

Chapter 4 - Probability Tools and Techniques

Introduction

Chapter Content

This chapter presents basic probability tools and techniques, drawing heavily from McCormick¹ for the basic probability theory. Alan Monier guided the bulk of the remainder. Paul Santamaura contributed to improving the chapter..

The objective of this chapter is to provide the basic probability tools and techniques needed to explore reactor safety analysis. This will allow the quantification of the concepts and designs developed in the rest of the course.

Chapter Layout

First, the general rules of probability (AND and OR rules) and Bayes Equation are introduced but, for the most part in this course, we will rely on the approximations of rare and independent events. Time dependent systems are addressed, covering failure rates, repair, continuous operation, and demand systems.

We encounter a simple shutdown system, illustrating the concept of testing to increase system availability. We also consider the basic '2 out of 3' system so prevalent in reactor safety systems. By way of contrast to the shutdown system, which is a demand type system, the emergency core cooling system is also examined as an example of a demand system with a mission time.

Definitions and Rules

If event A occurs x times out of n repeated experiments then:

$$P(A) \equiv \text{probability of event A} \\ = \lim_{n \rightarrow \infty} \left(\frac{x}{n} \right) \quad (1)$$

$$\text{(Axiom \#1)} \quad 0 \leq P(A) \leq 1 \quad (2)$$

$$\text{(Axiom \#2):} \quad P(A) + P(\bar{A}) = 1 \quad \text{where } \bar{A} \text{ means "not A".} \quad (3)$$

In other words, an event must either occur or not occur - there is no third possibility..

The *intersection* of 2 events, A_1 and A_2 , is denoted:

$$A_1 \cap A_2 \quad \text{or} \quad A_1 A_2 \quad \text{or} \quad A_1 \text{ AND } A_2 \\ \text{(This is not } A_1 \text{ times } A_2) \quad (4)$$

$A_1 A_2$ means that *both* events occur, so $P(A_1 A_2)$ is the probability that both events occur.

The *conditional probability* $P(A_1 | A_2)$ means the probability of A_1 given that A_2 has occurred.

The product rule for probabilities states:

$$\text{(Axiom\#3)} \quad P(A_1 A_2) = P(A_1 | A_2) P(A_2) \\ = P(A_2 | A_1) P(A_1) \quad (5)$$

For example, if A_1 is the probability that part 1 fails and A_2 is the probability that part 2 fails then
 $P(A_1 A_2)$ = probability that both part 1 fails and part 2 fails
 = probability that part 2 fails **and** (probability that part 1 fails given that part 2 fails)

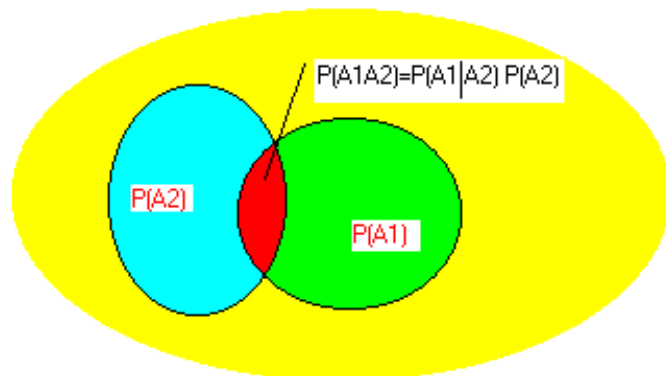


Figure 4-1 - Probability of Both of Two Events

green those events with outcome A1; blue with outcome A2; red, with outcome *both* A1 and A2.

See Appendix 1 for an example.

If the failures are independent,

$$P(A_2 | A_1) = P(A_2).$$

This can be extended to give:

$$P(A_1 A_2 \dots A_N) = P(A_1)P(A_2|A_1) \dots P(A_N|A_1 A_2 \dots A_{N-1}) \quad (6)$$

If events are independent:

$$P(A_1 A_2 \dots A_N) = P(A_1)P(A_2) \dots P(A_N) \quad (7)$$

The *union* of two events is denoted:

$$A_1 \cup A_2 \quad \text{or} \quad A_1 + A_2 \quad \text{or} \quad A_1 \text{ OR } A_2. \quad (8)$$

This means the cases where *either* event occurs, including the cases where *both* events occur.

We have:

$$P(A_1 + A_2) = P(A_1) + P(A_2) - P(A_1 A_2) \quad (9)$$

as shown in the figure. The reason for subtracting $P(A_1 A_2)$ is because what you want is the total area encompassed by the combination of the blue and green ovals in the diagram. If you just add $P(A_1)$ and $P(A_2)$, you count the intersection where both events occur (in red) twice. So you have to subtract one of them away.

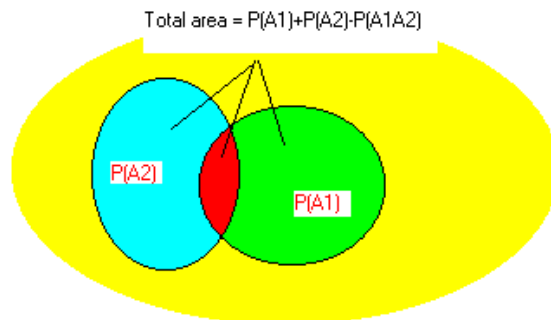


Figure 4-2 - Probability of Either of two Events

In general:

$$P(A_1+A_2+\dots+A_N) = \sum_{n=1}^N P(A_n) - \sum_{n=1}^{N-1} \sum_{m=n+1}^N P(A_n A_m) \pm \dots + (-1)^{N-1} P(A_1 A_2 \dots A_N) \quad (10)$$

If events are independent:

$$1 - P(A_1+A_2+\dots+A_N) = \prod_{n=1}^N [1 - P(A_n)] \quad (11)$$

See Appendix 2 for an example.

Rare events approximation means $P(A_n) \ll 1$, and assuming they are independent:

$$P(A_1+A_2+\dots+A_N) \approx \sum_{n=1}^N P(A_n) \quad (12)$$

and we previously had (equation 7):

$$P(A_1 A_2 \dots A_N) = P(A_1) P(A_2) \dots P(A_N) \quad (13)$$

The Bayes Equation

Given an event or hypothesis, B, and A_n mutually exclusive events or hypotheses ($n=1, 2, \dots, N$):

$$P(A_n B) = P(A_n) P(B|A_n) = P(B) P(A_n|B) \quad (14)$$

$$\therefore P(A_n|B) = P(A_n) \left[\frac{P(B|A_n)}{P(B)} \right] \quad (15)$$

Now, since the events, A_n are mutually exclusive:

$$\sum_{n=1}^N P(A_n|B) = 1 \quad (16)$$

Multiplying by P(B):

$$\begin{aligned}
P(B) &= \sum_{n=1}^N P(B) P(A_n|B) \\
&= \sum_{n=1}^N P(A_n B) \\
&= \sum_{n=1}^N P(A_n) P(B|A_n)
\end{aligned}
\tag{17}$$

Substituting (17) into (15):

$$P(A_n|B) = \frac{P(A_n) P(B|A_n)}{\sum_{m=1}^N P(A_m) P(B|A_m)}
\tag{18}$$

So if we know $P(B|A_n)$ then we can calculate $P(A_n|B)$. This is an important result because it enables you to “reverse” the order of information. This is especially useful for analysing rare events.

Example - Pipe Inspection

Suppose you are radiographing a Class I pipe for a defect. You know from past experience that the likelihood of a defect is one per 100,000 radiographs. You also know that the likelihood of the instrument indicating a defect when there is *no* defect (false positive) is 1%, and the likelihood of indicating a defect when there *is* a defect is 99%. Your test indicates a defect. What is the probability that the pipe actually has a defect?

Solution:

Apply Bayes theorem to two events:

A: pipe has a defect, so $P(A) = 0.00001$

B: instrument says that pipe has a defect, so $P(B)=0.01^a$

^a This is a bit of a simplification using the fact that $P(A)$ is small.. Actually

$$P(B) = P(B|A) P(A) + P(B|notA) P(notA)$$

$$= 0.99 \times .00001 + 0.01 \times 0.99999$$

$$= 0.0100098$$

or approx = 0.01 as stated

In English, the first term is the 99% chance of detecting the defect in the one pipe in 100,000 that has the defect; plus the second term, which is the 1% chance of indicating a false positive in the remaining 99,999 pipes out of 100,000.

$B|A$: instrument says pipe has a defect when it has a defect, so $P(B|A) = 0.99$

What we want is $P(A|B)$, the probability that the pipe actually has a defect when the instrument says it has one.

Using Bayes theorem:

$$P(A|B) = [P(B|A)][P(A)]/P(B)$$

$$= 0.99 \times 0.00001 / 0.01$$

$$= 0.00099$$

Comment:

This seems counterintuitive and suggests the test is not very good in detecting defects, despite the instrument's good accuracy rate. However the fact that the defect is so rare (we need about a hundred thousand samples before we have chance at seeing a real positive) magnifies the small false positive rate so that most positive tests are false positives.

This is quite important in medical tests - even a very accurate test for a rare cancer will often give far more false positives than real ones.

Example - Core Monitoring System

A Core Monitoring System (CMS) is composed of the 3 sensors as shown. All sensors are required to work for the core monitoring system to work.

We know from the manufacturer the failure probabilities over the period of time under consideration (this is the axiomatic data):

$$P(\text{IC}) = 0.02$$

$$P(\text{TS}) = 0.04$$

$$P(\text{PS}) = 0.01$$

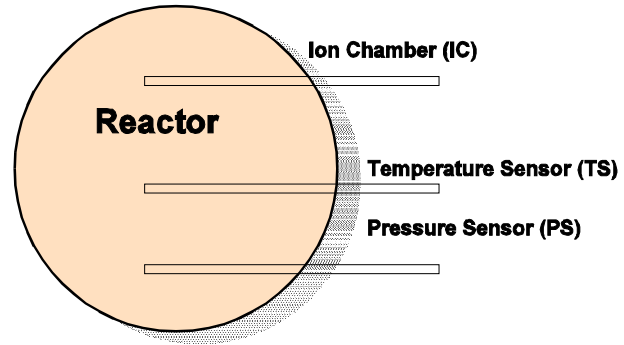


Figure 4-3 - Components of Core Monitoring System

Testing of the installed system shows that $P(\text{CMS}|\text{IC}) = 0.10$ (i.e., when IC fails, the CMS fails 10% of the time).

$$\text{Also } P(\text{CMS}|\text{TS}) = 0.15$$

$$P(\text{CMS}|\text{PS}) = 0.10$$

What is the chance that when CMS fails, TS has also failed?

Solution:

$$\begin{aligned} P(\text{TS}|\text{CMS}) &= \frac{P(\text{TS}) P(\text{CMS}|\text{TS})}{P(\text{IC}) P(\text{CMS}|\text{IC}) + P(\text{TS}) P(\text{CMS}|\text{TS}) + P(\text{PS}) P(\text{CMS}|\text{PS})} \\ &= \frac{0.04 \times 0.15}{0.02 \times 0.10 + 0.04 \times 0.15 + 0.01 \times 0.10} \\ &= 0.667 \end{aligned} \quad (19)$$

Comment:

Based on the axiomatic data $P(\text{IC})$, $P(\text{TS})$ & $P(\text{PS})$ one would expect the TS to be a problem in proportion to its failure rate relative to the other devices i.e.,

$$\frac{0.04}{0.02+0.04+0.01} = \frac{4}{7} \quad (20)$$

So, in the above example, the testing data, $P(\text{B})|A_n$) is used to modify the axiomatic data to yield a revised relative frequency of sensor failure, given a system failure, by $P(A_n|B)$. This is called a *posteriori* probability.

Failure rate estimation when no failures have occurred

We can use Bayes Equation to glean information from non-events as well.

Consider the case where 4000 fuel shipments have been made with no radioactive release.

Can we determine the probability of release per shipment?

Let B = 4000 shipments with no release

What we do now is take six cases, in each of which we hypothesize the value of the release probability. We then use Bayes theorem to test how good our hypotheses are (i.e. calculate the probability that each hypotheses is correct). We label our hypotheses A_1 to A_6 .

$$A_1 = \text{release prob.} = 10^{-3}$$

$$A_2 = \text{release prob.} = 10^{-4}$$

.

.

.

$$A_6 = \text{release prob.} = 10^{-8}$$

If A_1 were true, then:

$$P(B|A_1) = (1-10^{-3})^{4000} = 0.0183$$

since we can assume shipments are independent, the probability of a single success is $1-10^{-3}$, and $P(B|A_1)$ is just the intersection of 4000 events.

Likewise we find (as shown in Figure 4-4):

$$P(B|A_2) = 0.6703$$

$$P(B|A_3) = 0.9608$$

If we know $P(A_1), \dots, P(A_6)$ we could calculate $P(A_n|B)$ or the probability of our statement A_n being

	n					
	1	2	3	4	5	6
A_n	10^{-3}	10^{-4}	10^{-5}	10^{-6}	10^{-7}	10^{-8}
$P(B A_n)$	0.0183	0.6703	0.9608	0.9960	0.9996	0.99996
Uniform prior						
$P(A_n)$	0.1667	0.1667	0.1667	0.1667	0.1667	0.1667
$P(A_n B)$	0.004	0.1443	0.2068	0.2144	0.2152	0.2153
Nonuniform prior ^a						
$P(A_n)$	0.01	0.2	0.4	0.3	0.08	0.01
$P(A_n B)$	0.0002	0.1475	0.4228	0.3287	0.0880	0.0110

^a From S. Kaplan and B. J. Garrick, On the use of a Bayesian reasoning in safety and reliability decisions—three examples, *Nucl. Technol.* 44, 231 (1979).

Figure 4-4 - Bayesian calculations for the example [Source: MCC81, page 19]

actually true. If we assume $P(A_n) = 1/N = 1/6$, we find that $P(A_1|B) = 0.04$, ie, it is not too likely. If we use a more likely $P(A_n)$ we see that $P(A_n|B)$ is adjusted downwards and we conclude that the failure rate is significantly less than 10^{-3} . The practical application of this is in assigning a frequency - e.g., large pipe break - in a Probabilistic Safety analysis, when none have actually occurred and all we have is the number of reactor-years of experience.

Note that one of the criticisms of Bayes theorem when used this way is that the answer depends on the appropriateness of the initial hypotheses. If there is little data and you put in strange hypotheses, you get back strange answers.

Probability Distributions

Let $p(x)dx$ be the probability that an event occurs in an interval x to $x+dx$ - the probability density function. Let $P(X)$ be the cumulative probability that the event occurs somewhere between x_{min} and X . Then

$$\begin{aligned}
 P(X) &= \int_{x_{min}}^X p(x)dx \\
 &= \text{cumulative probability} \\
 &= P(x < X) \\
 &\text{where } p(x) \equiv \text{probability density function.}
 \end{aligned}
 \tag{21}$$

If $p(x)$ is a constant, p_o , then $P(X) = p_o(X-x_{min})$ as expected.

There are two types of systems:

- 1) Those that operate on demand (i.e., safety systems)
- 2) Those that operate continuously (i.e., process systems)

Demand Systems

We define:

$D_n = n^{\text{th}}$ demand

$P(D_n) =$ probability of success on demand n

$P(\bar{D}_n) =$ probability of failure on demand n

$W_n =$ case where system works for each demand up to and including demand n .

What is the probability that it works for $n-1$ demands and fails on demand n ?

$$\therefore P(W_{n-1}) = P(D_1 D_2 D_3 \dots D_{n-1}) \quad (22)$$

$$P(\bar{D}_n | W_{n-1}) = P(\bar{D}_n | W_{n-1}) P(W_{n-1}) \quad (23)$$

So

$$\begin{aligned} P(D_1 D_2 D_3 \dots D_{n-1} \bar{D}_n) &= P(\bar{D}_n | W_{n-1}) P(W_{n-1}) \\ &= P(\bar{D}_n | D_1 D_2 \dots D_{n-1}) \cdot P(D_{n-1} | D_1 D_2 \dots D_{n-2}) \dots P(D_2 | D_1) P(D_1) \end{aligned} \quad (24)$$

If all demands are alike and independent, this reduces to:

$$P(D_1 D_2 \dots D_{n-1} \bar{D}_n) = P(\bar{D}) [1 - P(\bar{D})]^{n-1} \quad (25)$$

Data for demand failure is often published using the symbol Q_d .

Example:

$P(\bar{D})$ for a switch is 10^{-4} . What is the probability that the switch fails at the end of 3 years when the switch is used 20 times per week?

Solution:

Number of demands = $20 \times 52 \times 3 = 3120$.

$$\begin{aligned} \therefore P(\bar{D}_{3120} | W_{3119}) &= 10^{-4} (1 - 10^{-4})^{3119} \\ &= 0.732 \times 10^{-4}. \end{aligned} \quad (26)$$

This is the same as the probability of any single specified failure, say on demand 25 or 87, out of 3120 demands (i.e., it doesn't matter when the failure occurs).

If the switch were repaired immediately upon any failure, then the probability that it would fail *once* at anytime within the 3 years is just 3120 times the probability that it would fail at any specified demand, i.e., $3120 \times 0.732 \times 10^{-4} = 0.228$.

Failure Dynamics

Failures are not static events. Let's look at failure dynamics.

$f(t)dt$ = probability of failure in the interval dt at time t

$$\begin{aligned} F(t) &= \text{accumulated failure probability} \\ &= \int_0^t f(t') dt' \end{aligned} \quad (27)$$

Assuming that the device eventually fails, the reliability, $R(t)$ is defined as

$$\begin{aligned} R(t) &= 1 - F(t) \\ &= \int_0^{\infty} f(t') dt' - \int_0^t f(t') dt' \\ &= \int_t^{\infty} f(t') dt' \end{aligned} \quad (28)$$

So,

$$f(t) = - \frac{dR(t)}{dt} = \frac{dF(t)}{dt} \quad (29)$$

If $\lambda(t) dt$ = probability of failure at time t given successful operation up to time t (defined as the conditional failure rate), then:

$$\begin{aligned} f(t)dt &= \lambda(t) dt R(t) \\ \text{or } f(t) &= \lambda(t) R(t) \\ &= - \frac{dR}{dt} \end{aligned} \quad (30)$$

$$\therefore \frac{dR}{dt} = -\lambda(t) R(t) \quad (31)$$

$$\therefore \frac{dR}{R} = -\lambda(t) dt \quad (32)$$

$$\therefore \int_{R(0)}^{R(t)} \frac{dR}{R} = - \int \lambda(t) dt = \ln R(t) - \ln R(0) \quad (33)$$

Since $R(0) = 1$,

$$R(t) = \exp\left[-\int_0^t \lambda(\tau) d\tau\right] \quad (34)$$

If λ is constant, (i.e., random failures):

$$R(t) = e^{-\lambda t} \quad (35)$$

Given $\lambda(t)$, we can determine everything else. See Figure 4-5 for a summary of commonly used terms and relationships. See Figure 4-6 for typical λ vs t .

Word description	Symbol =	First relationship =	Second relationship =	Third relationship
Hazard rate	$\lambda(t)$	$-(1/R) dR/dt$	$f(t)/(1 - F(t))$	$f(t)/R(t)$
Reliability	$R(t)$	$\int_t^\infty f(\tau) d\tau$	$1 - F(t)$	$\exp\left[-\int_0^t \lambda(\tau) d\tau\right]$
Cumulative failure probability	$F(t)$	$\int_0^t f(\tau) d\tau$	$1 - R(t)$	$1 - \exp\left[-\int_0^t \lambda(\tau) d\tau\right]$
Failure probability density	$f(t)$	$dF(t)/dt$	$-dR(t)/dt$	$\lambda(t)R(t)$

Figure 4-5 - A summary of equations relating $\lambda(t)$, $R(t)$, $F(t)$, and $f(t)$

Mean time to failure (MTTF)

$$\begin{aligned}
 \text{MTTF} &= \frac{\int_0^\infty t f(t) dt}{\int_0^\infty f(t) dt} = \int_0^\infty t f(t) dt \\
 &= \int_0^\infty t \lambda e^{-\lambda t} dt \quad (\text{assuming } \lambda = \text{random}) \\
 &= \frac{1}{\lambda}
 \end{aligned} \quad (36)$$

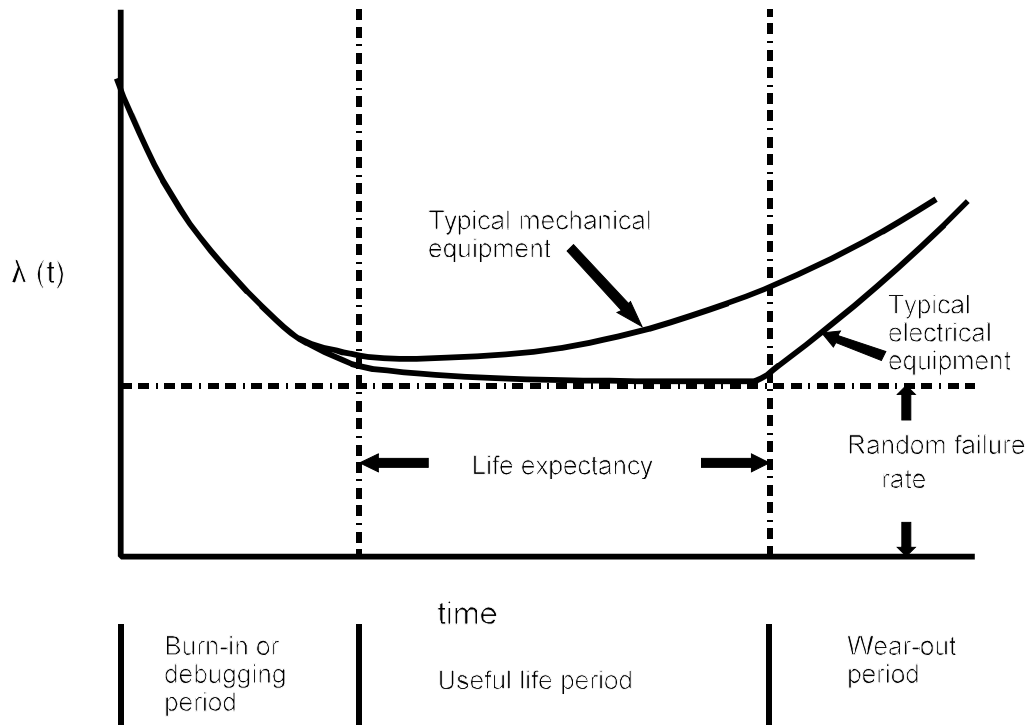


Figure 4-6 - Time dependence of conditional failure (hazard) rate [Source: Ref. 1, page 26]

Availability, $A(t)$

If a device undergoes repair then $R(t) \rightarrow A(t)$

$$R(t) \leq A(t) \leq 1. \quad (37)$$

$A(t) = R(t)$ for devices that are not repaired.

Continuous operation with Repair

Assume random failures. This implies

$$\lambda = \text{constant}$$

$R(t) = e^{-\lambda t}$ = reliability, illustrated in Figure 4-7.

Failure probability = $F(t) \equiv 1 - R(t) \equiv 1 - e^{-\lambda t}$
 illustrated in Figure 4-8.

Let repair occur at time interval, τ . Then $F(t)$ is a sawtooth as illustrated in Figure 4-9.

If $\tau \ll \lambda$ then

$$F(t) = 1 - (1 - \lambda t + \frac{\lambda^2 t^2}{2} \dots) \quad (38)$$

$\approx \lambda t$ for $t < \tau$ in any interval
 and t is measured the time of last repair.

$$\therefore \langle F \rangle = \frac{\lambda \tau}{2} \quad (39)$$

This is a useful rule of thumb but you can always calculate accurately from:

$$\langle F \rangle = \frac{\int_0^\tau F(t) dt}{\int_0^\tau dt} = \frac{t \Big|_0^\tau + \frac{e^{-\lambda t}}{\lambda} \Big|_0^\tau}{\tau} \quad (40)$$

$$= \frac{\lambda \tau + e^{-\lambda \tau} - 1}{\lambda \tau}$$

A common design task is to design a system (composed of components that have a known failure rate) to meet some target unavailability \bar{A} ($\bar{A} = F$). Given a design, the repair interval is the remaining variable. A frequent repair cycle (low τ) gives a low \bar{A} , but such frequent repair may be untenable due to excessive cost on downtime or even hazard to repair personnel. In such a situation, alternative designs would have to be considered.

Often, repair may not be required in order to return F to 0. It may be sufficient to simply test the components to ensure that they are available. This is usually the case for “demand” systems.

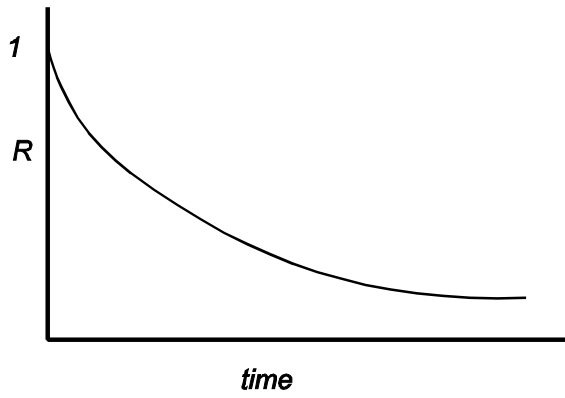


Figure 4-7 - Reliability vs. Time

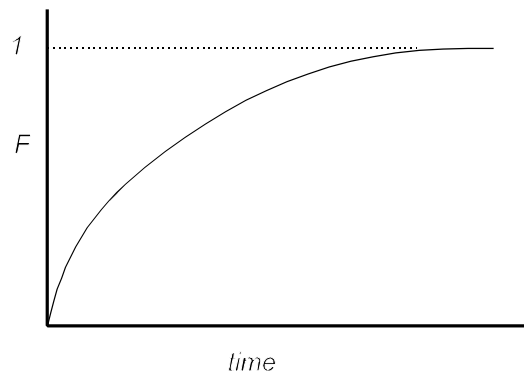


Figure 4-8 - Failure Probability vs. Time

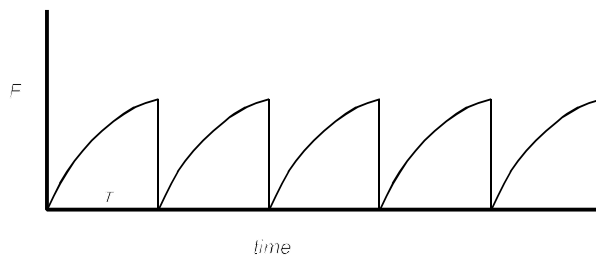


Figure 4-9 - Failure probability with repair

Example - Shutdown System

Consider the case of a single shutoff rod (SOR) for a reactor. Given a failure rate based on previous experience of $\lambda = 0.002/\text{year}$ and a required unavailability of $\leq 10^{-3}$, what is the required test period, τ ?

$$\bar{A} \approx \frac{\lambda\tau}{2} = 0.001 \tau \quad (41)$$

To meet the \bar{A} target of 10^{-3} ,

$$\tau \leq \frac{10^{-3}}{0.001/\text{year}} = 1 \text{ year} \quad (42)$$

This is certainly a reasonable test period. But if the \bar{A} target were 10^{-6} or if the failure rate were 2 / year, then the required test period would be 10^{-3} years or about 3 times per day! This would not be reasonable.

A more realistic shutdown system would have a bank of, say, 6 SORs, as illustrated in Figure 4-10.

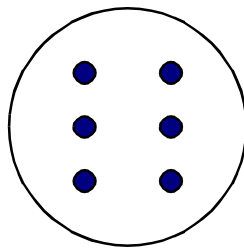


Figure 4-10 - Core with Six SORs (from top)

When the shutdown system (SDS) is activated some, all or none of the rods drop into the core. The possible events are enumerated in Table 4-1.

Assuming that the rods fail independently and that the failure rate is λ , then the probability of a given rod failing on average is:

$$\langle F \rangle \approx \frac{\lambda T}{2} \quad (\equiv p \text{ for conciseness}) \quad (43)$$

as before. And the success probability is $1-p$. In general the probability for event E_k , $k = 1, 2, \dots, N$ is

$$P(E_k) = \frac{N!}{(N-k)!k!} (1-p)^{N-k} p^k \quad (44)$$

The factor $\frac{N!}{(N-k)!k!}$ gives the number of possible ways

for that event to happen, the factor $(1-p)^{N-k}$ is the probability that $N-k$ rods all successfully drop and the factor p^k is the probability that k all fail to drop.

Thus:

$$\begin{aligned} P(E_0) &= (1-p)^6 \\ P(E_1) &= 6(1-p)^5 p \\ P(E_2) &= 15 (1-p)^4 p^2 \\ P(E_3) &= 20 (1-p)^3 p^3 \\ P(E_4) &= 15 (1-p)^2 p^4 \\ P(E_5) &= 6(1-p) p^5 \\ P(E_6) &= p^6 \end{aligned}$$

Since these are the only possibilities, they sum to unity, i.e:

$$\sum_{k=0}^N P(E_k) = 1 \quad (46)$$

Normally, there are more SORs than necessary for reactor shutdown and it is sufficient to require that, say, 4 of the 6 rods must drop. If this were the design criteria, then events E_0 , E_1 and E_2 represent the successful deployment of the SDS. Events $E_3 \rightarrow E_6$ represent system failures.

Table 4-1 - SDS event possibilities

Event	# rods drop	# rods fail to drop
E0	6	0
E1	5	1
E2	4	2
E3	3	3
E4	2	4
E5	1	5
E6	0	6

The system unavailability for a 4 out of 6 criterion is thus:

$$\begin{aligned}\bar{A} &= \sum_{k=3}^6 P(E_k) = 1 - \sum_{k=0}^2 P(E_k) \\ &= 1 - (1-p)^6 - 6(1-p)^5 p - 15(1-p)^4 p^2 \\ \text{where } p &= \frac{\lambda\tau}{2}\end{aligned}\tag{47}$$

Given a λ and an assumed τ , the \bar{A} is calculated and compared to the required unavailability.

The τ is then adjusted until the \bar{A} target (say 10^{-3}) is met. For a λ of, say 0.02/year, we find that

\bar{A} is 2×10^{-5} for a τ of 1 year. Thus testing every year is more than enough for this design to meet the unavailability target.

The above assumes that, when testing occurs, any deficiencies are immediately and instantaneously repaired so that the “clock” is effectively reset and the failure probability is reset to zero. However, repairs cannot usually be made right away. The plant will have to operate with less than 6 SORs available and the unavailability target must still be met.

For instance, assume that the operator finds that one rod fails the test and has to be declared “out of service”. The above calculation needs to be repeated based on a 4 out of 5 criterion rather than a 4 out of 6.

Thus:

$$\begin{aligned}\bar{A} &= 1 - \frac{5!}{5!0!} (1-p)^5 - \frac{5!}{4!1!} (1-p)^4 p \\ &= 1 - (1-p)^5 - 5(1-p)^4 p \\ &\equiv \bar{A}_1 \text{ (to denote unavailability with 1 rod out of service)}\end{aligned}\tag{48}$$

A τ of 1 year gives $\bar{A}_1 = 0.00098$, which just meets the \bar{A} target of 10^{-3} .

We continue in this way by also considering the case where 2 rods fail their test and are taken out of service. Now the SDS must operate on a 4 out of 4 basis. All remaining rods must drop. In this case the unavailability is

$$\bar{A}_2 = 1 - (1-p)^4$$

For $\tau = 1$ year, we find $\bar{A}_2 = 0.039$ and the operator must step up the testing programme

dramatically ($\tau = 0.02$ years or once every week) to achieve $\bar{A}_k = 10^{-3}$ or better.

To summarize:

Table 4-2 - SDS summary

Case	\bar{A}_k	τ (per year)	Operator Action
0 rods fail test	2×10^{-5}	1	None
1 rod fail test	0.00098	1	Repair rod
2 rods fail test	.0008	.02	Repair rods Test every week until rods are repaired
3 or more rods fail test	1		Shutdown since need at least 4 rods available

Fault Tree Example

A more systematic way to carry out the same analysis as per the previous section is to develop a fault tree. We start by identifying the end result (SDS1 fails to deploy) and itemize all the ways that this can happen. In this case, SDS1 can fail in any one of its 7 modes:

- Event E_0 0 rods out of service
- Event E_1 1 rods out of service
- Event E_2 2 rods out of service
- Event E_3 3 rods out of service
- Event E_4 4 rods out of service
- Event E_5 5 rods out of service
- Event E_6 6 rods out of service

These modes are automatic failures since at least 4 rods are required. The reactor is not operated in these modes.

All these modes are mutually exclusive so we OR their probabilities of failures. The fault tree is shown in Figure 4-13.

We digress briefly to explain the symbols used in the fault tree. One starts at the top with the

event of interest, usually the system failure. Then one determines each and every *immediate* cause of such an outcome. If either of several immediate causes is sufficient to cause the “top” event, then they are joined by an “OR” gate, which looks like Figure 4-11. It means: Event A OR event B must occur in order for event C to occur.

Conversely, if *all* of several immediate causes must occur in order to cause the “top” event, then they are joined by an “AND” gate, which looks like Figure 4-12. It means: Event A AND event B must occur in order for event C to occur. It can also be represented by the same symbol containing a \cdot sign

In Figure 4-13 below, the “OR” gate is represented by a symbol as in Figure 4-11. It can also be represented by the same symbol containing a $+$ sign, or just by a line junction (uncommon).

We expand each option until we can no longer decompose the event or we arrive at a point where we know the probability of failure.

For the case of 0 rods out of service, the probability of being in that mode is $(1-p)^6$ as before.

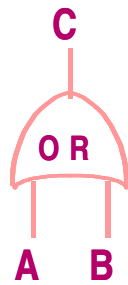


Figure 4-11 -
OR Gate



Figure 4-12 -
AND Gate

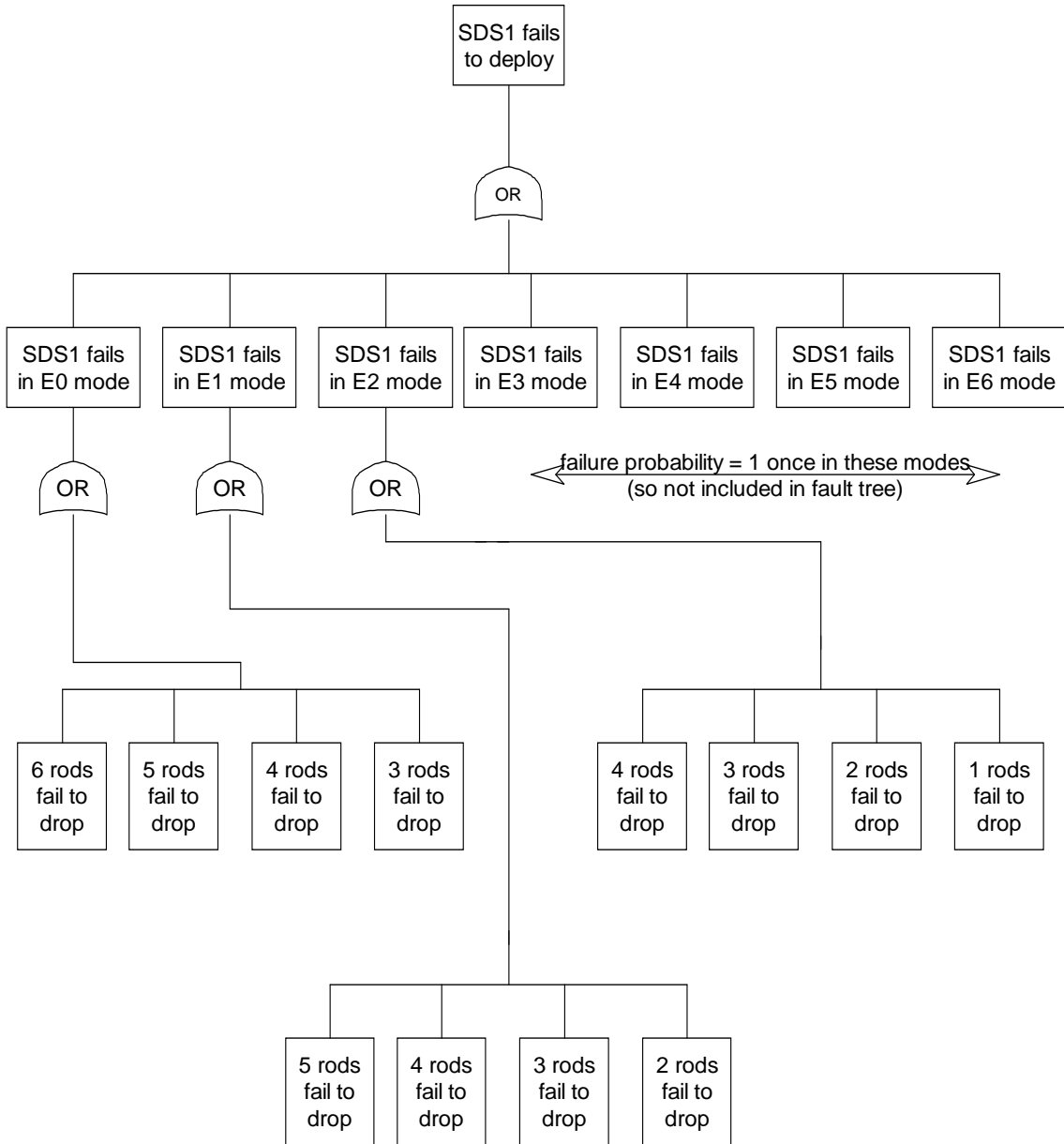


Figure 4-13 - Six ShutOff Rod System Fault Tree

Within that mode, failure occurs if either:

- 6 rods fail to drop [probability of this failure mode = p^6]
- 5 rods fail to drop [probability of this failure mode = $6(1-p)p^5$]
- 4 rods fail to drop [probability of this failure mode = $15(1-p)^2p^4$]
- 3 rods fail to drop. [probability of this failure mode = $20(1-p)^3p^3$]

These events are mutually exclusive. Thus that portion of the tree is expanded as shown. The unavailability of SDS1 while in the E_0 mode is simply:

$$\begin{aligned}\bar{A}_0 &= \sum \text{failure modes when 0 rods are out of service} \\ &= p^6 + 6(1-p)p^5 + 15(1-p)^2p^4 + 20(1-p)^3p^3 \\ \text{where } p &= \frac{\lambda\tau}{2}\end{aligned}\tag{49}$$

The contribution to unavailability of the system for this segment of the fault tree is:

$$\bar{A} \text{ (no rods out of service)} = (1-p)^6 \bar{A}_0\tag{50}$$

The other modes can be expanded in like fashion to give:

$$\begin{aligned}\bar{A}_1 &= \sum \text{failure modes when 1 rod is out of service} \\ &= p^5 + 5(1-p)p^4 + 10(1-p)^2p^3 + 10(1-p)^3p^2\end{aligned}\tag{51}$$

$$\begin{aligned}\bar{A}_2 &= \sum \text{failure modes when 2 rods are out of service} \\ &= p^4 + 4(1-p)p^3 + 2(1-p)^2p^2 + 4(1-p)^3p\end{aligned}\tag{52}$$

Finally, the total system unavailability is:

$$\bar{A} = (1-p)^6 \bar{A}_0 + 6(1-p)^5p \bar{A}_1 + 15(1-p)^4p^2 \bar{A}_2\tag{53}$$

Note that the system unavailability does *not* include the unavailability for modes 3 through 6 since these are modes where the unavailability is *known*. In those cases, the plant would be shut down and put in a fail safe mode by other means. Thus, these modes do not contribute to operating unavailability.

Also note that, in contrast to the example developed in the previous section, the above is based on a common τ . In the previous example τ was varied within each mode to meet the target unavailability so that:

$$\bar{A} = \bar{A}_0 = \bar{A}_1 = \bar{A}_2 = \bar{A}_{\text{target}}\tag{54}$$

2 / 3 Logic Example

Figure 4-14 illustrates a relay setup that operates on a 2 out of 3 logic, or 2/3 logic. There are 3 physical relays, D, E and F but each relay has two sets of terminal pairs, allowing them to be connected as shown. The relays are normally open but close when a signal (D, E or F) from their respective channels are received. If any two channels are activated, then the circuit is completed and current can flow between top and bottom. If the sub-circuit is in a safety system circuit, the safety system is activated when two or more of channels D, E and F are TRUE. If the probability of failure of any relay is p , what is the overall unavailability of the sub-circuit?

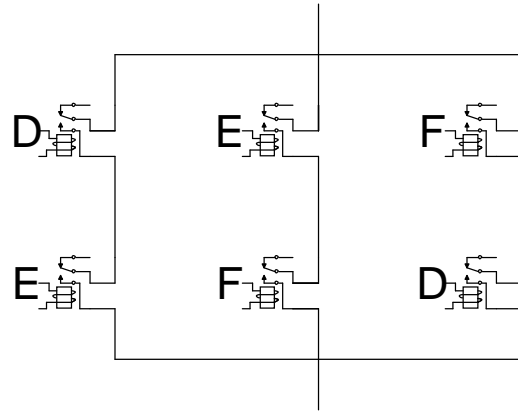


Figure 4-14 - '2 out of 3' Logic - Relay example

This situation is, in fact, completely similar to the SOR case previously examined. Here success is defined as 2 out of 3 events occurring. The unit fails if 3 relays fail or if 2 relays fail. All other states constitute a working sub-system. This is summarized in Table 4-3. All the states are mutually exclusive. The unavailability, then of the unit is simply the sum of the failure probabilities:

$$\begin{aligned} \bar{A} &= \frac{3!}{3! 0!} p^3 + \frac{3!}{2! 1!} p^2 (1-p) \\ &= p^3 + 3 p^2 (1-p) \end{aligned} \quad (55)$$

In general, for a M out of N system:

$$\begin{aligned} \bar{A} &= \sum_{k=M}^{k=N} \frac{N!}{(N-k)!k!} (1-p)^{N-k} p^k \\ &= 1 - \sum_{k=0}^{k=M-1} \frac{N!}{(N-k)!k!} (1-p)^{N-k} p^k \end{aligned} \quad (56)$$

Table 4-3 - Possible sub-system states and probabilities

Condition of relays DEF (1 = OK, 0 = FAILED)	Condition of sub-system	Probability
000	0	p^3
001	0	$p^2 (1-p)$
010	0	$p^2 (1-p)$
011	1	$p (1-p)^2$
100	0	$p^2 (1-p)$
101	1	$p (1-p)^2$
110	1	$p (1-p)^2$
111	1	$(1-p)^3$

Ladder Logic

Consider now the system shown in Figure 4-15 (a) where the relays D, E and F have two sets of terminals just like the previous example. In the standby or ready state, the relays are energized closed, providing a current path from top to bottom. When the system “fires”, i.e., when signals are received at the relays, the current path is broken if at least 2 relays change state (go from closed to open). Failure of a component (a relay in this case) occurs when it fails to change state as requested. The failure modes are the same as for the previous example and are given in Table 4-3. We conclude that the system depicted by Figure 4-15 is entirely equivalent to that of Figure 4-14.

Since safety systems are generally wired so that a power failure will invoke the safety system, the ready state has the relays powered closed and the relays open when power is lost. The relays are designed to fail open, thereby tending to fire the safety system if the safety system logic or components fail. The McMaster Nuclear Reactor safety trip signals, for instance, are all wired in series and any one signal breaks the current to the magnetic clutches holding up the shutoff rods.

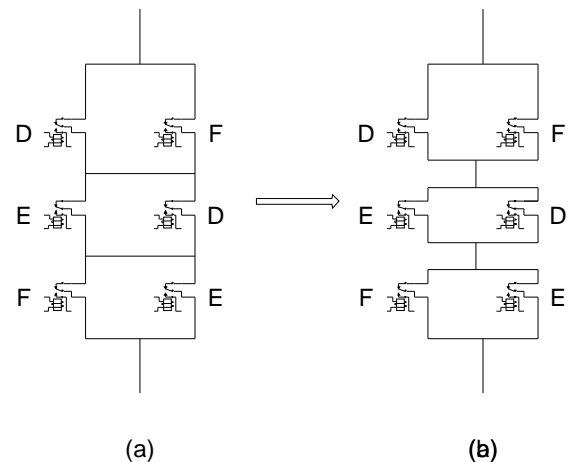


Figure 4-15 - '2 out of 3' Ladder Logic

In actual systems, the relays of the ladder shown in Figure 4-15 do not have dual terminals. Rather, separate relays are used, depicted as D1, D2, etc. in Figure 4-16.

Failure of the system due to relay failures now occurs when all 3 ladder steps fail, ie, when step 1 fails AND step 2 fails AND step 3 fails. The system will succeed if any step succeeds in breaking the circuit (assuming signals at all 3 channels D, E and F).

Step 1 fails if either D1 or F2 fails to switch state upon demand (from closed to open). The fault tree is shown in Figure 4-17. The system unavailability is thus:

$$\begin{aligned} \bar{A} &= (\bar{D1} + \bar{F2}).(\bar{E1} + \bar{D2}).(\bar{F1} + \bar{E2}) \\ &= (2p)^3 = 8p^3 \end{aligned} \quad (57)$$

if all relays fail with probability p . Since $p \ll 1$, the unavailability of this circuit with 6 relays is significantly lower than the previous example which uses 3 relays.

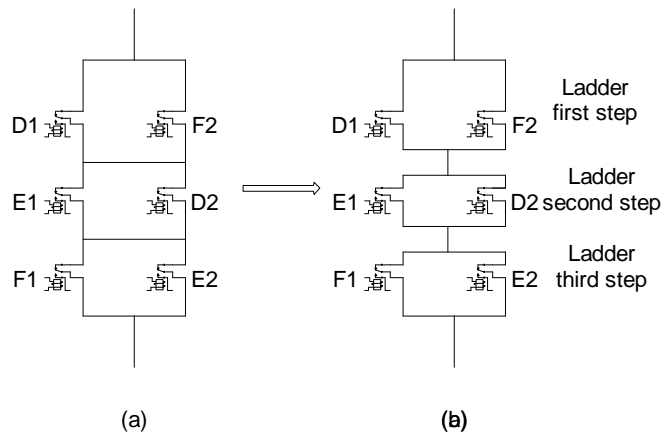


Figure 4-16 - '2 out of 3' Ladder Logic - Separate Relays

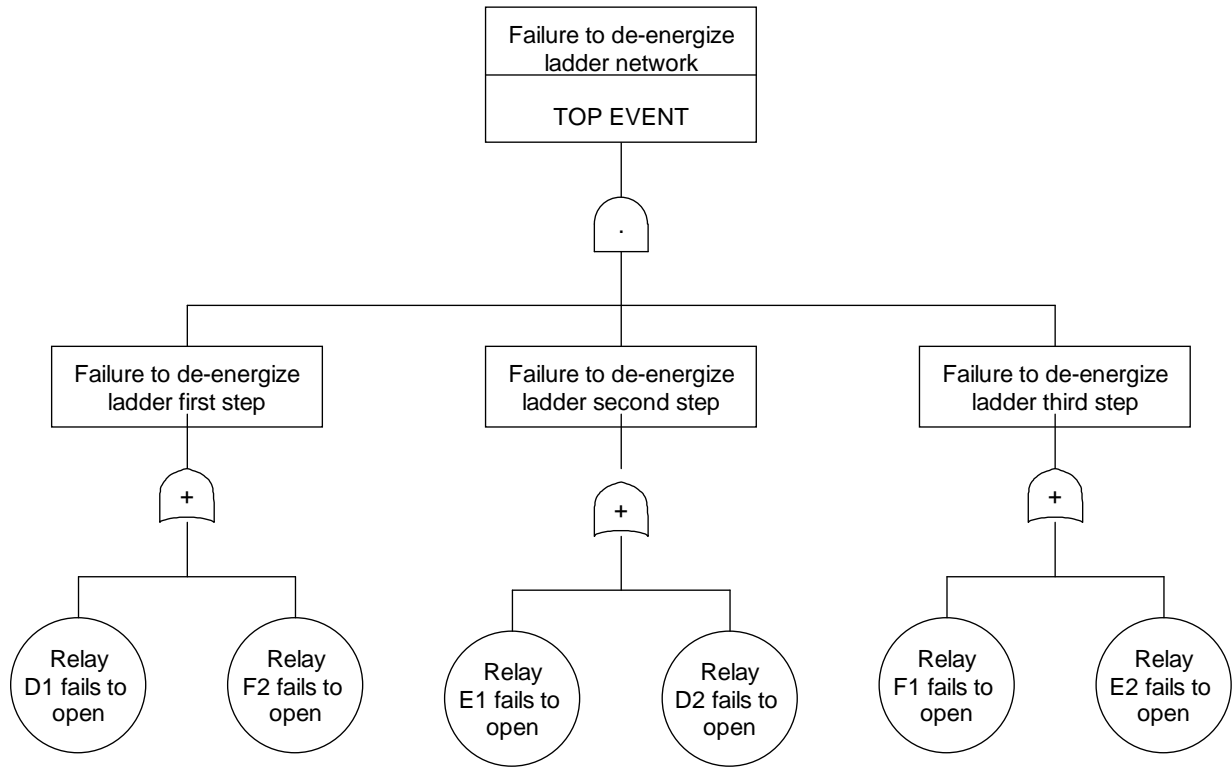
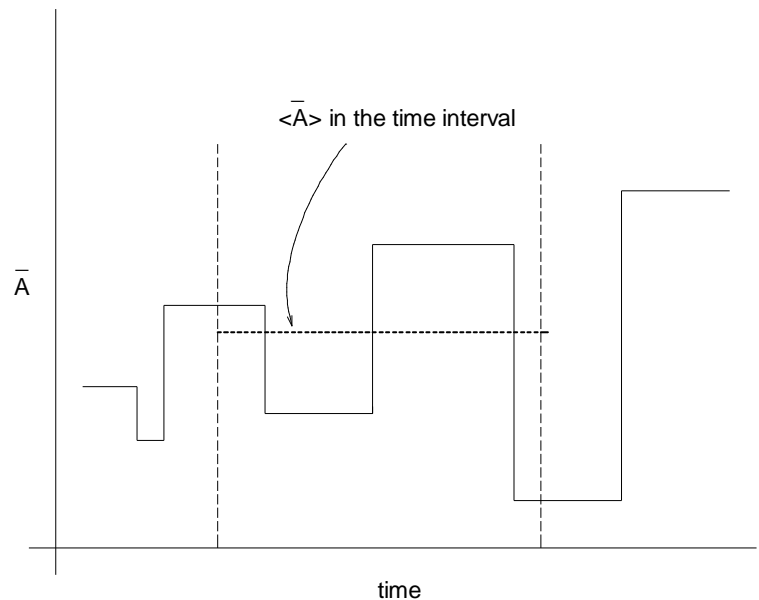


Figure 4-17 - Fault Tree for the Ladder Logic Relays

Unavailability Targets

The unavailability of a system at any given time is, in general, a function of the system configuration. Valves, switches, etc., fail from time to time. System configuration is a function of time. Hence, unavailability is a function of time, as illustrated in Figure 4-18. Safety targets can be defined in terms of some average unavailability \bar{A} or in terms of an instantaneous unavailability. In the later case, the operating station would need to continuously monitor the plant status in order to continuously calculate the station “risk” level. This is likened to having a “risk meter” for the station. Station personnel would respond to equipment failures that lead to a rise in station risk by fixing equipment, maintaining equipment or invoking standby or alternate systems. Working to an average unavailability, on the other hand, does not require such vigilance; instantaneous risk can be permitted to rise in the short term as long as the averages are achieved. This is more workable but less precise in maintaining control of station risk.

Having said that, many stations are using what is effectively an (analytical) ‘core melt’ meter. Core melt being the only event that can lead to significant public health effects, it is important to know whether changes in station configuration - such as equipment unavailability - lead to a significant increase in the likelihood of core melt during that period. This is particularly true during maintenance outages - what degradation in heat sink redundancy is acceptable, for example?



d:\teach\ep7\ola_aver.flo

Figure 4-18 - Time dependent unavailability

Dormant vs active systems

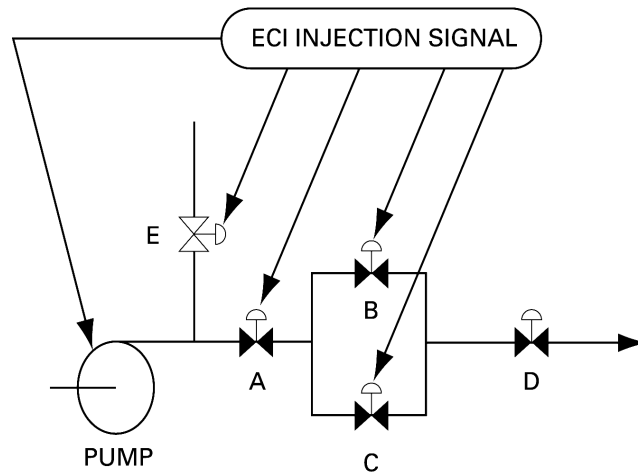
So far we have focussed on systems that are normally dormant and are required to operate on demand. Safety systems generally fall into this category. However, some systems, like the Emergency Core Cooling System (ECCS), are required to activate on demand *and* to continue to function for some defined mission time. The normal response of the ECC to a Heat Transport System (HTS) break (Loss of Coolant Accident or LOCA) is for the ECC to detect the event and initiate the injection of high pressure (HP) cooling water (strictly speaking the water injection function of ECC is called ECI, or Emergency Coolant Injection, since it has other functions such as steam generator cooldown and loop isolation^b). Then, after the HTS has depressurized, medium pressure and finally low pressure water is injected. The HP water is supplied, for example, from a water tank (accumulator) pressurized by huge gas cylinders. Medium pressure cooling water can be supplied from a water tank via ECC pumps; and low pressure water is retrieved from the sumps, cooled and pumped back into the HTS. For CANDU reactors a mission time of 1 to 3 months has been set^c. The ECCS is consequently divided into two separate fault trees for the purposes of analysis: Dormant ECC and Long Term ECC (designated DECC and LTECC respectively). The DECC fault tree focusses on failure to detect the LOCA event, failure to initiate high pressure (HP) cooling water, failure to distribute the flow, and failure to provide medium and low pressure water. The LTECC fault tree focusses on the failure to provide long term low pressure cooling due to pump failure, valve failure, flow blockage, loss of electrical power and loss of coolant supply.

^bSuch a distinction is made in Canada but most other places just use ECC

^cThe mission time is calculated as the time beyond which the decay heat can be removed from the fuel to the moderator *without any water in the fuel channel*, so as to prevent any further fuel failures due to overheating.

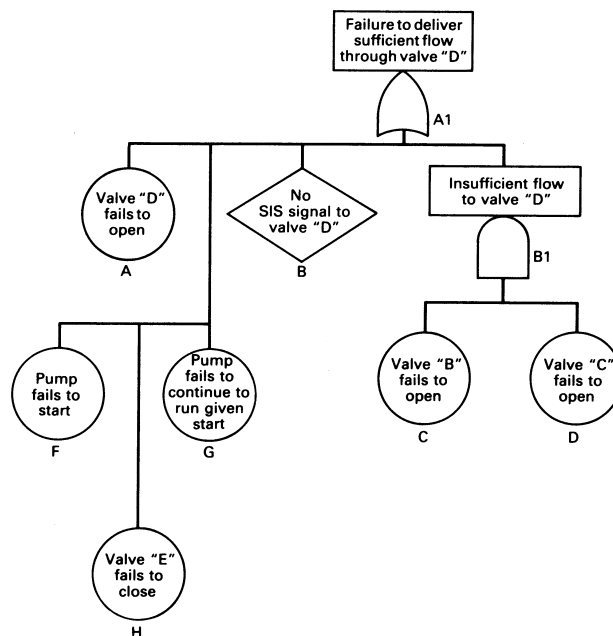
Exercises

1. For the example fault tree of shutoff rods, calculate \bar{A}_0 from the success modes. Which way is better
 - a. in the 4/6 case
 - b. in the 26/28 case?
2. From Ref. 1: A horn on a car operates on demand 99.96% of the time. Consider each event independent from all others. How many times would you expect to be able to honk the horn with a 50% probability of not having a single failure?
3. From Ref. 1: A light bulb has a $\lambda(t) = 5 \times 10^{-7} t$, where t is the time in days. What is the MTTF for the bulb?
4. What can you say quantitatively about the probability of a large LOCA in a CANDU?
5. In a fuel plant, two assembly lines, L1 and L2 produce 40% and 60% respectively of the fuel pellets. From past experience, it is known that 0.1% of L1 and 2% of L2 of the fuel pellets are defective. If a fuel pellet was chosen randomly and found defective, what is the probability that it was produced by L1?
6. Describe the advantages and disadvantages of Bayesian techniques for risk evaluations. What applications could you use Bayesian techniques in an operating nuclear power plant?
7. Two x 100% electrical motor driven auxiliary feedwater pumps are located in the turbine building and depend on recirculated cooling water and two independent power supplies. Identify common mode and cause failures. The utility wants to extend the life of the plant and is planning refurbishment. What mitigation features or modifications would you do to reduce or eliminate these failures?
8. Based on the slide below showing a simple emergency coolant injection system and the results of the fault tree analysis below, identify any weaknesses of the design. Draw a schematic of the system to improve the system reliability. Calculate the unavailability if the pump and valves have a failure rate of 0.01/y and 0.002/y respectively. How would you meet an unavailability of 1E-3? List any assumptions.

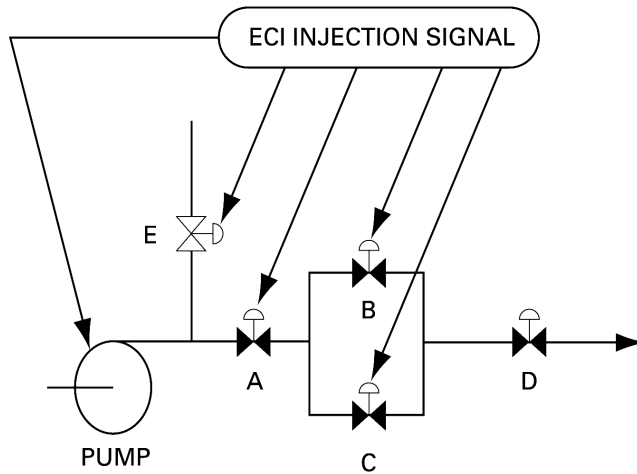


Actions for necessary for success:

- 1 Start pump
- 2 Close valve 'E'
- 3 Open valves 'A' and 'D'
- 4 Open either or both valves 'B', 'C'



9. Consider the simplified ECC system shown below.



Assuming the signal has a demand failure probability of 0.005, the pump has a demand failure probability of 0.02 and each valve has a demand failure probability of 0.01, work out the demand failure probability of the system.

Note: Actions for necessary for success:

- 1 Start pump
- 2 Close valve 'E'
- 3 Open valves 'A' and 'D'
- 4 Open either or both valves 'B', 'C' (i.e. valves are 2 x 100%)

Appendix 1 - Example of Common Cause Failure

Consider two shutoff rods, each of which has a probability of failure of 0.001 per demand. What is the probability that they both fail when required?

If they are independent, then $P(A1A2) = P(A1)P(A2) = (0.001)^2 = 10^{-6}$ per demand.

Suppose there is a common cause failure 10% of the time. That is:

$$P(A1) = P(A2) = 0.0009 \text{ (random)} + 0.0001 \text{ (CC)}$$

so the probability of one rod failing *given that the other has failed* is 90% random and 10% common cause (with probability 1):

$$P(A1|A2) = 0.9 * 0.001 + 0.1 * 1 = 0.1009$$

or

$$P(A1A2) = 0.1009 * 0.001 = 0.0001009 \sim 10^{-4}$$

Thus a 10% common cause probability has increased the combined failure by a factor of 100!

Appendix 2 - Example of Probabilities for “OR”ed Events

Recall for independent events:

$$1 - P(A_1 + A_2 + \dots + A_N) = \prod_{n=1}^N [1 - P(A_n)] \quad (58)$$

Let’s take an example to see how this works. Take two dice. What is the probability that die 1 shows a six OR die 2 shows a six (i.e., that there is *at least* one six). Recall:

$$P(A_1 + A_2) = P(A_1) + P(A_2) - P(A_1 A_2) \quad (59)$$

Since $P(A_1) = P(A_2) = 1/6$, and $P(A_1 A_2) = 1/36$, then clearly

$$P(A_1 + A_2) = 1/6 + 1/6 - 1/36 = 11/36.$$

Confirm by counting:

Die 1	Die 2	Number of Cases showing ‘six’
1	123456	1
2	123456	1
3	123456	1
4	123456	1
5	123456	1
6	123456	6
Total Combinations Showing ‘six’		11

[Aside: Note that if the question had been “What is the probability that there is *only* one six showing (i.e., that die 1 shows a six OR die 2 shows a six but not both), then you have to subtract off the intersection again, i.e.,

$$P(A_1+A_2) = P(A_1) + P(A_2) - 2 P(A_1A_2) \quad (60)$$

or

$$P(A_1+A_2) = 1/6 + 1/6 - 1/36 - 1/36 = 10/36.]$$

Here is another way of looking at it. The probability of getting one or more sixes is [1 - the probability of getting no sixes], since the events are mutually exclusive and complete:

$$P(\text{at least one six}) = 1 - P(\text{no sixes})$$

The probability of getting no sixes for each die is [1 - the probability of getting a six]. The probability of getting no sixes for both dies is the product of the probability of getting no six for each die, since the events are independent (see equation 7):

$$P(\text{no six for die 1}) = 1 - P(\text{six for die 1})$$

$$P(\text{no six for die 2}) = 1 - P(\text{six for die 2})$$

So:

$$P(\text{no six for die 1 AND no six for die 2}) = [1 - P(\text{six for die 1})][1 - P(\text{six for die 2})]$$

Hence

$$\begin{aligned} P(\text{at least one six}) &= 1 - P(\text{no sixes}) = 1 - [1 - P(\text{six for die 1})][1 - P(\text{six for die 2})] \\ &= 1 - [1 - 1/6][1 - 1/6] = 1 - 25/36 = 11/36 \end{aligned}$$

as we had before.

There are two lessons from this example:

- if you're having trouble understanding some of the arcane equations of probability theory, work through some examples. Mathematicians and purists may cringe - but real science goes from example to theory, not the other way around.
- sometimes it is easier to work from the probability of the complementary event - $P(\text{not } A)$ or $P(\bar{A})$ - rather than the probability of the event - $P(A)$, remembering that

$$P(\bar{A}) = 1 - P(A)$$

In this example it didn't make much difference. However suppose you had a thousand dice and asked the same questions - which approach (equation 10 or equation 11) would be easier to use?

References

1. Norman J. McCormick, *Reliability and Risk Analysis*, Academic Press, 1981, ISBN 0-12-482360-2.