Chapter 2 Probability Tools and Techniques

2.1 Introduction

2.1.1 Chapter Content

This chapter presents basic probability tools and techniques, drawing heavily from McCormick [MCC81] for the basic probability theory (up to Section 2.9). Alan Monier guided the bulk of the remainder.

2.1.2 Learning Outcomes

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. The overall learning outcomes for this chapter are as follows:

Objective 2.1	The student should be able to identify the terms and symbols used in probability calculations.					
Condition	Closed book written examination.					
Standard	100% on key terms and symbols.					
Related concept(s)						
Classification	Knowledge	Comprehension	Application	Analysis	Synthesis	Evaluation
Weight	a	a				

Objective 2.2	The student should be able to recall typical values and units of parameters.					
Condition	Closed book written or oral examination.					
Standard	100% on key terms and symbols.					
Related concept(s)						
Classification	Knowledge	Comprehension	Application	Analysis	Synthesis	Evaluation
Weight	a					

Objective 2.3	The student should be able to analyse simple systems and compute unavailabilities.					
Condition	Open book written examination.					
Standard	75%.					
Related concept(s)						
Classification	Knowledge	Comprehension	Application	Analysis	Synthesis	Evaluation
Weight	a	a	a	a		

2.1.3 The 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.

2.2 Definitions and Rules

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

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

(*Axiom* #1) $$0 \le P(A) \le 1 \tag{2}$$

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

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

$$A_1 \cap A_2 \quad \text{or} \quad A_1A_2 \quad \text{or} \quad A_1 \text{ AND } A_2 \quad (\text{This is } \underline{\text{not}}\ A_1 \text{ times } A_2) \tag{4}$$

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

The product rule for probabilities states:

(*Axiom*#3) $$P(A_1\ A_2) = P(A_1|A_2)\ P(A_2) = P(A_2|A_1)\ P(A_1) \tag{5}$$

For example, if A_1 is the probability that part 1 fails and A_2 is the probability that part 2 fails then

$P(A_1\ A2)$ = probability that both 1 and 2 fail
= probability that 2 fails and (part 1 fails given that part 2 fails).

If the failures are independent,

$P(A2 \mid A_1) = P(A_2)$.

This can be extended to give:

$$P(A_1A_2....A_N) = P(A_1)P(A_2|A_1)....P(A_N|A_1A_2....A_{N-1}) \tag{6}$$

If events are independent:

$$P(A_1A_2....A_N) = P(A_1)P(A_2)....P(A_N) \tag{7}$$

The union of two events is denoted:

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

We have:

$$P(A_1+A_2) = P(A_1) + P(A_2) - P(A_1A_2) \tag{9}$$

In general:

$$P(A_1+A_2+...+A_N) = \sum_{n=1}^{N} P(A_N) - \sum_{n=1}^{N-1}\sum_{m=n+1}^{N} P(A_nA_m) \pm ... +(-1)^{N-1}P(A_1A_2...A_N) \tag{10}$$

If events are independent:

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

Rare events approximation (and independent)

$$P(A_1 + A_2 + \ ... \ A_N) \simeq \sum_{n=1}^{N} P(A_N) \tag{12}$$

and we previously had (equation 7):

$$P(A_1 A_2 .... A_N) = P(A_1)P(A_2).....P(A_N) \tag{13}$$

2.3 The Bayes Equation

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

$$P(A_nB) = P(A_n)\ P(B|A_n) = P(B)P(A_n|B) \tag{14}$$

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

Now, since the events, A_n are mutually exclusive:

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

Multiplying by P(B):

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

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 analyzing rare events.

2.4 Example - Core Monitoring System

A Core Monitoring System (CMS) is composed of the 3 sensors as shown:

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

P(IC) = 0.02
P(TS) = 0.04
P(PS) = 0.01

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

Also P(CM|TS) = 0.15
P(CMS|PS) = 0.10

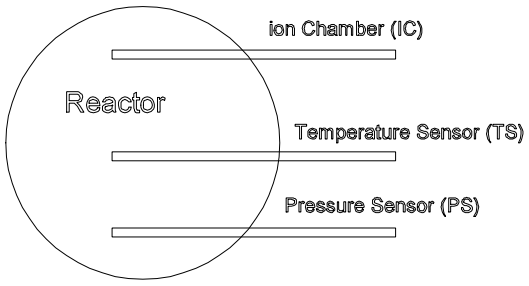

Figure 2.1 Core Monitoring System

What is the chance that a failed CMS is caused by a failed TS?

Solution:

$$P(TS|CMS) = \frac{P(TS)\ P(CMS|TS)}{P(IC)\ P(CMS|IC) + P(TS)\ P(CMS|TS) + P(PS)\ P(CM|TS)}$$
$$= \frac{0.04 x 0.015}{0.02\ x\ 0.10 + 0.04\ x\ 0.15 + 0.01\ x\ 0.10} \qquad (19)$$
$$= 0.667$$

Comment:

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

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

So, in the above example, the testing data, $P(B)|A_n)$ 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 posterior probability.

2.5 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
A_1 = release prob. = 10^{-3}
A_2 = release prob. = 10^{-4}
.
.
.
A_6 = 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 table 2.1):

$P(B|A_2) = 0.6703$
$P(B|A_3) = 0.9608$

Table 2.1 Bayesian calculations for the example [Source: MCC81, page 19]

	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).

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

2.6 Probability Distributions

$$P(X) = \int_{x_{min}}^{X} p(x)dx$$
$$= \text{cumulative probability} \quad (21)$$
$$= P(x < X)$$

where $p(x) \equiv$ probability density function.

There are two types of systems:

1) Those that operate on demand (ie, safety systems)
2) Those that operate continuously (ie, process systems)

2.7 Demand Systems

We define:

$D_n \equiv n^{th}$ demand

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

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

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

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

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

So

$$\begin{aligned} P(D_1D_2D_3\ldots D_{n-1}\ \bar{D}_n) &= P(\bar{D}_n|W_{n-1})\ P(W_{n-1}) \\ &= P\ (\bar{D}_n|D_1D_2\ldots D_{n-1})\ .\ P\ (D_{n-1}|D_1D_2\ldots D_{n-2})\ldots P(D_2|D_1)\ P(D_1) \end{aligned} \tag{24}$$

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

$$P(D_1D_2\ldots D_{n-1}\bar{D}_n) = P(\bar{D})\ [1-P(\bar{D})]^{n-1} \tag{25}$$

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 = 20x52x3 = 3120.

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

This is the same as any single specified failure, say on demand 25 or 87.

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 x 0.732 x 10^{-4} = 0.228.

2.8 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

$$F(t) = \text{accumulated failure probability} = \int_0^t f(t')dt' \tag{27}$$

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

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

So,

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

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

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

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

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

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

Since R(0) = 1,

$$R(t) = \exp\left[-\int_0^t \lambda(t)dt\right] \tag{34}$$

If λ is constant, (ie, random failures):

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

Given $\lambda(t)$, we can determine everything else. See table 2.2 for a summary of commonly used terms and relationships. See figure 2.2 for typical λvs t.

Table 2.2 A summary of equations relating $\lambda(t)$, R(t), F(t), and f(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	$f(t)$	$dF(t)/dt$	$-dR(t)/dt$	$\lambda(t)R(t)$

Mean time to failure (MTTF)

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

Availability, A(t)

If a device undergoes repair then R(t) → A(t)

$$R(t) \le A(t) \le 1. \tag{37}$$

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

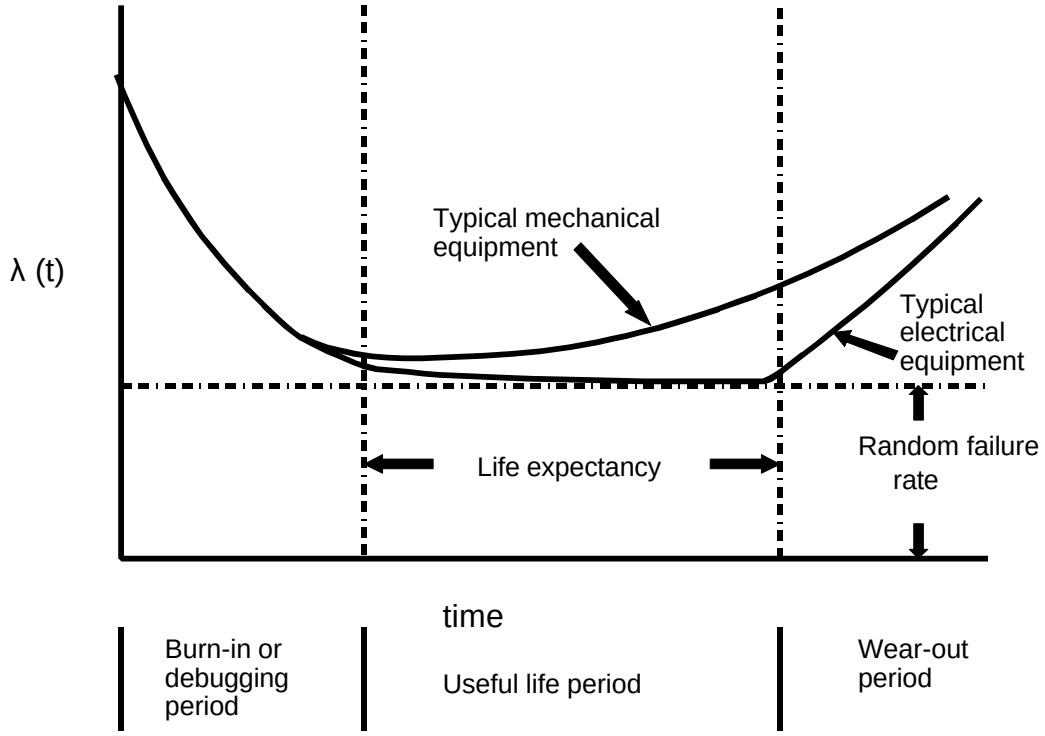

Figure 2.2 Time dependence of conditional failure (hazard)rate [Source: MCC81, page 26]

2.9 Continuous operation with Repair

Assume random failures. This implies

λ = constant

$R(t) = e^{-\lambda t}$ = reliability, illustrated in figure 2.3.

Failure probability = $F(t) \equiv 1 - R(t)$

$\equiv 1 - e^{\lambda t}$, illustrated in figure 2.4.

Let repair occur at time interval, τ. Then F(t) is a sawtooth as illustrated in figure 2.5.

If $\tau << \lambda$ then

$$F(t) = 1 - \left(1 - \lambda t + \frac{\lambda^2 t^2}{2} ...\right) \approx \lambda t \quad \text{for } t < \tau \text{ in any interval and t is measured the time of lastrepair.} \tag{38}$$

$$\therefore \langle F \rangle = \frac{\lambda \tau}{2} \quad . \tag{39}$$

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

$$\langle F \rangle = \frac{\int_0^\tau F(t)dt}{\int_0^\tau dt} = \frac{t\Big|_0^\tau + \frac{e^{-\lambda t}\Big|_0^\tau}{\lambda}}{\tau} = \frac{\lambda\tau + e^{-\lambda\tau} - 1}{\lambda\tau}. \tag{40}$$

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.

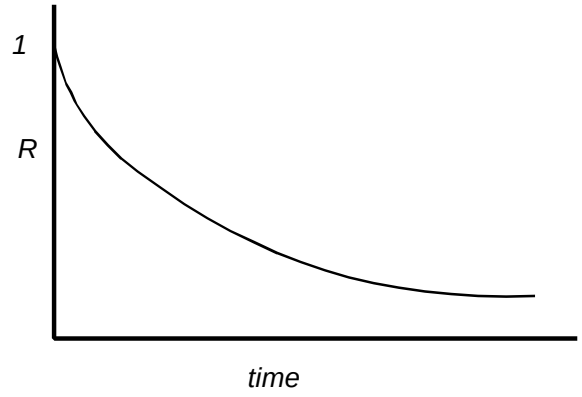

Figure 2.3 Reliability vs. Time

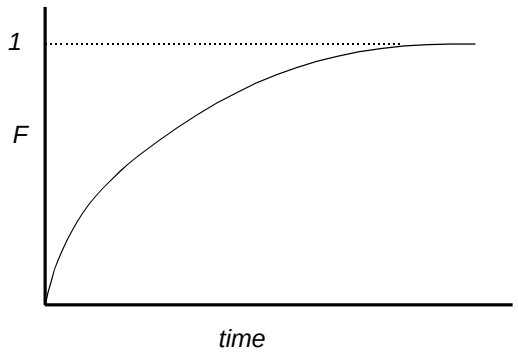

Figure 2.4 Failure probability vs. Time

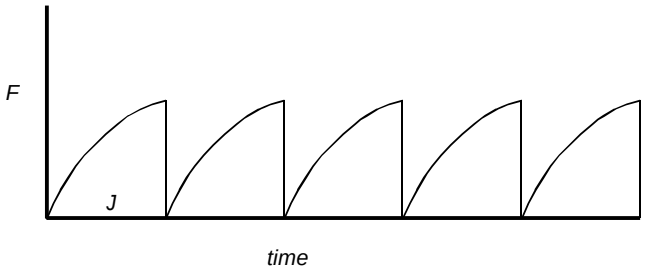

Figure 2.5 Failure probability with repair

2.10 Example - Shutdown System

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

$$\bar{A} \approx \frac{\lambda\tau}{2} = 0.001\ \tau \tag{41}$$

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

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

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 2.5.

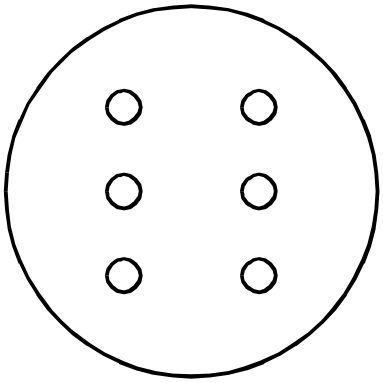

Figure 2.6 Simple SDS

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 2.3.

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

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

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

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

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.

Table 2.3 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

Thus:

$P(E_o) = (1\text{-}p)^6$
$P(E_1) = 6(1\text{-}p)^5 p$
$P(E_2) = 15\ (1\text{-}p)^4 p^2$
$P(E_3) = 20\ (1\text{-}p)^3 p^3$
$P(E_4) = 151\text{-}p)^2 p^4$
$P(E_5) = 6(1\text{-}p) p^5$
$P(E_6) = p^6$

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

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

Normally, there are more SOR's 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_o, E_1 and E_2 represent the successful deployment of the SDS. Events $E_3 \rightarrow E_6$ represent system failures.

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

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

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:

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

A τ of 1 year gives $\bar{A}_1 = 0.00098$, which <u>just</u> 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

$A_2 = 1 - (1-p)^4$

For τ = 1 year, we find $\bar{A}_2 = 0.039$ and the operator must step up the testing program dramatically (τ = 0.02 years or once every week) to achieve $\bar{A} = 10^{-3}$ or better.

To summarize:

Table 2.4 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

2.11 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.

All these modes are mutually exclusive so we OR
their probabilities of failures. The fault tree is shown in figure 2.6. 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 $(1\text{-}p)^6$ as before. 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 = $6\,(1\text{-}p)\,p^5$]
4 rods fail to drop [probability of this failure mode = $15\,(1\text{-}p)^2\,p^4$]
3 rods fail to drop.[probability of this failure mode = $20\,(1\text{-}p)^3\,p^3$]

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 <u>not</u> include the unavailability for modes 3 through 6 since these are

modes where the unavailability if 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:

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

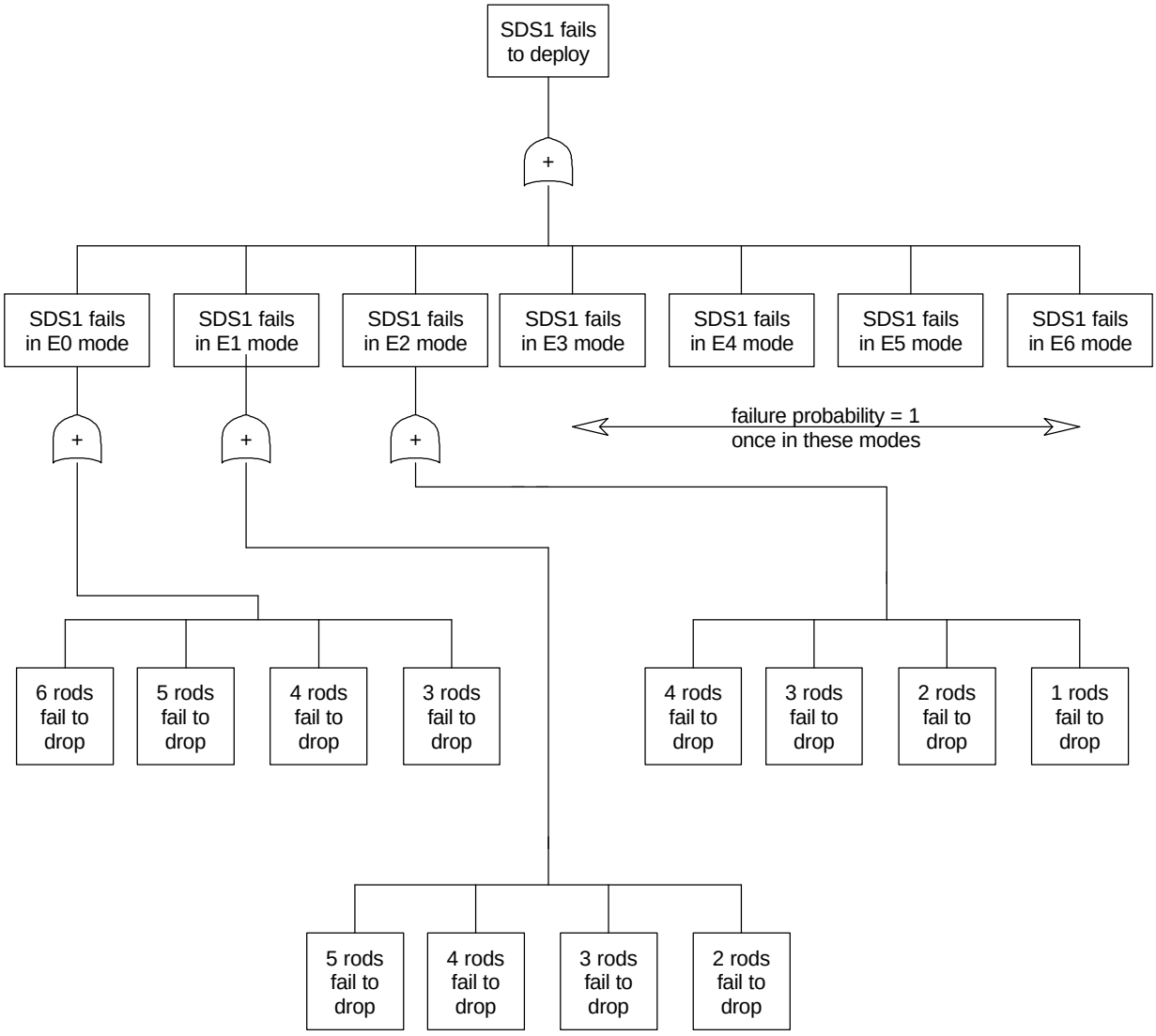

Figure 2.7 SDS1 fault tree

2.12 2 / 3 Logic Example

Figure 2.8 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?

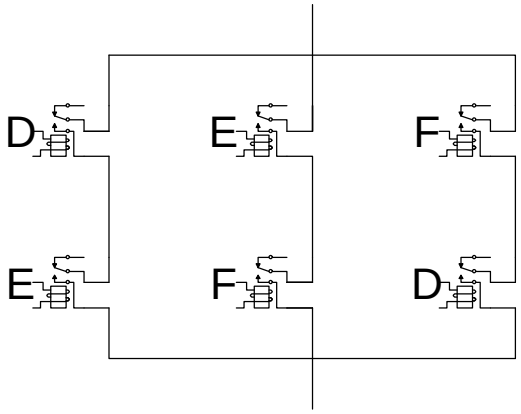

Figure 2.8 '2 out of 3' Logic - Relay example

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 2.4. All the states are mutually exclusive. The unavailability, then of the unit is simply the sum of the failure probabilities:

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

In general, for a M out of N system:

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

Table 2.5 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	p $(1-p)^2$

2.13 Ladder Logic

Consider now the system shown in Figure 2.9(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", ie, 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 2.5. We conclude that the system depicted by figure 2.9 is entirely equivalent to that of figure 2.8.

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 MNR 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.

In actual systems, the relays of the ladder shown in figure 2.9 do not have dual terminals. Rather, separate relays are used, depicted as D1 , D2, etc. in figure 2.10.

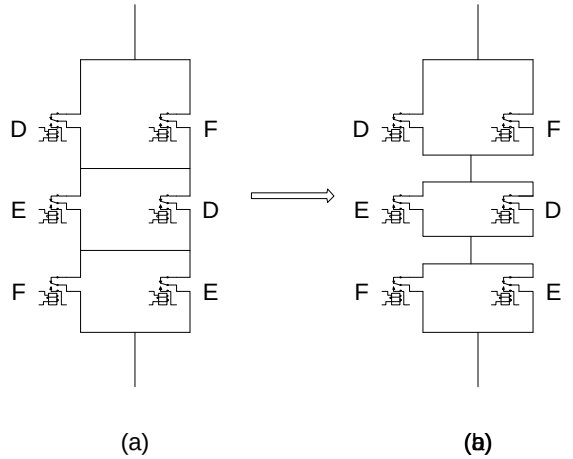

Figure 2.9 '2 out of 3' Ladder Logic

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 2.10. The system unavailability is thus:

$$\bar{A} = (\bar{D1}+\bar{F2}).(\bar{E1}+\bar{D2}).(\bar{F1}+\bar{E2}) = (2p)^3 = 8p^3 \qquad (57)$$

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.

We'll see in Chapter 5 how we can combine the relay fault tree with the SOR fault tree to give the full fault tree for a shutdown system.

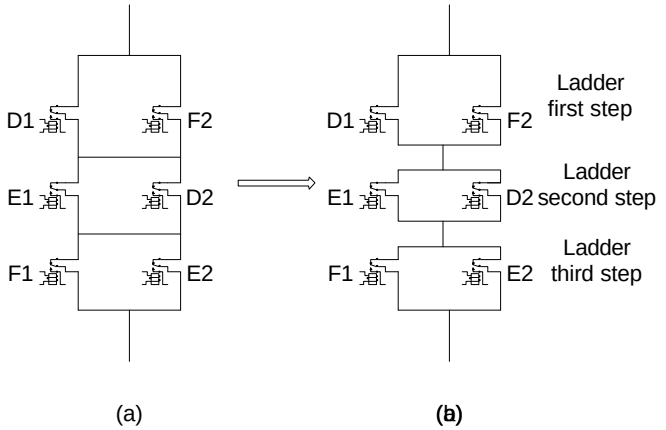

Figure 2.10 '2 out of 3' Ladder Logic - Separate Relays

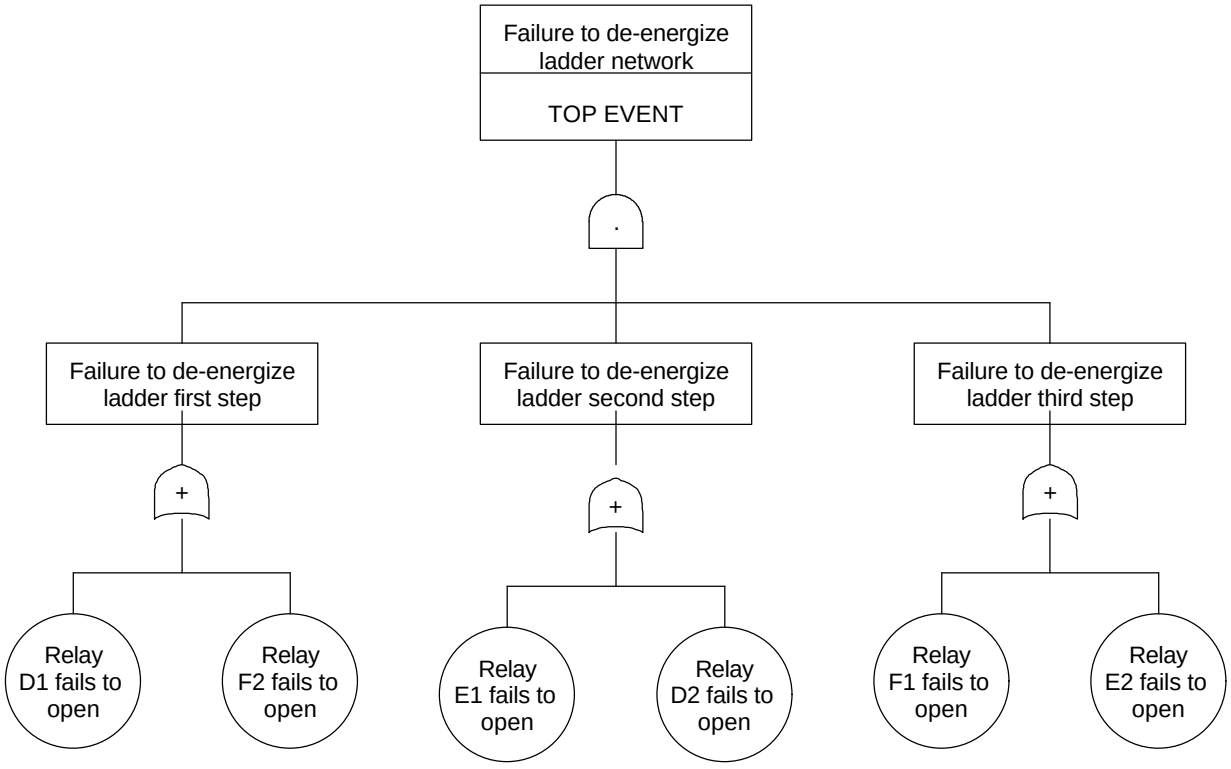

Figure 2.11 Fault Tree for the Ladder Logic Relays

2.14 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 2.7. Safety targets can be defined in terms of some average unavailability 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 a 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.

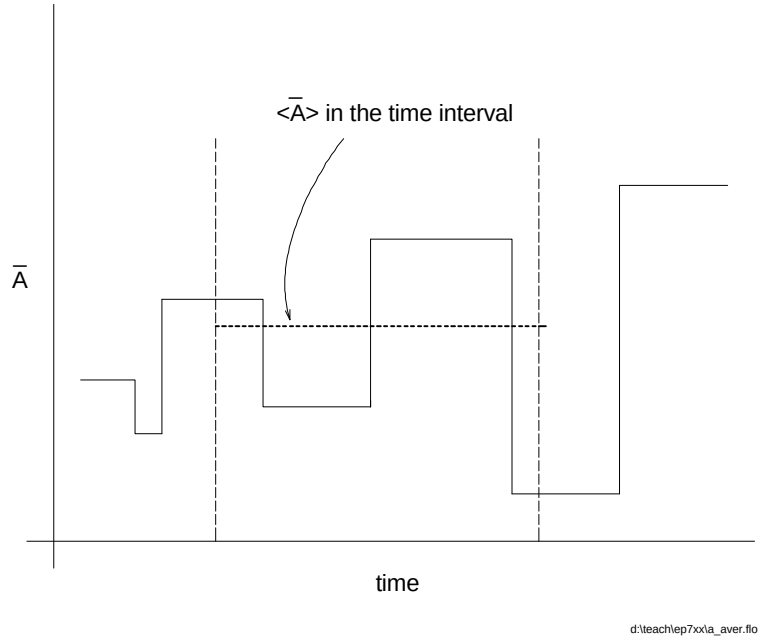

Figure 2.12 Time dependent unavailability

2.15 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 (termed a Loss of Coolant Accident or LOCA) is for the ECC to detect the event and initiate the injection of high pressure (HP) cooling water. Then , after the HTS have depressurized, medium pressure and finally low pressure water is injected. The HP water is supplied via a water supplied that is pressurized by gas cylinders. Medium pressure cooling water is supplied from the dousing water via ECC pumps and low pressure water is retrieved from the sumps. For CANDU reactors a 3 month mission time has been set. 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 and loss of coolant supply. ECC is discussed in more detail in Chapter 7.

. . . . . .

Before we get into the specifics of applications, we develop safety criteria and design basis accidents in the next two chapters.

2.16 Exercises

1. For the example fault tree of Section 2.11, 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. 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. A light bulb has a $\lambda(t) = 5x10^{-7}$ t, where t is the time in days.
   a. What is the MTTF for the bulb?
   b. What is the MTTF if $\lambda(t) = 5x10^{-7}$ t?