ANNEX B: ELEMENTS OF RELIABILITY THEORY AND APPLICATIONS TO SAFETY ANALYSIS

B.1 INTRODUCTION

The aim of this chapter is to provide the main tools for understanding the application of the techniques of reliability on safety studies. Therefore, after recalling the **definition of the main variables** used in the reliability analysis, the focus will be on assessing **the reliability of components and systems, simple or complex**. It will also briefly examined a crucial aspect for applications: the common causes of failure and human error.
Obviously we are not going to do a full discussion of the reliability theory and application techniques to the analysis of complex systems, but only introduce this theme, with sufficient understanding of its use in the safety analysis. For further information and more details, see the books mentioned in the references.

B.2 DEFINITIONS

Failure rate λ (t): fraction of components that fail per unit of time;
Reliability R (t): probability that an apparatus performs the task assigned in a specific time interval (0-t), under certain environmental conditions;
Unreliability Q (t): probability that the equipment has failed during the considered time interval (0-t) (it does not carry out the function assigned at the instant t, for a fault occurred at any instant in the interval 0 -t);
Availability A (τ): probability that the system is operating properly during the mission time τ;
Unavailability I (τ): probability that the system is not able to perform its function during the mission time τ, namely fraction of τ for which, an average, the system is defective (Relative Dead Time).

B.3 CLASSIFICATION OF COMPONENTS FAILURES

To determine the reliability of components produced industrially in large quantities (eg. electrical components, such as resistors,

capacitors, transistors, etc.), we can do an experiment, putting them into operation simultaneously in a large number N_0 in the same conditions, according to the manufacturer's specifications (see Fig. B.1).
As shown in the upper part of Fig. B.1, the number of components in operation is reduced rapidly in the initial stage of the experiment; then the rate of decrease is stabilized for a long period of time to a minimum value, while it returns to increase towards the end of the life of the components. The graph shows clearly the three periods mentioned above, and their name:
0 - t1, "**trial stage**";
t1 - t2, "**useful life**";
> t2, "**usury**" or "**old age**."

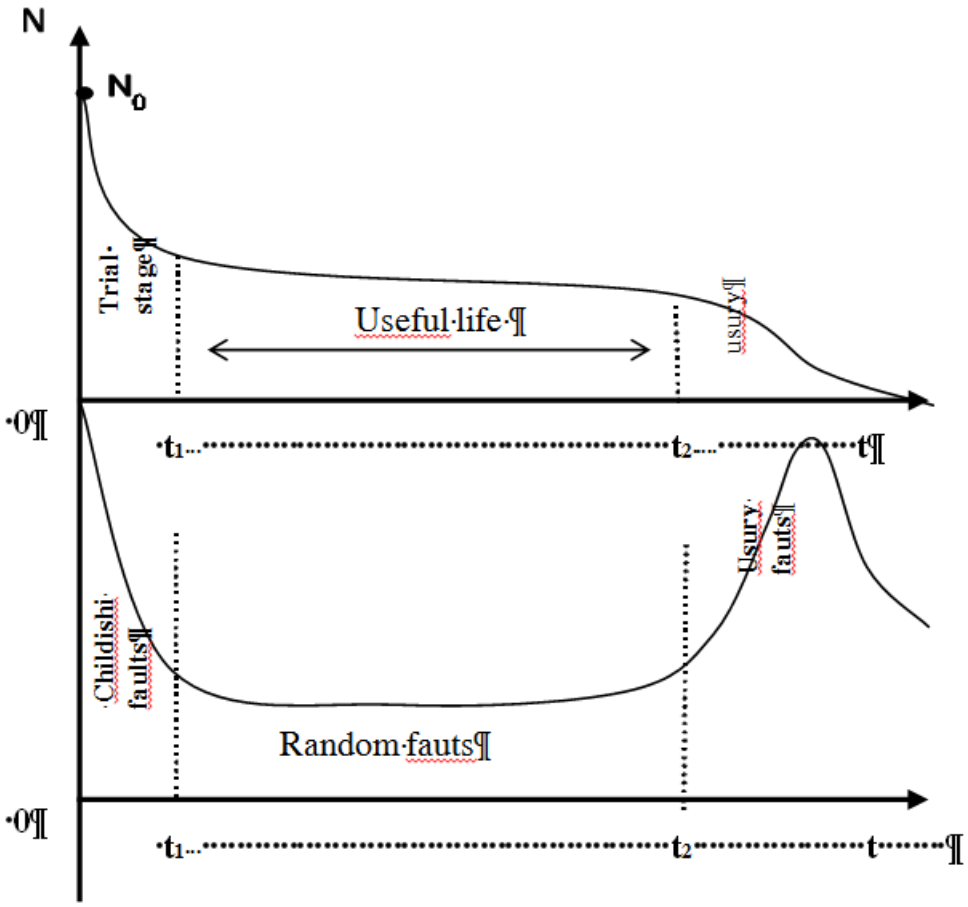


Fig. B.1 Periods characteristic of operation and corresponding failure classification of the components

According to the definition given in the previous paragraph, you can easily draw the trend of the corresponding failure rate λ as a function

of time, shown in the lower part of the same Fig. B.1, It is the well-known curve "bathtub", leading to the classification component failures in:
"**childish**", due to defects and imperfections of construction that are evident readily during the break-in period, leading to the exclusion from the use of components that are affected;
"**random**", during the period of useful life, corresponding to a rate of fault minimum and almost constant;
"**usury**", during the corresponding period and due to the deterioration of the characteristics of the component by the stresses to which has been subjected during operation.

Previous observations imply that for optimum reliability, it is necessary to make a proper break-in components, using the same only during the period of useful life; consequently it is also necessary to perform maintenance operations programmed, by replacing the components which have reached the end of their useful life. Only by doing so you can rely on a minimum and also almost constant, in time, failure rate for the components used.

B.4 ASSESSMENT OF COMPONENTS RELIABILITY

B.4.1 Non repairable components

Assuming, as usual engineering practice, that is possible to approximate the probability with the observed frequency (hypothesis acceptable if the statistical basis is sufficiently wide), the reliability is given by the relation:

$$R(t) = N / N_0 \qquad (B.1)$$

where N is the number of components "survivors" at time t, and N_0 is the initial number of components at the time t=0.

Similarly, the unreliability is expressed by the relation:

$$Q(t) = 1-R(t) = N_g / N_0 \qquad (B.2)$$

where N_g is the number of failed components between the initial instant and the generic time t.

Note that the two relationships listed above are valid for **non-repairable** components, or that, once they faults, remain in a state of failure for the whole duration of the observation.
The definition of the failure rate can be expressed with the relationship:

$$\lambda = \frac{1}{N}\frac{dN}{dt} \qquad \text{(B.3)}$$

from which, according to (1) is immediately obtained:

$$\lambda = -\frac{1}{R}\frac{dR}{dt} \qquad \text{(B.3')}$$

Solving:

$$R = \exp\left(-\int_0^t \lambda dt\right) \qquad \text{(B.4)}$$

and under the assumption that λ is constant over time:

$$R = e^{-\lambda t} \simeq 1-\lambda t \qquad \text{if } \lambda t << 1 \qquad \text{(B.4')}$$

According to the fundamental theorem of probability theory we therefore have:

$$Q(t) = 1 - e^{-\lambda t} \simeq \lambda t \qquad \text{if } \lambda t << 1 \qquad \text{(B.5)}$$

In the study of a system composed of non-repairable components (eg. missile, etc.), the probability that the system fails during the mission time τ will be given by $Q(\tau)$. Furthermore:

$$A(\tau) = R(\tau) \quad \text{and} \quad I(\tau) = Q(\tau) \qquad \text{(B.6)}$$

The assumption of constant (and minimum) failure rate is generally valid for units ([1]) that have been passed the break-in period (elimination of defects "childish", namely due to defects in the construction, trivial errors, etc.) and are used during the period of "useful life", before they will overtake the usury. Using always process units in the period of useful life (and then by making systematic and scheduled maintenance, with units replacement at the end of their useful life), the mean time between failure period (**MTBF - Mean Time Between Failures**) is:

MTBF = 1/τ (B.7)

More generally one can demonstrate the validity of the following relationship:

$$MTBF = \int_0^\infty R(t)\,dt \qquad \text{(B.8)}$$

valid whatever the mathematical expression of R (t).
The previous definitions and relationships extends easily to the case of process units with cyclic operation, with the replacement of the MTBF with the average number of cycles of correct operation "c" (to be put in previous relationship (B.7) in place of 1 / τ).

B.4.2 Repairable components

Differently from the previous case (and most interest cases for the industry), the failing component is usually repaired (or replaced) and put back into operation. In this case, it becomes important the concept of **Mean Time To Repair (MTTR)**, namely the time interval during which the component remains in a fault state.
Similarly to the failure rate, it can be defined a repair rate m:

m = 1/MTTR (B.9)

For repairable components the availability is therefore defined as:

1 In this chapter, the term "unit" is meant indifferently component, equipment or system.

A = MTBF / (MTBF + MTTR) (B.10)

and analogously the unavailability as:

I = 1 - A = MTTR / (MTBF + MTTR) = $\frac{\lambda}{\lambda + \mu}$ (B.11)

B5 RELIABILITY OF PROTECTION AND SAFETY SYSTEMS

For equipment and systems devoted to protection and safety, it is necessary to premise a further classification of types of failure:

- **faults in favor of safety** (fail safe), namely involving the intervention of the unit in the absence of a dangerous situation. In consequence of an intervention "fail safe", the plant changes state from that of normal operation to a situation of greater safety. This automatically reveals the failure of the unit.
- **faults to the detriment of safety** (fail to danger), which involve the non-availability of a unit in the event that it be called to operate as a result of a failure (demand) of the process system.

The faults fail to danger can be **revealed** (and in such case promptly repaired) or **not revealed**; in the latter case they can be detected only by a request of the process system (which cannot be satisfied and therefore result in an incident) or from an ad hoc test at the end of the mission time. Clearly, as the risk of incidents arises mainly from occurrence of faults fail to danger, the designer puts a certain cure in minimizing the relative failure rate, particularly for faults not revealed.

We have already mentioned that an incident in a highly dangerous plant occurs only for the concomitant occurrence of a fault in the system process (demand) and the failure of the system for protection and safety. Hence the definition of "**unavailability**" of a safety and protection system such as **probability of non-intervention following a request of the process system**. In this way the probability of occurrence of an accident is given by the product of the probability of failure of the process system for the unavailability of the protection system.

For protection system failures "fail to danger" unrevealed, it is easily to demonstrate that the unavailability for a mission time τ (interval between two successive tests, which can reveal the faulted protection system) is given by:

$$I = \frac{1}{\tau}\int_0^{\tau} Q(t)\,dt \qquad \text{(B.12)}$$

Ultimately this relation expresses the fact that I is the average value of Q (t) within the mission time. I is also equal to the Relative Dead Time, namely the fraction of the time τ for which on average the protection system is broken:

$$I = \frac{1}{\tau}\int_0^{\tau} (\tau - t)\,dQ \qquad \text{(B.13)}$$

In the previous relation dQ is the probability that the protection system fails at a generic instant t, in which case remains faulted for the remaining interval (t-τ).
In the case of a protection system with exponential reliability:

$Q(t) = 1 - e^{-\lambda t} \simeq \lambda t$ if $\lambda t << 1$

and:

$$I = \frac{1}{\tau}\int_0^{\tau} (1 - e^{-\lambda t})\,dt \simeq \frac{1}{\tau}\int_0^{\tau} \lambda t\,dt = \frac{1}{2}\lambda\tau \qquad \text{(B.14)}$$

In the previous expression it is implicitly admitted that the tests are all perfect and of infinitesimal duration (namely negligible compared to τ). With this hypothesis would be sufficient to reduce the time interval between two tests to reduce accordingly, as you want, the unavailability of the protection system, in accordance with (B.14). At the limit, by tending τ to zero, I also tends to zero, against the obvious conclusion that if a system of protection is constantly under test, it is never available to perform its function (and therefore has unavailability equal to 1).
Introducing the test duration τ_t (and including in τ_t the repair time when the test reveals a fault), the previous relationship becomes:

$$I = \frac{1}{2}\lambda\tau + \frac{\tau_t}{\tau} \qquad \text{(B.15)}$$

given the fact that during the test the system is not available and its Q is 1. The latter relationship is suitable to an optimization of the interval between two successive tests; The minimum is obtained deriving equation (B.15) and putting the derivative to 0:

$$\frac{dI}{d\tau} = \frac{1}{2}\lambda - \frac{\tau_t}{\tau^2} = 0 \qquad \text{(B.16)}$$

from which:

$$\tau_0 = \sqrt{\frac{2\tau_t}{\lambda}} \qquad \text{(B.17)}$$

By substituting this optimum mission interval in (B.15), we have:

$$I_m = \lambda\tau_0 = \sqrt{2\lambda\tau_t} \qquad \text{(B.18)}$$

Previous conclusion is consequence of the hypothesis of perfect testing (which do not introduce faults). This hypothesis can be removed, assuming that λ is function of the number of tests and increases by increasing the number of tests:

$$\lambda = \lambda_0 \cdot f(\tau) \qquad \text{(B.19)}$$

The simplest expression for (B.19) is

$$\lambda = \lambda_0 \cdot \left(1 + \frac{K}{\tau}\right) \qquad \text{(B.19')}$$

that, by substituting in (B.16), leads to the relationship:

$$I = \frac{1}{2}\lambda_0\tau + \frac{\tau_t}{\tau} + \frac{K\lambda_0}{2} \qquad \text{(B.20)}$$

To conclude this section we have to treat the case of a system malfunction fail to danger revealed. The solution of the problem is immediate, remembering that unavailability is equal to the Relative Dead Time and therefore the relationship (B.11) holds, already seen in the case of repairable parts. In addition it is implicit the assumption that the plant continues to be operated during the repair time. In the case of installations with a high hazard, this can be admitted only if

there are other safety systems capable of carrying out the function performed by the system under repair.

B.6 RELIABILITY ASSESSMENT OF 'SIMPLE SYSTEMS

The most common cases of reliability and unavailability calculation, in the field of safety reporting, are those schematized with the series and parallel logics. Any case also other logics are used, as the majority and reserve ones.

B.6.1 System with series logic (Fig. B.2)

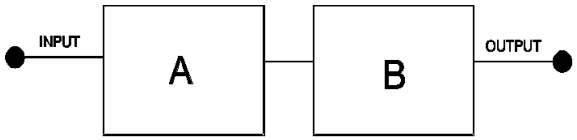


Fig. B.2 - Scheme of a system with series logic

In the case of non-repairable components, the reliability of the system as function of time t is given by:

$$R_S = R_A \cdot R_B \qquad (B.21)$$

and the unreliability by:

$$Q_S = Q_A + Q_B - Q_A\, Q_B \qquad (B.22)$$

More broadly in the case of N units, as to have the correct operation of the system it is necessary that all the units are working properly, the reliability of the system is simply given by the product of the reliability of the individual units:

$$R_S = \prod_{i=1}^{N} R_i \qquad (B.21')$$

If the single units have exponential reliability, the system also has exponential reliability, with a failure rate equal to the sum of those of the individual units; in fact the (B.21') becomes:

$$R_S = \prod_i e^{-\lambda_i t} = exp(-t\sum_i \lambda_i) = e^{-\lambda_S t} \qquad \text{(B.21'')}$$

where:

$$\lambda_S = \sum_i \lambda_i \qquad \text{(B.23)}$$

B.6.2 System with parallel logic (Fig. B.3)

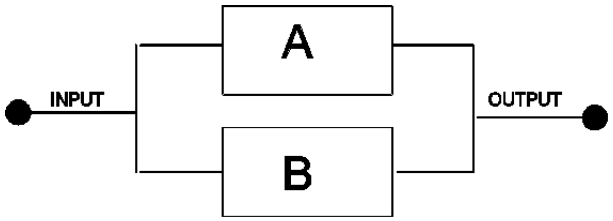


Fig. B.3 - Scheme of system with parallel logic

In the case of non-repairable components, the reliability of the system at time t is given by:

$$R_P = R_A + R_B - R_A * R_B \qquad \text{(B.24)}$$

and the unreliability by:

$$Q_P = Q_A * Q_B \qquad \text{(B.25)}$$

Here, it is necessary that all the units that constitute the system (and are working simultaneously with the capacity of achieving the system goal even though only one unit is functioning regularly) fail for having a situation in which the system does not perform its functions.
In case of n units with parallel logic:

$$Q_p = \prod_{i=1}^{n} Q_i \qquad \text{(B.25')}$$

If all the units have exponential reliability, the previous relationship becomes:

$$Q_p = \prod_{i=1}^{n} (1 - e^{-\lambda_i t}) \cong t^n \prod_{i=1}^{n} \lambda_i \qquad \text{(B.25'')}$$

$$R_p = 1 - Q_p = 1 - \prod_{i=1}^{n} (1 - e^{-\lambda_i t}) = 1 - t^n \prod_i \lambda_i \qquad \text{(B.24')}$$

In the particular case, of practical interest, of n equal units that constitute the system,
with $\lambda t << 1$, the relationship (B.25") becomes:

$$Q_p = (\lambda t)^n \qquad \text{(B.25''')}$$

Even if the components A and B have constant failure rate, the parallel system is characterized by a failure rate function of the time: null at the initial time, then increases, more or less rapidly, to the value corresponding at the component more reliable (with lower λ).

B.6.3 Systems with majority logic

A third case of elementary logic, of considerable practical interest for the realization of safety systems, is that of the majority logic. Such logic allows to keep the advantages of the parallel logic minimizing the number of spurious trips of the system for faults "fail safe".
The reliability of a system with majority logic m/n (i. e. in which for the functioning of the system it is required the correct operation of m units on n available) is immediately obtained from the development of Newton's binomial formula:

$$(R + Q)^n = 1 \qquad \text{(B.26)}$$

$$R^n + \binom{n}{1} R^{n-1} Q + \ldots\ldots + \binom{n}{m} R^{n-m} Q^m + \ldots\ldots + Q^n = 1$$

If R and Q are the reliability and unreliability of the single unit, in the last expression the first term is the probability that all units are working properly, the second is that (n-1) units are working properly and any one fails , etc. . Therefore, the reliability of the system with logic m/n is given by the sum of the first (m + 1) terms of (B.26), while the unreliability is the sum of the remaining (n-m) terms:

$$R_{m/n} = R^n + \binom{n}{1} R^{n-1} Q + \ldots\ldots\ldots + \binom{n}{m} R^{n-m} Q^m \qquad \text{(B.27)}$$

If we denote by r = n-m + 1 the minimum number of units that must fail because the system fails we obtain:

$$Q_{m/n} = \binom{n}{r} R^{n-r} Q^r + \ldots\ldots\ldots\ldots + Q^n \qquad \text{(B.28)}$$

In the usual case of units with exponential reliability, with $\lambda t << 1$, equation (B.28) can be approximated by the first term:

$$Q_{m/n} = \binom{n}{r} (\lambda t)^r \qquad \text{(B.28')}$$

A particularly important case is the logic 2/3; in this case the (B.28') becomes:

$$Q_{2/3} = 3\lambda^2 t^2 \qquad \text{(B.29)}$$

B.7 THE UNAVAILABILITY OF REDUNDANT SAFETY SYSTEMS

For systems with series logic, the treatment done in the preceding paragraph B5 (relationships from (B.12) to (B.20)) for the case of an individual apparatus are immediately applicable.
The unavailability for faults fail to danger unrevealed of systems with parallel or majority logic is obtainable by applying the general relationship (B.12); for example, in the case of the logic 1/2 and parallel (with the usual approximations, valid for $\lambda t << 1$), we have:

$$I_{1/2} = \frac{1}{\tau}\int_0^{\tau} \lambda^2 t^2 dt = \frac{1}{3}\lambda^2 \tau^2 \qquad \text{(B.30)}$$

Similarly in the case 1/3, one can achieve immediately the following result:

$$I_{1/3} = \frac{1}{\tau}\int_0^{\tau} \lambda^3 t^3 dt = \frac{1}{4}\lambda^3 \tau^3 \qquad \text{(B.31)}$$

Taking into account the contribution of testing and maintenance, in the case of test and maintenance (of average duration τ_t) carried out simultaneously at the end of the mission time τ, the relationship (B.30) becomes ([2]):

$$I_{1/2}^{pc} = \frac{1}{3}\lambda^2 \tau^2 + \frac{\tau_t}{\tau} \qquad \text{(B.32)}$$

This case is really theoretical and substantially irrational; if you have two units, in order to have always at least one unit running, you can stagger the tests of the two units. The smallest unavailability is achieved by stagger tests of $\tau/2$; then (Fig. B.4), the unreliability of the first unit is given by the usual Q '= λt, while that of the second (after commissioning the test at the instant -τ / 2) is Q " = λ(t + τ / 2), from which:

$Q_p = \lambda^2 t(t+\tau/2)$ (B.33)

in the interval where both units work, and

$Q_p = \lambda t$ when a unit is under test.

The evaluation of the unavailability can be made with reference to the interval 0-τ/2, being the situation clearly repetitive (Fig. B.4):

$$I_{1/2}^{ps} = \frac{2}{\tau}\left\{ \int_0^{\tau/2-\tau_t} \lambda^2 t(t+\frac{\tau}{2})dt + \int_{\tau/2-\tau_t}^{\tau/2} \lambda t dt \right. \qquad \text{(B.34)}$$

By developing the (B.32) and unless than infinitesimals of higher order, we obtain:

---

2 In this and in subsequent pages the apex "pc" stands for "contemporaneous tests", the apex "ps" for staggered tests.

$$I_{1/2}^{ps} = \frac{5}{24}\lambda^2\tau^2 + \lambda\tau_t \qquad \text{(B.35)}$$

By comparing this relationship with the (B.32), one can immediately see that the term due to the faults fail to danger not detected of the two units is reduced by a factor of 8/5, while the contribution of the tests and maintenance is reduced by some orders of magnitude.
By operating in a similar way in the case of logic 1/3, it is easily shown that, in case of tests and maintenance contemporary in the 3 units, the unavailability is given by the relation:

$$I_{1/3}^{pc} = \frac{1}{4}\lambda^3\tau^3 + \frac{\tau_t}{\tau} \qquad \text{(B.36)}$$

while with tests staggered at intervals equal to τ / 3, one achieves the following result:

$$I_{1/3}^{ps} = \frac{1}{12}\lambda^3\tau^3 + \frac{4}{9}\lambda^2\tau\tau_t \qquad \text{(B.37)}$$

smaller than the previous one by a factor 3 for the part due to failures of the various units and several orders of magnitude with regard to the contribution of the tests and maintenances.

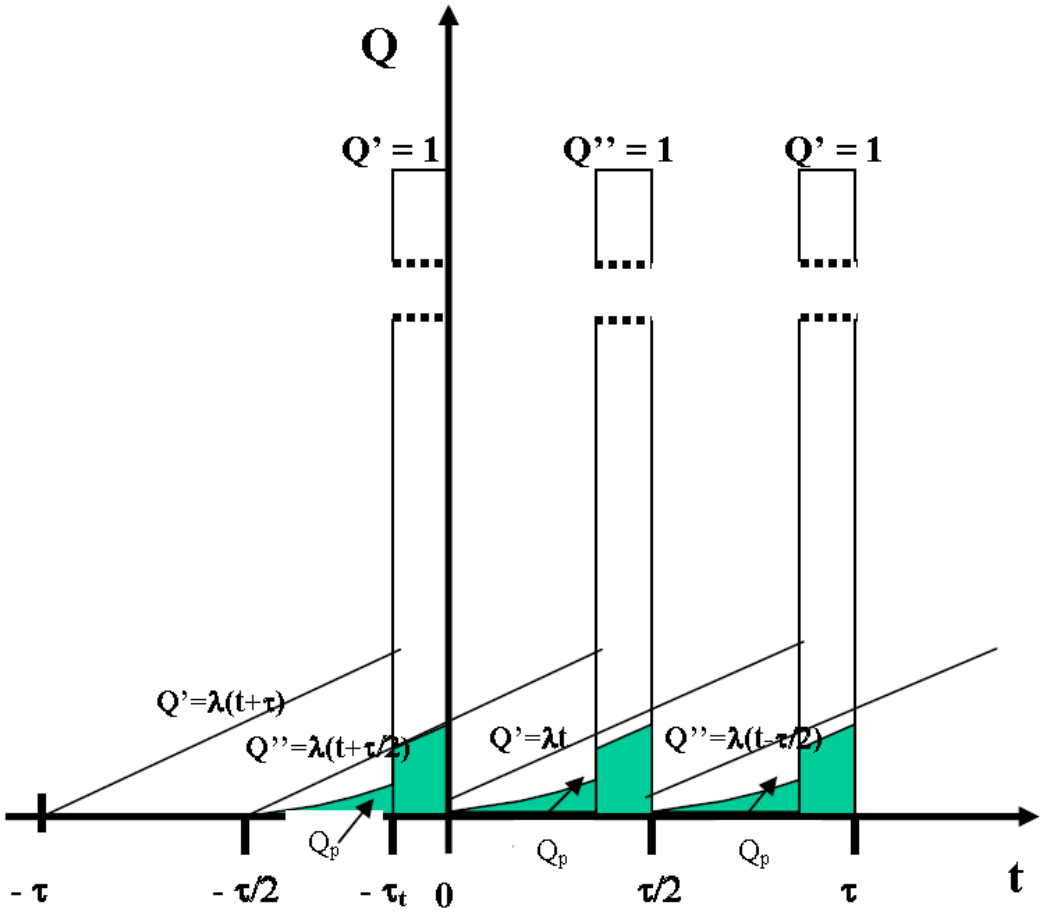


Fig. B.4 - Graphical representation of the unreliability and the unavailability (dashed areas) of a protection system with parallel logic 1/2 and tests staggered of τ / 2.

Finally, in the case of systems with majority logic 2/3, reminding that $Q^{2/3} \simeq 3\lambda^2\tau^2$, we have:

$$I_{2/3}^{pc} = \lambda^2 \tau^2 + \frac{\tau_t}{\tau} \qquad \text{(B.38)}$$

in the case (theoretical) of contemporaneous tests and maintenances of all units at the end of the interval of mission.

Usually the best results are achieved by staggering the tests at intervals of τ / 3. It is left to the reader the solution, yet simple, of the problem of determination of the unavailability in this case, warning that one needs to consider, during the tests and maintenances, two possibilities:

- the unit under test is excluded and the logic becomes 2/2; in this case the system has unreliability sum of those of the remaining units: $Q = \lambda t + \lambda(t + \tau/3) = 2\lambda t + \lambda\tau/3$;
- the unit under test is replaced by a signal in the shutter release position, for which the logic of the remaining units becomes 1/2: $Q = \lambda^2 t\ (t+\tau/3)$.

A remark deserves explicit considerations, about the fact that relationships (B.35) and (B.37), valid for tests staggered, seem not to allow optimization of the mission interval τ (on the contrary, this is possible in the case of contemporaneous tests and repairs - relationships (B.32), (B.36) and (B.38)). In this regard it can be stated that:

• staggering the tests, the optimization problem for τ is less important because, during the test drive, one (or more) unit remains operational;
• optimization is still possible, but in the development of relationships (B.35), (B.37) or similar one must include the infinitesimal terms for higher order omitted in previous formulas.

To complete this section, it should be noted that the all the previous formulas (and the similar one valid in case of logics 1/4, 2/4, etc.) assume the complete independence between the various units, never fully achievable. Usually, there are dependencies between the various units due to design, construction and installation, to the location on the system, etc. These dependencies will ultimately result in a finite probability of common failures or otherwise contemporary loss of function; this probability is orders of magnitude greater than that calculated in the hypothesis of complete independence of the various units. Operational guidance on this topic (which is critical for risk analysis) is a very important topic.

B.8 METHODS FOR THE RELIABILITY ANALYSIS OF COMPLEX SYSTEMS

In order to study the probability of failure of a complex system several methods have been developed. These, in addition to being a (relatively) simple calculation tool for obtaining this probability, always provide **qualitative** information also of considerable importance for

the knowledge of the system and allow then to make decisions based on a knowledge, as far as possible complete and correct, on the system under examination.
The main techniques used for this purpose, on which we will focus briefly at application level, have already been introduced in previous chapters: the fault tree and events tree, logic diagrams borrowed from the decision theory.

B.8.1 Fault tree method

The fault tree is a **deductive** technique that analyzes a particular event ("Top Event") for identify the causes.
For a proper construction of the fault tree of a complex system it is appropriate the use techniques such as the Hazard and Operability Analysis (HAZOP) and FMEA (Failure Mode and Effects Analysis), that help identify the "Top Events" and the logical structure that determines them through a comprehensive and consistent analysis of the system.
The analysis by fault tree proceeds through the following steps:
- **Construction of the tree**;
- **Qualitative analysis:** solution of the logic tree by applying the rules of Boolean algebra, for the identification of "minimal cutting sets " ("Minimal Cut Sets-MCS") of the system;
- **Quantitative analysis**: solution of the unavailability of the "Top Event" or of the expected number of events during the mission time, as the sum of the unavailability or of the number of events of the individual "MCS".

A minimum set of cutting (MCS) is a combination of events, not further subdivided (hence the adjective "minimum"), whose occurrence involves the occurrence of the "Top-Event". The fault tree analysis allows the detection of events that can lead directly to the "Top Event" (MCS of the first order), the MCS of order 2 (for which is required the occurrence of two independent events), etc .; at the end you can also list the different "Minimal Cut Sets" in order of relative importance (contribution to the probability of occurrence of the "Top Event").

The rules of Boolean algebra are recalled in Appendix B.1, while an example of application of the fault tree method is shown in Appendix B.2.

The fault tree is currently perhaps the most used tool in the field of safety analyzes for the study of the causes of accidents, the identification of the most critical components for the assessment of the effects of different maintenance policies (time intervals between tests, etc.) and to quantify the probability of an accident.

Note: the fault tree technique assumes that all basic events listed are **independent**. In reality this is not always true (e.g. components where the probability of failure depends on the state of failure or performance of another component, or dependencies caused by maintenance). These causes of dependence must be taken into account with the adoption of appropriate techniques.

B.8.2 Event Tree Method

In contrast to fault tree, the event tree technique is an **inductive** method which, from the knowledge of the possible states of components, enables to build the set of all possible "stories" of the system.
The logical process start on the assumption that a certain event (initiating event) has occurred; then the tree is constructed studying all the possible ramifications, depending on the success or not of action of various protection systems.

The stories constructed by the event tree are mutually exclusive and are caused by the simultaneous occurrence of all events belonging to the branch of the tree that defines them. Their probability is then expressed as a product of the probabilities of the nodes of the tree; the probability of more stories is the sum of the probability of occurrence of each individual story.

Differently from the fault tree, the event tree method allows to treat, with greater flexibility, dependencies between events and to simulate the variation of the probability of an event as a function of the occurrence or not of previous events. In this regard, see the explanatory example shown in Appendix B.3.
Within the framework of safety analysis, currently the event tree founds aso application in the analysis of phenomenologies consequent

to an event (e. g., study of the probability of the different possible scenarios resulting from a given release, in dependence of the presence of ignition, of particular weather conditions, etc.).

Appendix B.1 Elements of Boolean Algebra

PROBABILITY CONCEPT

- FREQUENCY APPROACH

  "IF AN EVENT A OCCURS X TIMES IN A SERIES OF N REPETITIVE EXPERIMENTS"

  $P(A) = \lim (X/N) \approx X/N$

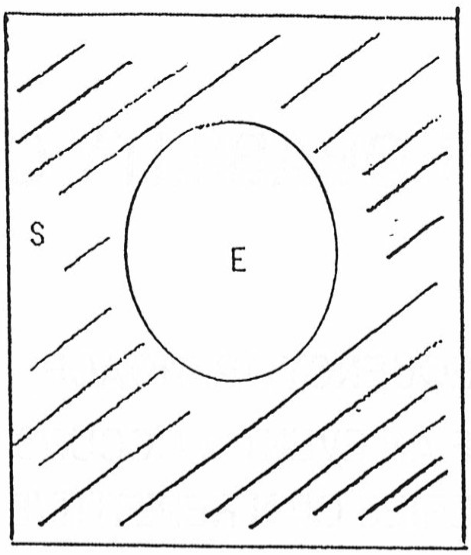
- SUBJECTIVE APPROACH

  " IS A MEASURE OF ONE'S SUBJECTIVE DEGREE OF KNOWLEDGE (CERTAINTY) OF A PARTICULAR OUTCOME"

  It can be calibrated between 1 and 0 using frequency as a scale.

ELEMENTARY PROBABILITY THEORY

VENN DIAGRAMS



S - UNIVERSAL SET

E - SET WHERE A PARTICULAR NUMBER OF EVENTS OCCUR

$\bar{E}$ - SET OF ALL EVENTS WHICH DO NOT BELONG TO E

ϕ - EMPTY SET (NO EVENTS)

P(E) - PROBABILITY OF SET E

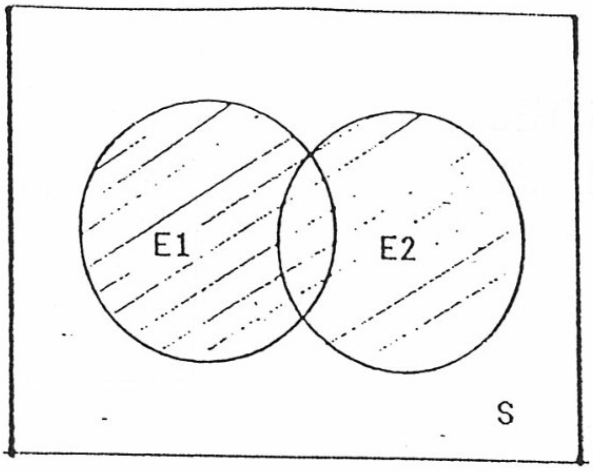
P(S) = 1

SETS CANNOT BE ADDED OR MILTIPLIED ONLY PROBABILITIES CAN

BOOLEAN ALGEBRA CONCEPTS

UNION OF SETS

E1 U E2
E1 + E2



$P(E1 \text{ OR } E2) = P(E1) + P(2) - P(E1.E2)$

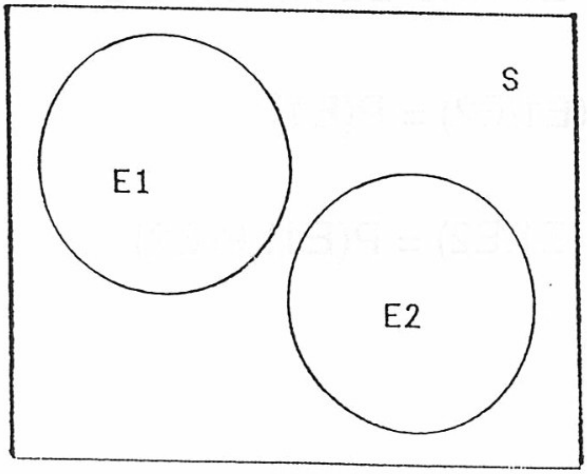
FOR MUTUALLY EXCLUSIVE EVENTS THE SETS
E1, E2 DO NOT INTERCEPT

$P(E1 \text{ OR } E2) = P(E1) + P(E2)$

$P(E1 \text{ OR } \overline{E}1) = P(E1) + P(\overline{E}1) = 1$

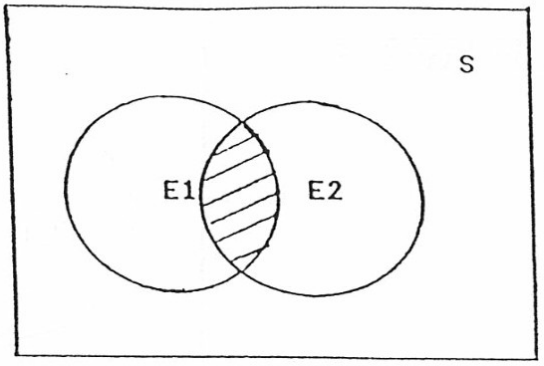
$E1 + E1 = E1$

$E1 + \overline{E}1 = S$



INTERSECTION OF SETS

$E1 \cap E2$
$E1 \,.\, E2$



$$P(E1 \text{ AND } E2) = P(E1/E2).P(E2) = P(E2/E1)\,P(E1)$$

E1/E2 CONDITIONAL PROBABILITY OF E1 GIVEN E2

$E1.E2 = E2.E1$

$E1 \,.\, S = E1$

$E1.\bar{E}1 = \phi$

IF E1 AND E2 ARE INDEPENDENT

$P(E1/E2) = P(E1)$

$P(E1.E2) = P(E1).P(E2)$

BAYES THEOREM

$$P(E1.E2) = P(E1/E2) \cdot P(E2) = P(E2/E1) \cdot P(E1)$$

$$P(E1/E2) = \frac{P(E2/E1)\, P(E1)}{P(E2)}$$

EXERCICES:

A) PROVE THAT $P(A + B) = P(A) + P(B) - P(A.B)$
(hint: write $A = A(B+\overline{B})$; $B = B(A+\overline{A})$

B) GENERALIZE FOR $P(A1 + A2 + \ldots AN)$

C) PROVE DE MORGAN'S THEOREM
$\overline{A + B} = \overline{A} \cdot \overline{B}$

Appendix B.2 Fault Tree Development and Application

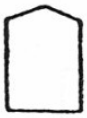
SOME TOOLS

EVENTS

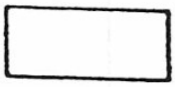
BASIC EVENT — A basic initiating fault requiring no further development

CONDITIONING EVENT — Specific conditions or restrictions that apply to any logic gate (used primarily with PRIORITY AND and INHIBIT gates)

UNDEVELOPED EVENT - An event which is not further developed either because iy is of negligeable consequences or because information in unavailable



EXTERNAL EVENT — An event which is normally expected to occur



INTERMEDIATE EVENT — A fault event that occurs because of one or more antecedent causes acting through logic gates

GATES

AND — Output fault occurs if all of the input faults occur

OR — Output fault occurs if at least one of the input faults occurs

EXCLUSIVE OR — Output fault occurs if exactly one of the input faults occurs

PRIORITY AND — Output fault occurs if all of the input faults occur in a specific sequence (the sequence is represented by a CONDITIONING EVENT drawn to the right of the gate)

INHIBIT — Output fault occurs if the (single) input fault occurs in the presence of an enabling condition (the enabling condition is represented by a CONDITIONING EVENT drawn to the right of the gate)

GENERAL STEPS IN FAULT TREE DEVELOPMENT

- EXPLICITLY DEFINE THE UNDESIRED TOP EVENT IN "FAILURE SPACE"

  TOP EVENTS DEVELOPED FOR:

  - EVENT TREE TOP-LOGIC SYSTEM SUCCESS CRITERIA
  - SYSTEM FAILURES THAT LEAD TO AN INITIATING EVENT

    EXAMPLE: Loss of instrument air leads to MSIV closure

  - SYSTEM FAILURES THAT LEAD TO FAILURES OF OTHER IMPORTANT SYSTEMS

    EXAMPLE: Loss of SW leads to loss of RCCW which leads to loss of ECCS

- LOOK FOR EVENTS THAT ARE IMMEDIATE CAUSE OF TOP EVENT

- CONSTRUCT BOOLEAN REPRESENTATION OF THE IMMEDIATE EVENTS THAT LEAD TO TOP EVENT

GENERAL STEPS IN FAULT TREE DEVELOPMENT (continued)

- IDENTIFY EVENTS THAT ARE THE IMMEDIATE CAUSE FOR THE FIRST SET OF EVENTS UNDER THE TOP EVENT

- CONSTRUCT BOOLEAN REPRESENTATION OF THOSE EVENTS

- CONTINUE WITH IMMEDIATE-CAUSE ANALYSIS TO DESIRED LEVEL OF RESOLUTION

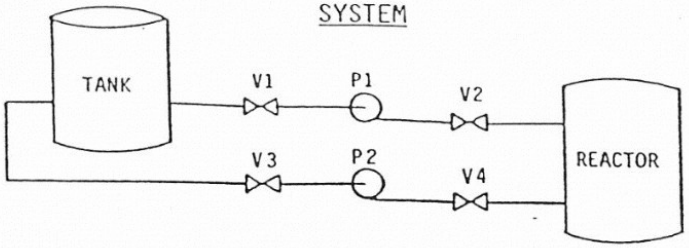
- PLAN TO ITERATE AS SYSTEM KNOWLEDGE IS ENHANCED

MAY IDENTIFY:

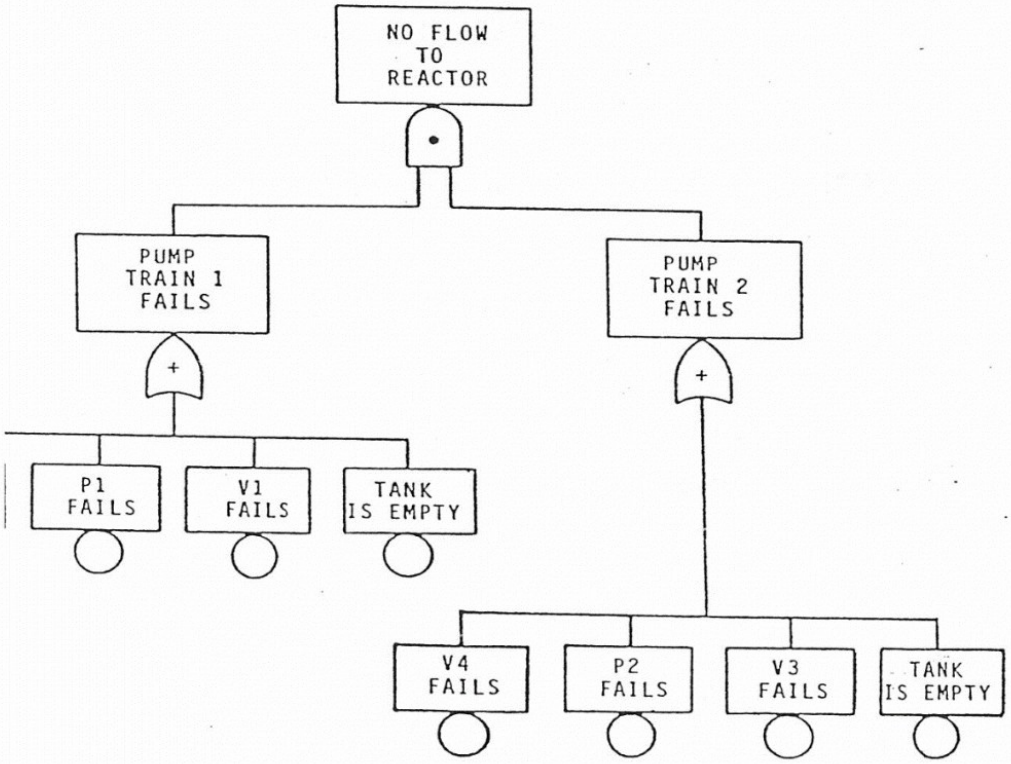
- New initiating events
- New top-logic events or logic for ET
- New events or logic for FT

EXAMPLE FAULT TREE

SYSTEM



FAULT TREE



CUT SET vs. MINIMAL CUT SET

CUT SET: A COMBINATION OF COMPONENT FAILURES WHICH, IF THEY ALL OCCUR, WILL CAUSE THE TOP EVENT TO OCCUR

MINIMAL CUT SET: THE SMALLEST COMBINATION OF COMPONENT FAILURES WHICH, IF THEY ALL OCCUR, WILL CAUSE THE TOP EVENT TO OCCUR

EXAMPLES: (USING THE EXAMPLE FAULT TREE)

CUT SETS	MINIMAL CUT SETS
V2·V4	TE
V2·P2	V2·V4
V2·V3	V2·P2
V2·TE	V2·V3
TE·TE	P1·V4
.	.
.	.
.	.
16 ELEMENTS	10 ELEMENTS

TO WHAT LEVEL OF DETAIL SHOULD FAULT TREES BE DEVELOPED?

- PURPOSE OF ANALYSIS
  - ROOT CAUSE
  - SYSTEM RELIABILITY
  - SEQUENCE QUANTIFICATION
  - SECONDARY FAILURE/EXTERNAL EVENTS ANALYSIS
- DATA LIMITS
- COMPUTER CODE LIMITS

DETAILED EXAMPLE OF FAULT TREE DEVELOPMENT

- FAULT TREE IS CONSTRUCTED IN SUCCESSIVE LEVELS WHICH DESCEND FROM AN EVENT USUALLY DEFINED AT THE SYSTEM LEVEL, THE UNDESIRED EVENT.

- LAYERS PROGRESS FROM THE SYSTEM LEVEL, THROUGH THE SUBSYSTEM LEVEL, THROUGH THE COMPONENT LEVEL, TO THE SUBCOMPONENT LEVEL.

FIRST STEP - - THE UNDESIRED EVENT

- THE FIRST STEP IN FAULT TREE CONSTRUCTION IS TO DEFINE THE UNDESIRED EVENT. THE UNDESIRED EVENT CONSTITUTES THE TOP EVENT AND GENERALLY CONSISTS OF A COMPLETE OR CATASTROPHIC FAILURE OF THE SYSTEM. DEFINITION OF THE UNDESIRED EVENT CAN INFLUENCE THE FAILURE MODES WHICH THE ANALYST WILL INCLUDE IN THE TREE.

SUCCESS CRITERIA

- DETERMINE THE SUCCESS CRITERIA OF THE SYSTEM BEING ANALYZED

- CONVERT SUCCESS CRITERIA TO "FAILURE SPACE" (I.E., FAILURE CRITERIA)

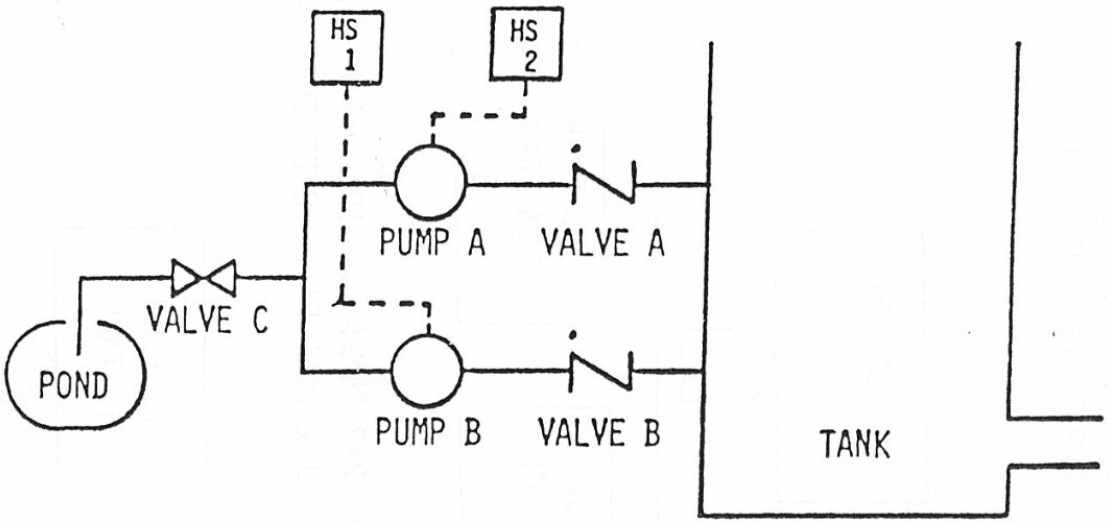
  RULE: IF SUCCESS = N/M,
  THEN FAILURE = M-(N-1)/M

  EXAMPLE:

SUCCESS (N/M)	FAILURE (M-[N-1]/M)
1/4	4/4
2/4	3/4
3/4	2/4
4/4	1/4

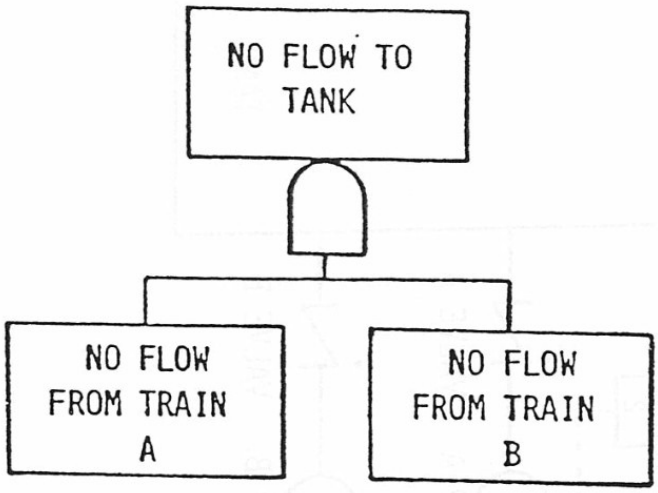
- SUCCESS CRITERIA CAN CHANGE FOR A SYSTEM.
- THE CRITERIA ARE OFTEN DEPENDENT ON THE INITIATING EVENT.

EXAMPLE SYSTEM

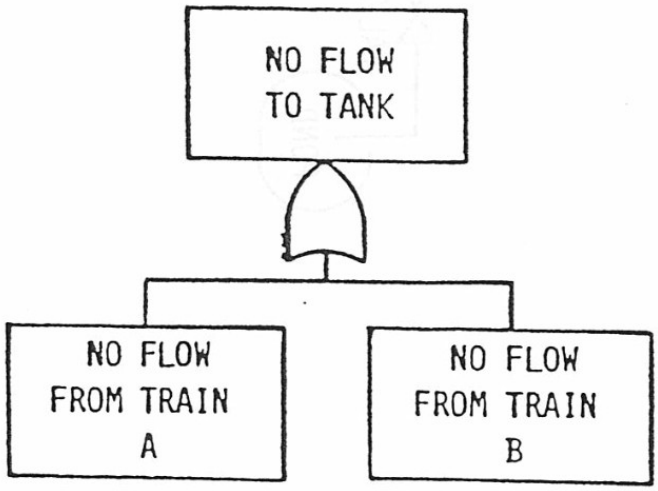


EXAMPLE OF SUCCESS CRITERIA

SUCCESS CRITERIA: 1/2 PUMPS REQUIRED TO DELIVER FLOW TO TANK
FAILURE CRITERIA: 2/2 PUMPS FAIL TO DELIVER FLOW



SUCCESS CRITERIA: 2/2 PUMPS REQUIRED TO DELIVER FLOW TO TANK
FAILURE CRITERIA: 1/2 PUMP FAIL TO DELIVER FLOW



WHAT SHOULD BE INCLUDED IN THE FAULT TREE?

- ANY FAULT WHICH COULD SINGULARLY OR IN COMBINATION WITH OTHER FAULTS RESULT IN THE TOP EVENT

- THESE USUALLY INCLUDE
  - Local Faults
  - Initiation and Control Faults
  - Support System Faults
  - Operator-Related Faults
  - Functional Faults
  - Secondary Faults

LOCAL FAULTS

- DIRECTLY ATTRIBUTABLE TO THE COMPONENT

  EXAMPLES: PUMP FAILS TO START
  VALVE FAILS TO OPEN
  RELAY FAILS TO ENERGIZE

- EASIEST TO IDENTIFY

- LEVEL OF DETAIL DEPENDS ON:

  - PURPOSE
  - DATA
  - COMPUTER CODE

INITIATION AND CONTROL CIRCUIT FAULTS

- INCLUDES:
  - SIGNALS
  - CIRCUITS
  - OPERATOR ACTIONS

  NECESSARY TO:
  - START
  - OPERATE
  - CONTROL

  A COMPONENT

- CONTROL CIRCUITS:
  - INCLUDE WIRING AND CIRCUIT COMPONENTS THAT START, STOP AND CONTROL THE COMPONENT BEING ANALYZED
  - USUALLY DO NOT SERVE ANY OTHER COMPONENT

INITIATION AND CONTROL CIRCUIT FAULTS (continued)

- INITIATION CIRCUITS
  - INCLUDE WIRING AND CIRCUIT COMPONENTS USED TO ACTIVATE A CONTROL CIRCUIT FOR A GIVEN COMPONENT
  - OFTEN SHARED BY MORE THAN ONE COMPONENT

SUPPORT SYSTEM FAULTS

- INCLUDES FAULTS IN SYSTEMS WHICH ARE NECESSARY FOR COMPONENT OPERATION

EXAMPLES:

- AC OR DC POWER TO COMPONENTS
- DC POWER TO CONTROL AND INITIATION CIRCUITS
- LUBRICATION
- HVAC

OPERATOR - RELATED FAULTS

- ACTIONS TAKEN BY THE OPERATOR WHICH CAN CAUSE A COMPONENT TO BE UNAVAILABLE WHEN REQUIRED.

EXAMPLES :

- COMPONENT UNAVAILABLE DUE TO TESTING
- SCHEDULED OR UNSCHEDULED MAINTENANCE
- RESTORATION ERRORS

FUNCTIONAL FAULTS

- EVENTS ASSOCIATED WITH THE FUNCTIONAL CHARACTERISTICS OF A FLUID SYSTEM OR MONITORED PARAMETER

EXAMPLES:

- FLUID TEMPERATURE CHANGES WHICH COULD CAUSE PUMP CAVITATION

- STEAM BINDING PRIMARY SIDE OF S/G WHICH CAN AFFECT RCS FLOW OR RCS/SG HEAT TRANSFER

- POND LEVEL TOO LOW TO MAINTAIN PUMP NPSH

SECONDARY FAULTS

- EQUIPMENT FAILURES OR OTHER EVENTS WHICH ARE NOT NECESSARY FOR PROPER OPERATION OF THE COMPONENT BUT WHOSE OCCURRENCE MAY RENDER THE EQUIPMENT UNAVAILABLE. THESE INCLUDE EVENTS COMMONLY REFERRED TO AS COMMON MODE EVENTS. THESE FAILURES USUALLY AFFECT MULTIPLE COMPONENTS AND ARE NORMALLY ON THE SYSTEM OR SUBSYSTEM LEVEL.

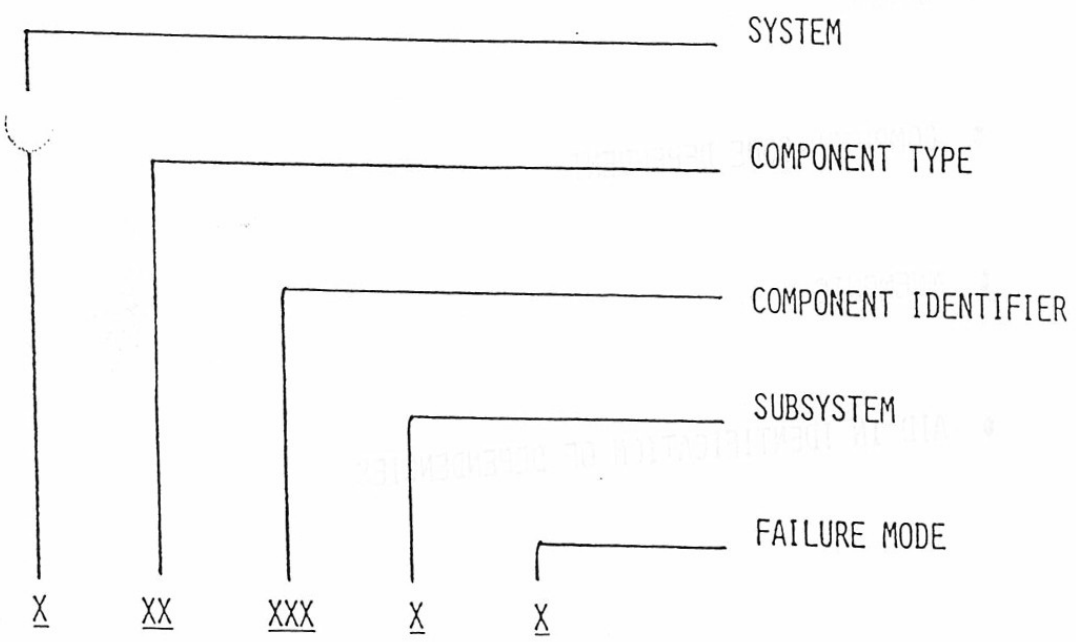
EXAMPLES ARE:

- FIRES
- FLOOD
- EARTHQUAKE

NAMING BASIC EVENTS AND GATES

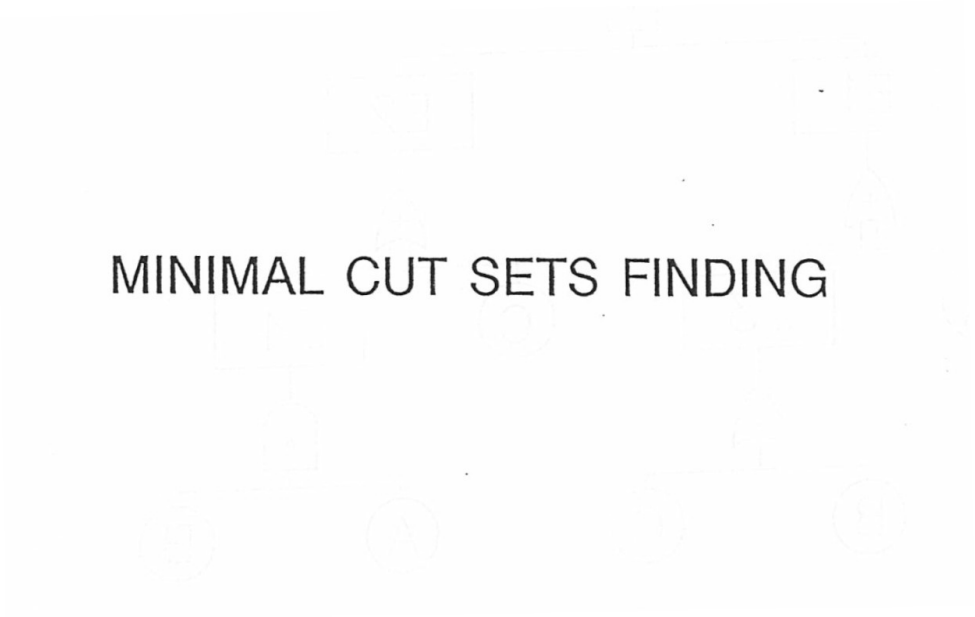
- SIMPLE
- UNIQUE
- COMPUTER-CODE DEPENDENT
- MNEMONIC
- AID IN IDENTIFICATION OF DEPENDENCIES

EXAMPLE OF BASIC EVENT NAMING SCHEME

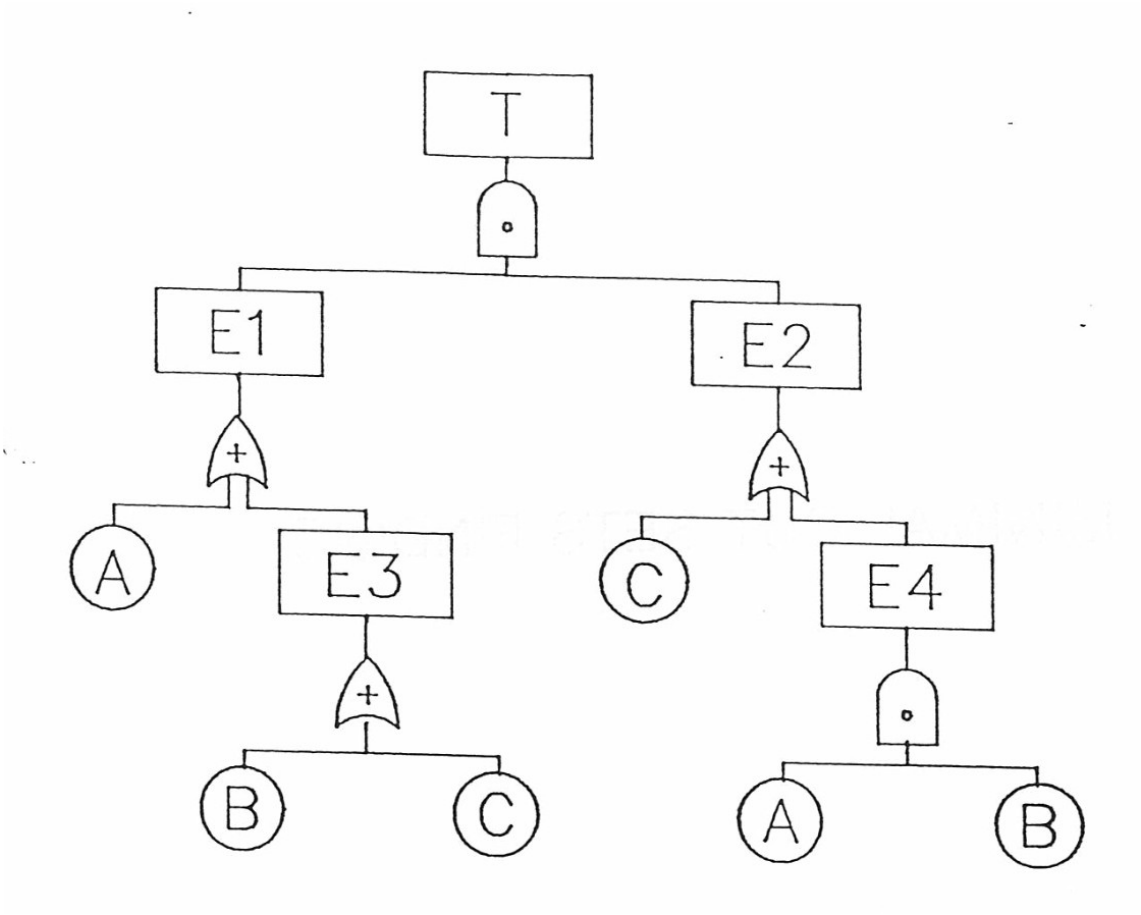


EXAMPLE: SPMØA1AS

TRANSLATION:
S - Service water
PM - Pump (motor-driven)
ØA1 - Pump No. A1
A - Train A
S - Does not start



MINIMAL CUT SETS FINDING


T
E1
E2
A
E3
C
E4
B
C
A
B

$$T = E1.E2$$
$$E1 = A+E3$$
$$E3 = B+C$$
$$E2 = C+E4$$
$$E4 = A.B$$

$T = (A+E3) \;.\; (C+E4)$ EXPAND

$= AC + AE4 + E3C + E3E4$ SUBST. E3, EXPAND

$= AC + AE4 + BC + CC + BE4 + CE4$

$= AC + AE4 + BC + C + BE4 + CE4$

$AC + BC + C + CE4 = C$

$= AE4 + C + BE4$ SUBTITUTE E4

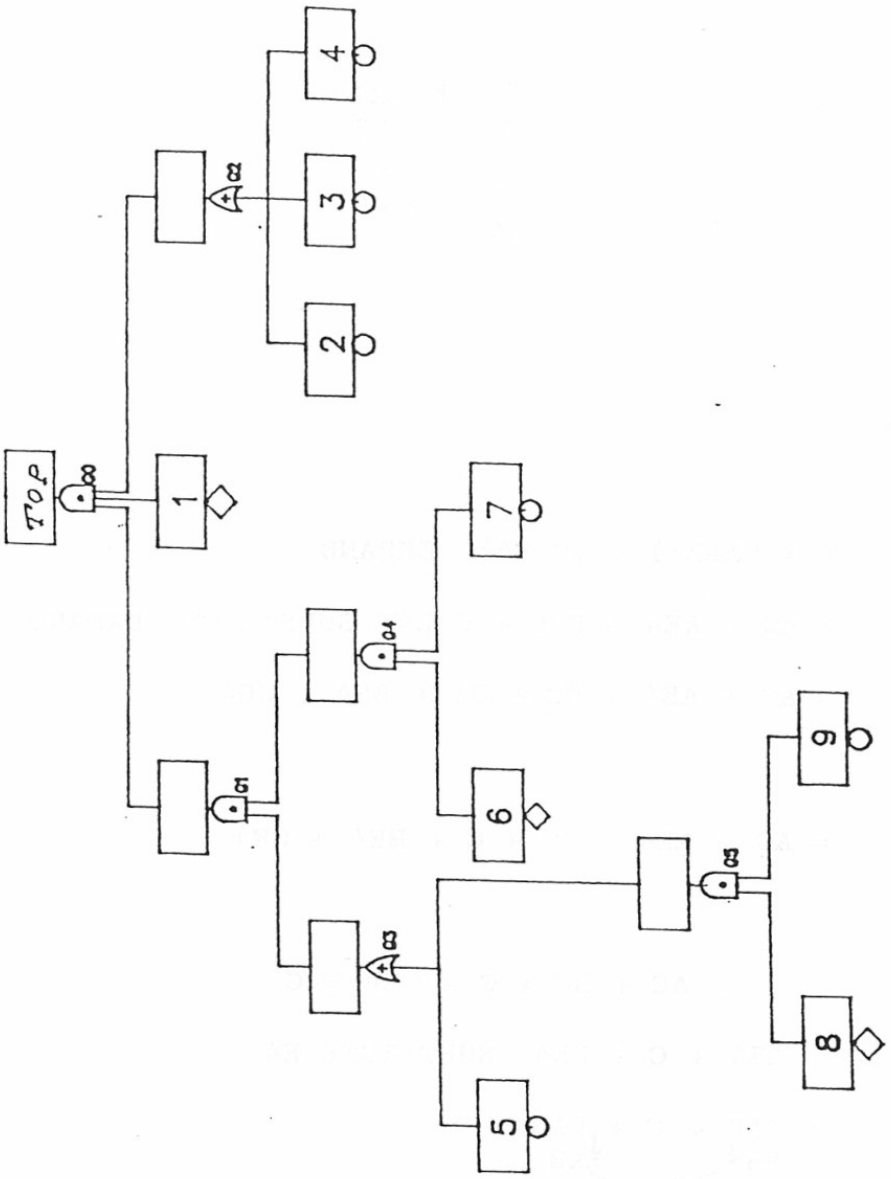
$= AAB + C + BAB$

AB ↓ ↘ ↙ ↓ AB

: AB

$$\boxed{T = AB + C}$$

EXAMPLE 2



TOP DOWN EXPANSION/SUBSTITUTION

OR GATE - NEW LINES
AND GATE - SAME LINE

G0
G1, 1, G2
G3, G4, 1, G2
+ 5, G4, 1, G2 → 5, 6, 7, 1, G2
+ G5, G4, 1, G2 → 5, 6, 7, 1, 2 / 5, 6, 7, 1, 3 / 5, 6, 7, 1, 4
8, 9, G4, 1, G2
8, 9, 6, 7, 1, G2
8, 9, 6, 7, 1, 2
8, 9, 6, 7, 1, 3
8, 9, 6, 7, 1, 4

BOOLEAN CUT SETS

1, 4, 5, 6, 7
1, 2, 5, 6, 7
1, 3, 5, 6, 7
1, 2, 6, 7, 8, 9
1, 3, 6, 7, 8, 9
1, 4, 6, 7, 8, 9

BECAUSE NO SET IS FULLY CONTAINED IN ANOTHER, ALL ARE MINIMAL CUT SETS

FAULT TREE QUANTIFICATION

- USE RARE EVENT APPROXIMATION TO MINIMAL CUT SETS

- USE GATE BY GATE CALCULATION (NO REPEATED EVENTS)

- GATE TYPE -OR-

  . PROBABILITIES ADDED
  . FREQUENCIES ADDED
  . CANNOT ADD PROBAB. AND FREQUENCY

- GATE TYPE -AND-

  . PROBABILITIES MULTIPLY
  . ONE FREQUENCY CAN BE MULTIPLIED TO VARIOUS PROBABILITIES
  . FREQUENCIES CANNOT BE MULTIPLIED

IF DURATION IS KNOWN A TRANSFORMATION IS POSSIBLE TO ADD FREQUENCIES:

EXAMPLE: EVENT -A- Fa , Pa, Ta
EVENT -B- Fb , Pb, Tb
f= PaFb + FaPb

Appendix B.3 Event Tree Development and Application

EVENT TREES

- GRAPHICAL LOGICAL MODEL THAT IDENTIFIES AND QUANTIFIES POSSIBLE OUTCOMES FOLLOWING THE OCCURRENCE OF AN INITIATING EVENT.

- USES INDUCTIVE LOGIC (NORMALLY BINARY).

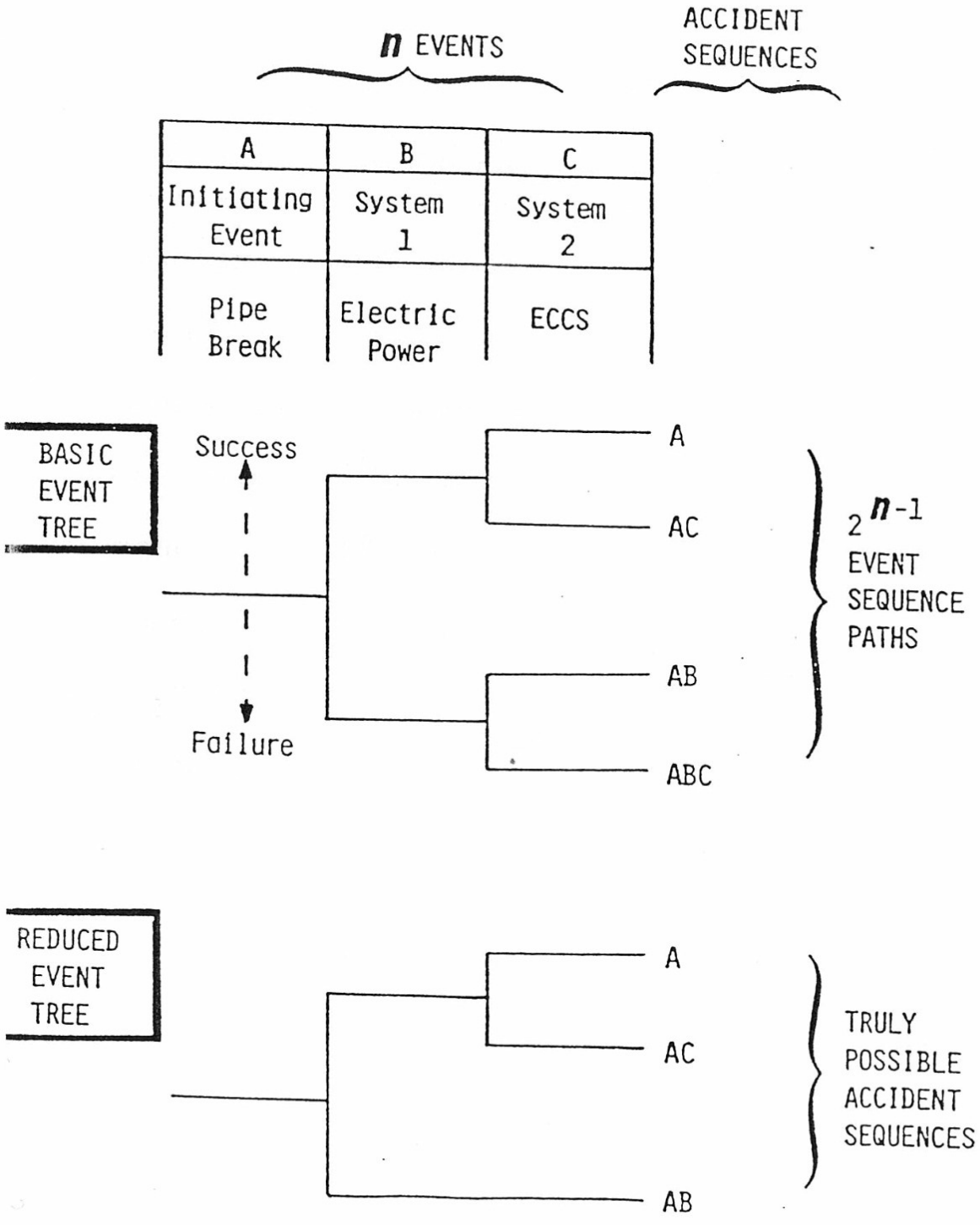
- PRE-INCIDENT EVENT TREES.

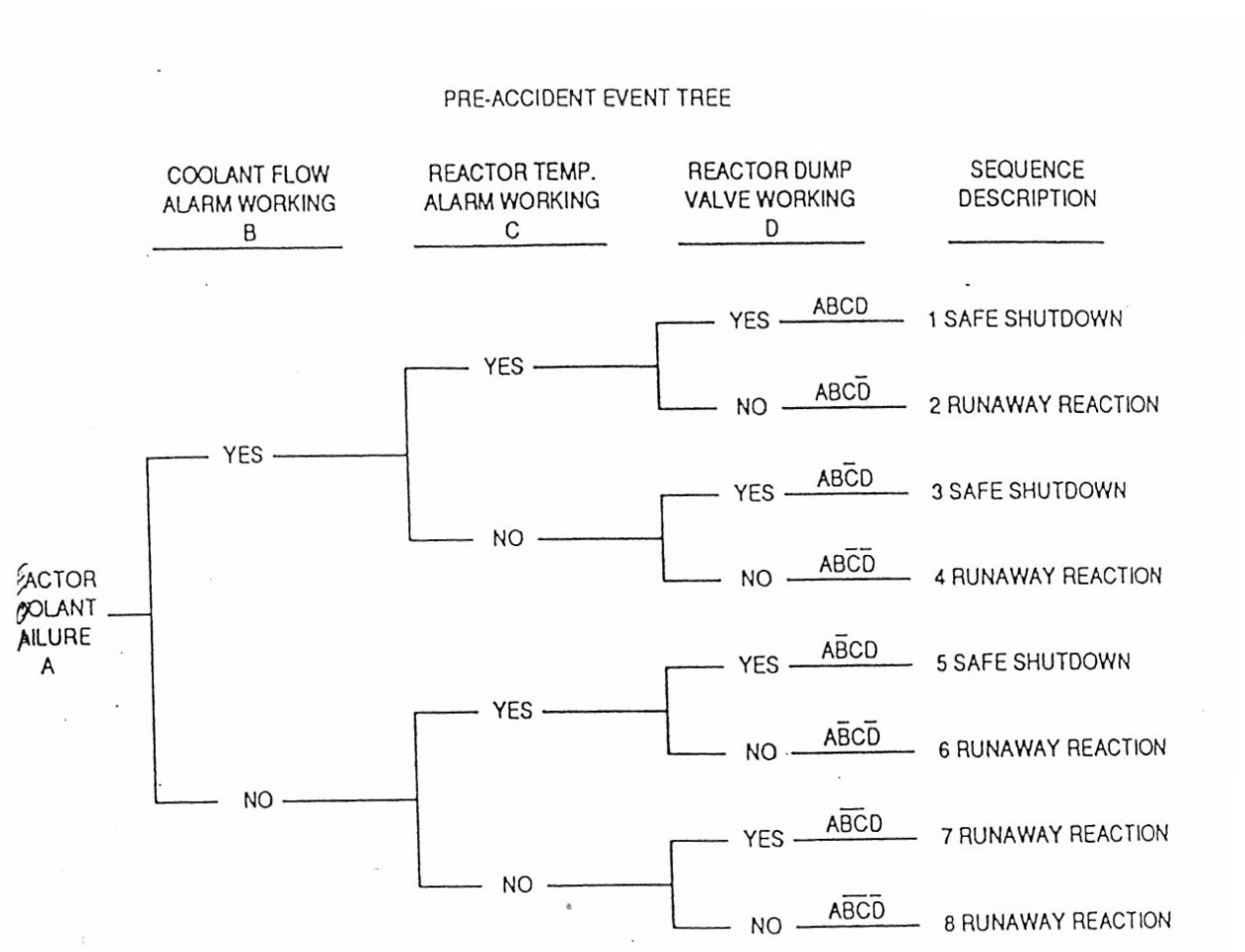
- POST ACCIDENT EVENT TREES.

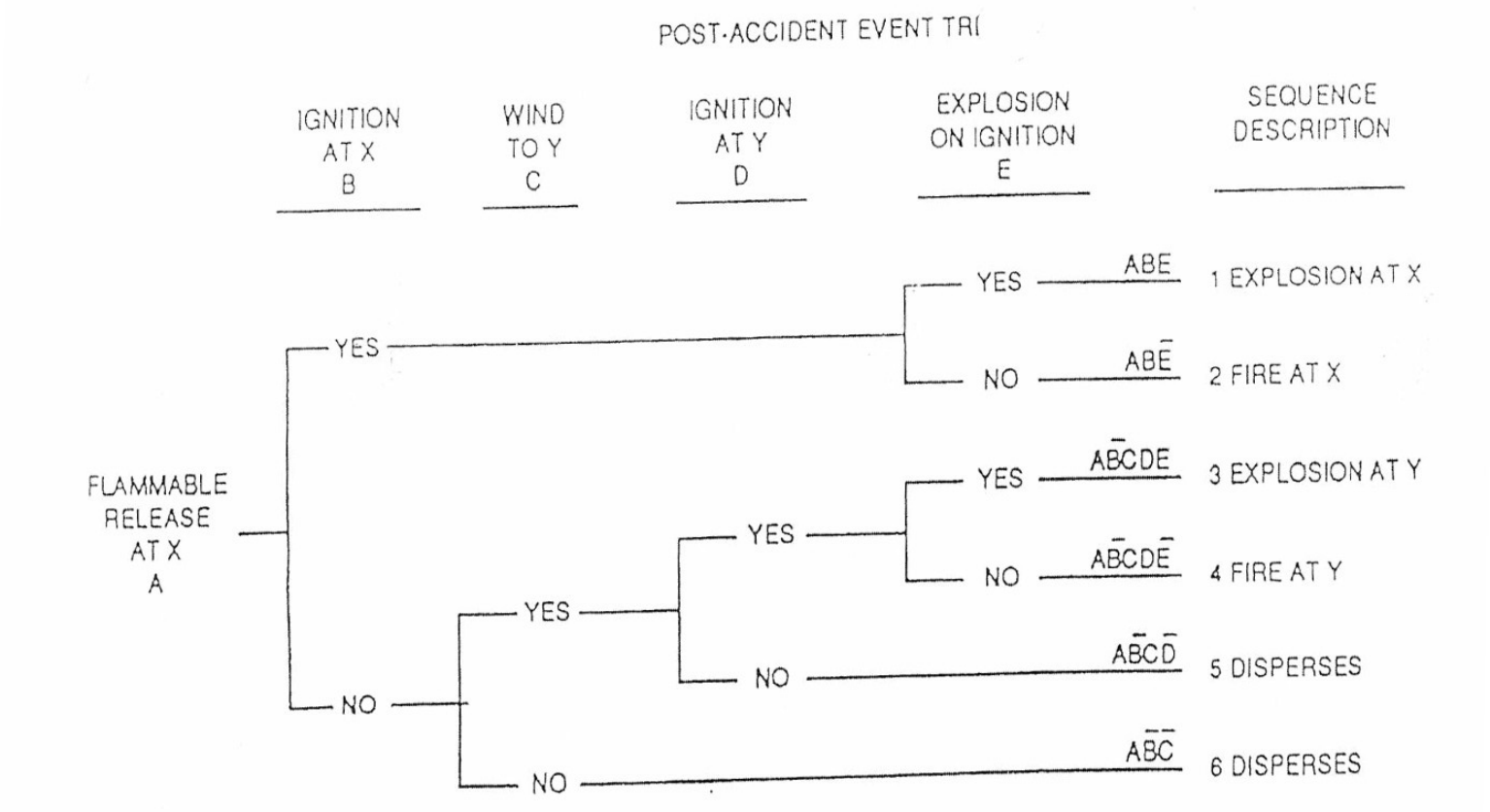
- STEPS OF ET ANALYSIS.

. IDENTIFY INITIATING EVENTS
. IDENTIFY SAFETY FUNCTIONS
(PRE-INCIDENT ET)
. IDENTIFY HAZARD FACTOR
(POST-INCIDENT ET)
.. DEVELOP ALL POSSIBLE OUTCOMES
. CLASSIFY OUTCOMES IN CATEGORIES OF SIMILAR CONSEQUENCES
. QUANTIFY PROBABILITY OF EACH BRANCH
. QUANTIFY SEQUENCES

EXAMPLE EVENT TREE

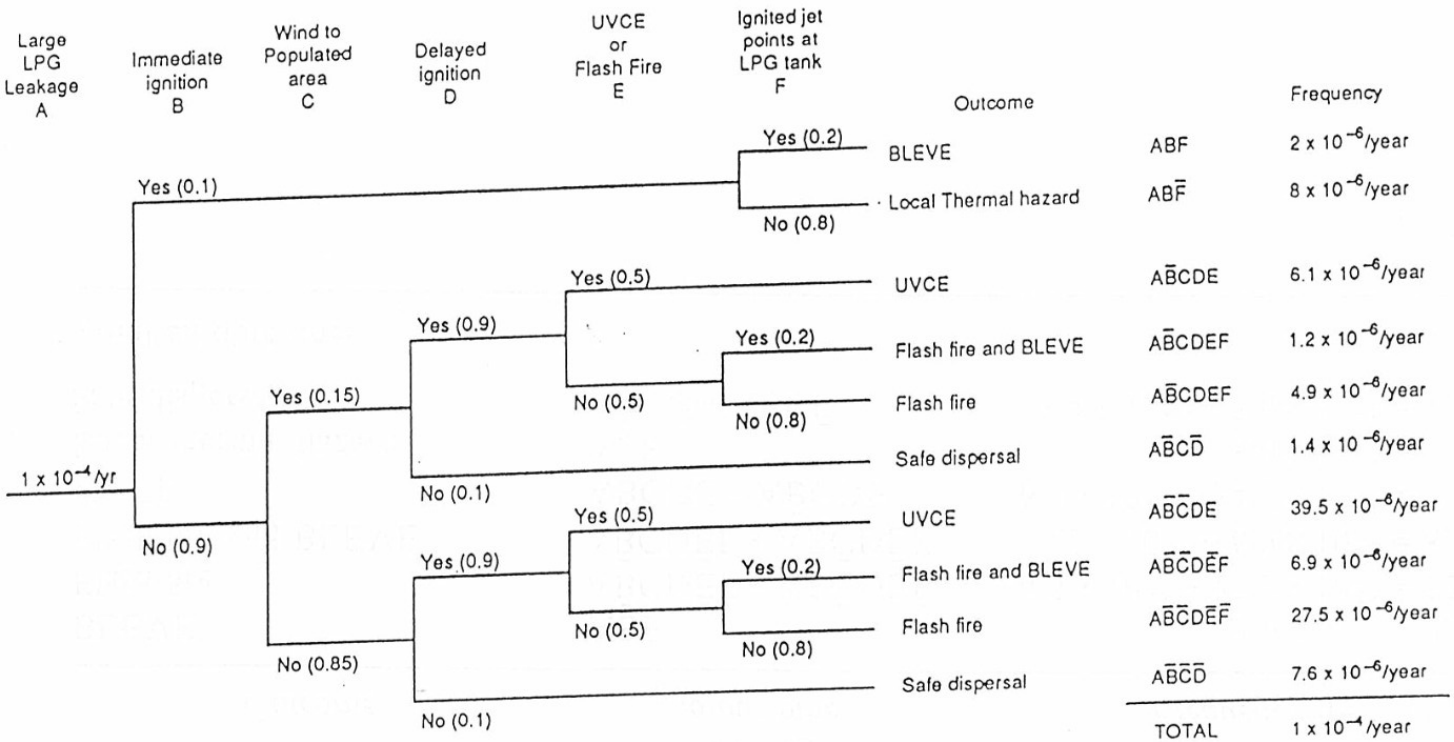



PRE-ACCIDENT EVENT TREE
COOLANT FLOW ALARM WORKING B
REACTOR TEMP. ALARM WORKING C
REACTOR DUMP VALVE WORKING D
SEQUENCE DESCRIPTION
REACTOR COOLANT FAILURE A
YES
NO
YES
NO
YES
NO
YES
NO
ABCD
ABCD̄
ABC̄D
ABC̄D̄
AB̄CD
AB̄CD̄
AB̄C̄D
AB̄C̄D̄
1 SAFE SHUTDOWN
2 RUNAWAY REACTION
3 SAFE SHUTDOWN
4 RUNAWAY REACTION
5 SAFE SHUTDOWN
6 RUNAWAY REACTION
7 RUNAWAY REACTION
8 RUNAWAY REACTION


POST-ACCIDENT EVENT TRI
IGNITION AT X B
WIND TO Y C
IGNITION AT Y D
EXPLOSION ON IGNITION E
SEQUENCE DESCRIPTION
FLAMMABLE RELEASE AT X A
YES
NO
YES
NO
YES
NO
YES
NO
ABE
ABĒ
ĀBCDE
ĀBCDĒ
ĀBCD̄
ĀB̄C̄
1 EXPLOSION AT X
2 FIRE AT X
3 EXPLOSION AT Y
4 FIRE AT Y
5 DISPERSES
6 DISPERSES

Event	*probability*[a]	*Source of data*[a]
A. Large leakage of pressurized LPG	1.0×10^{-4}/yr	Fault Tree Analysis
B. Immediate ignition at tank	0.1	Expert opinion
C. Wind blowing toward populated area	0.15	Wind rose data
D. Delayed ignition near populated area	0.9	Expert opinion
E. UVCE rather than flash fire	0.5	Historical data
F. Jet flame strikes the LPG tank	0.2	Tank layout geometry

[a]These data are for illustrative purposes only.



Event tree outcomes for sample problem.

Outcome	*Sequences leading to outcome*	*Frequency (per year)*
BLEVE	$AB\bar{F}$	$2.0 \times 10^{-6} = 2.0 \times 10^{-6}$
Flash fire	$A\bar{B}\bar{C}D\bar{E}\bar{F} + A\bar{B}\bar{C}D\bar{E}\bar{F}$	$4.9 \times 10^{-6} + 27.5 \times 10^{-6} = 32.4 \times 10^{-6}$
Flash fire and BLEVE	$A\bar{B}CD\bar{E}F + A\bar{B}\bar{C}D\bar{E}F$	$1.2 \times 10^{-6} + 6.9 \times 10^{-6} = 8.1 \times 10^{-6}$
UVCE	$A\bar{B}CDE + A\bar{B}\bar{C}DE$	$6.1 \times 10^{-6} + 34.5 \times 10^{-6} = 40.5 \times 10^{-6}$
Local thermal hazard	$AB\bar{F}$	$8.0 \times 10^{-6} = 8.0 \times 10^{-6}$
Safe dispersal	$A\bar{B}C\bar{D} + A\bar{B}\bar{C}\bar{D}$	$1.4 \times 10^{-6} + 7.6 \times 10^{-6} = 9.0 \times 10^{-6}$
Total all outcomes		$= 100.0 \times 10^{-6}$

IMPORTANCE MEASURES

BIRNBAUM IMPORTANCE

$R(1) - R(0)$

FUSSEL VESELY IMPORTANCE

$q\ (\ R(1) - R(0)\ )$

q - component unavailability

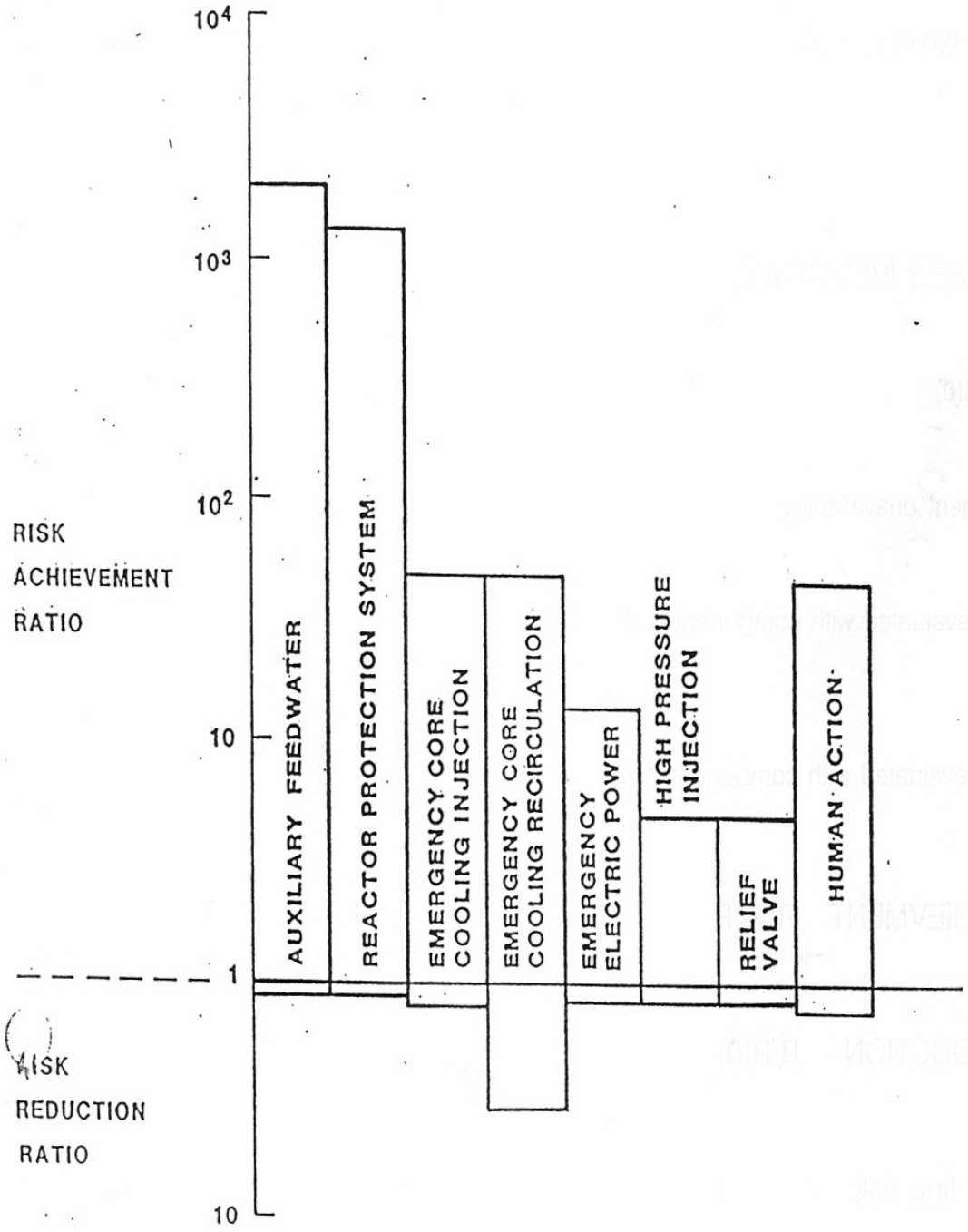
R(0) - risk evaluated with component up
q=0

R(1) - risk evaluated with component down
q=1

RISK ACHIEVMENT $R(1)/R$

RISK REDUCTION $R/R(0)$

R - base line risk



Risk-Worth Ratios for Sequoyah Safety Systems with Regard to Core-Melt Frequency