always have

$$Q_0(t) \geq 1 - \prod_{j=1}^k (1 - \tilde{Q}_j(t)) \quad (11)$$

and that in fact $Q_0(t)$ approximately equals the right hand side of (11) at least when the $q_i(t)$'s are close to 0.

It should be noted that the inequality (11) for $Q_0(t)$ is also applicable when the input events in the fault tree are positively dependent (so-called *associated*) rather than independent.

7.2.2 Exact Calculation of $Q_0(t)$; the ERAC Algorithm

The upper bound approximation presented in section 7.2.1 may in some situations be rather inaccurate. A number of alternatives have therefore been proposed. One of these alternatives is the ERAC algorithm (Exact Reliability/Availability Calculation) which was developed by Aven (1985).

7.3 Calculation of $R_0(t)$, MTTF and $Freq(TOP)$ Using Simulation

The reliability function for the TOP event is defined as

$$R_0(t) = P(\text{"TOP event has not occurred in the time interval } [0,t]\text{"})$$

where it is assumed that the system is perfect at time 0, i.e. no input events have occurred by time 0.

Thus $R_0(t)$ is the *survival function* of the system with respect to the non-occurrence of TOP event. The function $R_0(t)$ should not be confused with the function $U_0(t) = 1 - Q_0(t)$, which is the probability that the TOP event does not occur at time t , *without regard to whether the TOP event has occurred or not before time t* . Thus we always have $R_0(t) \leq 1 - Q_0(t)$.

A lower bound for $R_0(t)$ is obtained by putting all repair times equal to infinity and computing the resulting " $Q_0(t)$ " by one of the methods described above.

Generally one may obtain an estimate of the exact value of $R_0(t)$, together with other information from a Monte Carlo simulation. The user then has to specify the time interval $[0,t]$, and the number of runs.

Each run constitutes a simulated realisation of the system performance in the time interval $[0,t]$, and the times of occurrences of the TOP event are recorded for each run. The results are, after all runs have been done, summarised to obtain estimates for

- $R_0(t)$
- MTTF (= mean time to first occurrence of the TOP event)
- Frequency distribution for the number of occurrences of the TOP event in $[0,t]$
- $A_{0,av}(t)$ (= system availability in $[0,t]$)

$R_0(t)$ is estimated as the relative number of runs with no TOP event occurring in $[0,t]$.

The simulation procedure is not of interest for *static* fault trees, i.e. fault trees for which the $q_i(t)$ do not depend on t . Thus the analysis is restricted to *dynamic* trees, i.e. fault trees for which each minimal cut set contains at least one input event i with $q_i(t)$ depending on t .

The Monte Carlo simulation gives inaccurate values for very reliable systems. If reliable systems are considered, the numerical integration method described below should be used.

7.4 Calculation of $R_0(t)$, MTTF and $E(\#failures)$ Using Numerical Integration

We will now present a method for obtaining TOP event measures by using numerical integration. The method is due to Vesely *et.al* (1981), who also wrote the computer program KITT where this method was implemented. This method is also referred to as Kinetic Tree Theory, KTT.

As in Section 7.2.1 we denote the minimal cut sets by K_1, K_2, \dots, K_k . The probability of occurrence of cut set K_j is:

$$\tilde{Q}_j(t) = \prod_{i \in K_j} q_i(t) \quad (12)$$

Now introduce

$w_i(t)$ = failure frequency of the i 'th component
 $w_{K_j}(t)$ = failure frequency of cut set K_j
 $w_0(t)$ = system failure frequency

The system failure density can now be obtained by:

$$w_0(t) = \sum_{j=1}^k \frac{\partial Q_0(t)}{\partial \tilde{Q}_j(t)} w_{K_j}(t) \quad (13)$$

where

$$\frac{\partial Q_0(t)}{\partial \tilde{Q}_j(t)} \approx 1 - \sum_{\substack{l=1 \\ l \neq j}}^k \tilde{Q}_l(t) \quad (14)$$

and

$$w_{K_j}(t) = \sum_{i \in K_j} \frac{\tilde{Q}_j(t)}{q_i(t)} [1 - q_i(t)] \lambda_i \quad (15)$$

(λ_i is the failure rate for the i 'th component, thus we do not sum for components with *on demand* failure data)

The system failure rate is defined by

$$\lambda_0(t) = \frac{w_0(t)}{1 - Q_0(t)} \quad (16)$$

Finally we find by (numerical) integration:

$$R_0(t) = e^{-\int_0^t \lambda_0(\tau) d\tau} \quad (17)$$

$$MTTF = \int_0^\infty R_0(t) dt \quad (18)$$

$$E(\text{no. fail up to } t) = \int_0^t w_0(\tau) d\tau \quad (19)$$

The above formulas only applies to very reliable systems. For unreliable systems, the formulas are inaccurate, and simulation should be considered.

7.5 Calculation of *Freq*(TOP) Using the Hand Calculation Method

The hand calculation method can be used to obtain the frequency of the TOP event. In the situation where each minimal cut set contains one and only one component with data type “frequency” and the remaining component in each cut set is of type “on demand probability” the formula is given by:

$$Freq(TOP) = \sum_{\text{all cut sets } K_j} \left\{ f_{k_j} \cdot \prod_{\substack{i \in K_j \\ i \neq k_j}} q_i(t) \right\} \quad (20)$$

where f_{k_j} is the frequency of the input event with “frequency” data in cut set K_j , and $q_i(t)$ is the probability that input event i in cut set K_j occurs at time t .

In the general situation the following formula may be used:

$$Freq(TOP) = \sum_{\text{all cut sets } K_j} \left\{ \sum_{i \in K_j} \lambda_i \prod_{\substack{l \in K_j \\ l \neq i}} q_l(t) \right\} \quad (21)$$

where λ_i is the frequency/failure rate of component i and $q_l(t)$ is the probability that input event l occurs at time t .

8. Measures of Importance

The reliability importance of a component in a system will generally depend on the location of the component in the system, and the reliability of the component. In the following we will describe some measures which quantify this relation. A number of different measures have been defined, and in this presentation the following measures will be described:

- Vesely-Fussell's measure of reliability importance.
- Birnbaum's measure of reliability importance.
- Improvement potential.
- Criticality Importance.
- Order of smallest cut set
- Birnbaum's measure of structural importance.

8.1 Vesely-Fussell's Measure of Reliability Importance

Vesely-Fussell's measure of reliability importance for component i is defined by:

$I^{VF}(i|t_0)$ = the conditional probability that at least one minimal cut set containing input event no. i is failed at time t_0 , given that the system fails at time t_0 .

(We say that a minimal cut set fails if all the input events in the set occur).

The following approximation, which is usually good, may be used to compute I^{VF} :

$$I^{VF}(i|t) \approx \frac{\sum_{j=1}^{m_i} \tilde{Q}_j^i(t)}{Q_0} \quad (22)$$

where the upper index i means that, in the numerator, only the minimal cut sets containing input event no. i are considered. Then m_i is the number of minimal cut sets containing input event no. i . Vesely-Fussell's measure of importance can be interpreted as the probability that the TOP event is caused by input event no. i , when it is given that the TOP event has occurred. Then by saying that "the TOP event is caused by input event no. i ", we mean that input event no. i occurs and the rest of the input events in the fault tree are in such states that the TOP event occurs if and only if input event no. i occurs.

8.2 Birnbaum's Measure of Reliability Importance

Birnbaum's measure of reliability importance for component i is defined as follows:

$I^B(i|t)$ = the partial derivative of $Q_0(t)$ with respect to $q_i(t)$

Thus an increase of $q_i(t)$ by a (small) amount a_i , say, will increase $Q_0(t)$ by an amount (approximately) a_i times $I^B(i|t)$.

In order to calculate Birnbaum's measure of reliability importance we may introduce another interpretation:

$$I^B(i|t) = P(\text{“TOP-event occurs at } t_0\text{”} \mid q_i(t)=1) - P(\text{“TOP-event occurs at } t\text{”} \mid q_i(t)=0) \quad (23)$$

i.e. the difference between the probabilities of the TOP-event computed under the assumptions that input event no. i is known to occur and is known to not occur, respectively. This difference may be interpreted as the probability that input event no. i is *critical* at time t .

To give a simple example, consider a parallel system of two components. Then, for the TOP-event “system failure” we have $Q_0(t) = q_1(t)q_2(t)$, so

$$I^B(1|t) = q_2(t), \quad I^B(2|t) = q_1(t).$$

8.3 Improvement potential

The improvement potential reliability measure for component i is defined by:

$I^{IP}(i|t)$ = the increase in system reliability if component i is replaced with a perfect component at time t .

The improvement potential measure is related to Birnbaums measure by:

$$I^{IP}(i|t) = I^B(i|t) \cdot q_i(t)$$

8.4 Criticality Importance

The criticality importance reliability measure for component i is defined by:

$I^{CR}(i|t)$ = the probability that component i is critical for the system and is failed at time t , given that the system is failed at time t .

The criticality importance measure is related to Birnbaums measure by:

$$I^{CR}(i|t) = \frac{I^B(i|t) \cdot q_i(t)}{Q_0(t)}$$

8.5 Order of smallest cut set

The order of smallest cut set importance measure is defined by:

$I^O(i)$ = The order of the smallest cut set containing component i

Note that this is a qualitative measure that does not depend on the component reliabilities.

8.6 Birnbaum’s Measure of Structural Importance

Birnbaum’s measure of structural importance for component i is defined as follows:

$B_\phi(i)$ = the relative number of system states for which component i is **critical** for the system.

Component i is *critical* if the state of the system is such that the system functions if and only if component i functions. A more precise definition of this measure is:

$$B_{\phi}(i) = \frac{\eta_{\phi}(i)}{2^{n-1}} \quad (24)$$

where $\eta_{\phi}(i)$ is the total number of *critical path vectors* for component i . A critical path vector for component i is a state vector of the other components in the system such that the system functions if and only if the i 'th component functions. The idea behind this measure is to count the relative number of different states of the system (all *other* components than i) which cause component i to be *critical* for the system.

It can be shown that if all components have $q_i(t) = 0.5$, then $B_{\phi}(i) = I^B(i)$.

8.7 Cut set importance

The cut set importance for cut set j is defined by

$I^{Cj}(j) =$ the conditional probability that at minimal cut set $\{ XE \text{ "Cut set" } \}$ $XE \text{ "Cut set" } \}$ j is failed at time t , given that the system is failed at time t .

Cut set importance is calculated by the formula

$$\frac{\prod_{i \in K_j} q_i(t)}{Q_0(t)} \quad (25)$$

where $Q_0(t)$ is the probability that the TOP event is occurring at time t .

9. References

- T. Aven. Reliability/Availability Evaluations of Coherent Systems Based on Minimal Cut Sets. *Reliability Engineering*, 12:93-104, 1985.
- A. Høyland and M. Rausand. *Reliability Theory; Models and Statistical Methods*. John Wiley & Sons, New York, 1994.
- IEC 1025. *Fault tree analysis (FTA)*. International Electrotechnical Commission, Geneva, 1990.
- SAE ARP 926. *Fault/Failure Analysis Procedure (Aerospace Recommended Practice)*. Society of Automotive Engineers, 400 Commonwealth Drive, Warrendale, PA.15096, 1979.
- J. Vatn. Finding minimal cut sets in a fault tree. *Reliability Engineering and System Safety*, 36:59-62, 1992.
- W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl. *Fault Tree Handbook*. U.S. Nuclear Regulatory Commission, NUREG-0492, Systems and Reliability Research, Washington, D.C. 20555, USA, 1981.
- WASH-1400. Reactor Safety Study. US Nuclear Regulatory Commission, NUREG-75/014, 1975.