Lecture 5 – Probability

Dr. V.G. Snell
Nuclear Reactor Safety Course
McMaster University

Probability – Basic Ideas

$$P(A) \equiv \text{probability of event } A$$

$$= \lim_{n\to\infty} \left(\frac{x}{n}\right) \qquad (1)$$

(Axiom #1) $\quad 0 \le P(A) \le 1 \qquad (1)$

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

Intersection

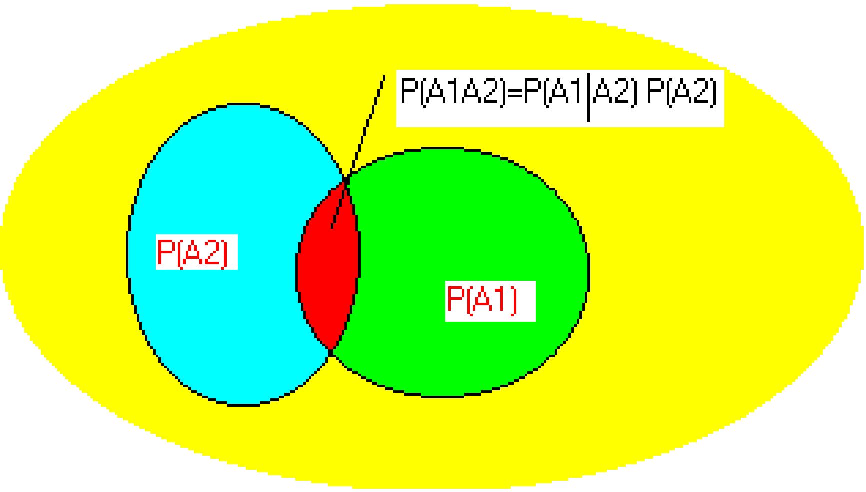
$$A_1 \cap A_2 \quad \text{or} \quad A_1A_2 \quad \text{or} \quad A_1 \text{ AND } A_2 \qquad (1)$$

(This is <u>not</u> A_1 times A_2)

(*Axiom*#3)

$$P(A_1 \; A_2) = P(A_1|A_2)\; P(A_2) \qquad (1)$$
$$= P(A_2|A_1)\; P(A_1)$$

In Pictures

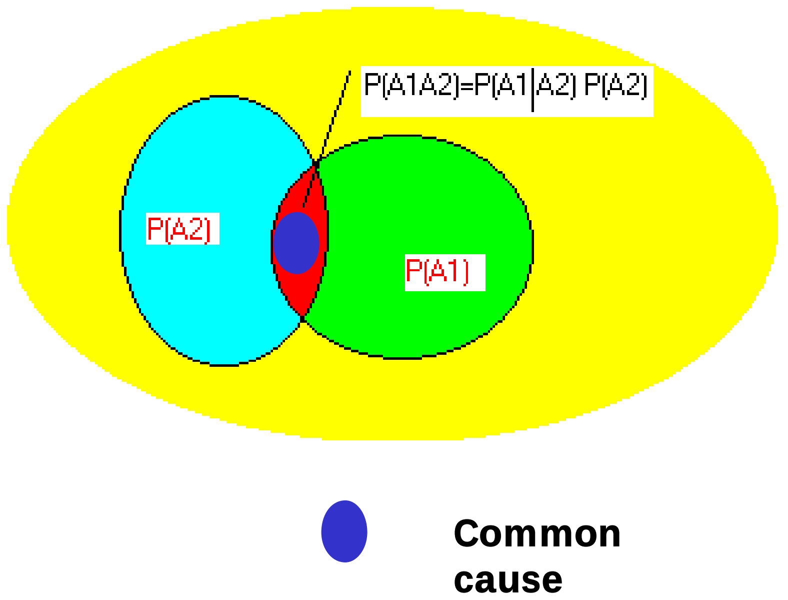


If the events are independent:

P(A2|A1) = P(A2)

Probability of Two Shutoff Rods Failing

- $P(A1) = P(A2) = 0.001$
- If independent, $P(A1A2) = (0.001)^2 = 10^{-6}$
- Suppose there is a common cause failure 10% of the time
- $P(A1) = P(A2) = 0.0009$ (random) + 0.0001 (CC)



Two Shutoff Rods – cont'd

- $P(A1|A2) = 0.9 * 0.001 + 0.1 * 1 = 0.1009$
- $P(A1A2) = 0.1009 * 0.001 = 0.0001009 \sim 10^{-4}$
- A 10% common cause probability has increased the combined failure by a factor of 100!

Generalization

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

If the events are independent:

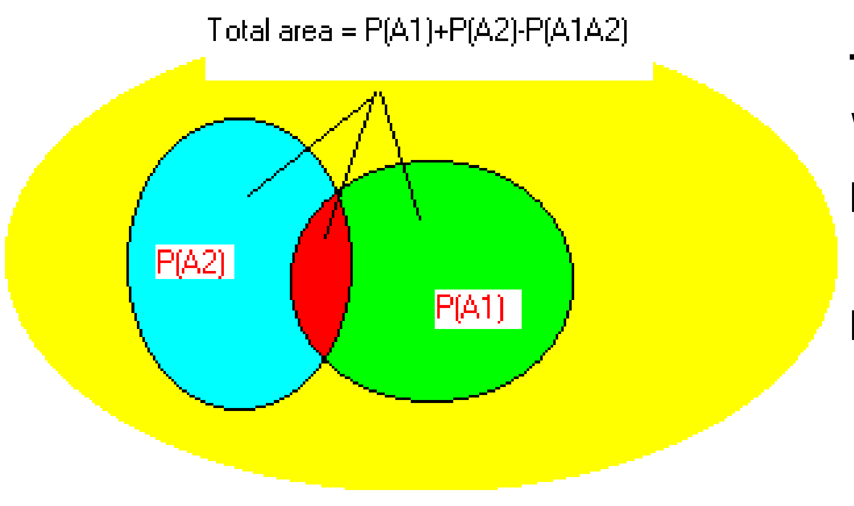
$$P(A_1A_2....A_N) = P(A_1)P(A_2)....P(A_N) \qquad (1)$$

For example: Probability of flipping heads twice in succession = (1/2) * (1/2)

Union

$$A_1 \cup A_2 \quad \text{or} \quad A_1 + A_2 \quad \text{or} \quad A_1 \text{ OR } A_2. \qquad (1)$$

$$P(A_1 + A_2) = P(A_1) + P(A_2) - P(A_1A_2) \qquad (1)$$



Why subtract P(A1A2)?

Think of probability of getting one head when you flip two coins:

P(first head OR second head)

= P(first head) + P(second head) – P(both heads)

= 0.5 + 0.5 – 0.25

= 0.75

Generalizing

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

For independent events

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

Rare Independent Events

$$P(A_1 + A_2 + \ldots A_N) \simeq \sum_{n=1}^{N} P(A_N) \qquad (1)$$

$$\mathrm{P}(\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_N) = \mathrm{P}(\mathrm{A}_1)\mathrm{P}(\mathrm{A}_2)\ldots\mathrm{P}(\mathrm{A}_N) \qquad (1)$$

Bayes Theorem

Start from event *B* and A_n mutually exclusive events or hypotheses, where n = 1,…,N

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

Bayes with Known Statistics

- Radiographing a Class I pipe for a defect
- Known likelihood of a defect is one per 100,000 radiographs
- Known likelihood of instrument giving false positive is 1%
- Known accuracy or likelihood of indicating a defect when there *is* a defect is 99%.
- One test indicates a defect
- What is the probability that the pipe actually has a defect?

Working it out...

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

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

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

Want likelihood of a defect when instrument gives a positive

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

$$= 0.99 \times 0.00001 / 0.01$$

$$= 0.00099$$

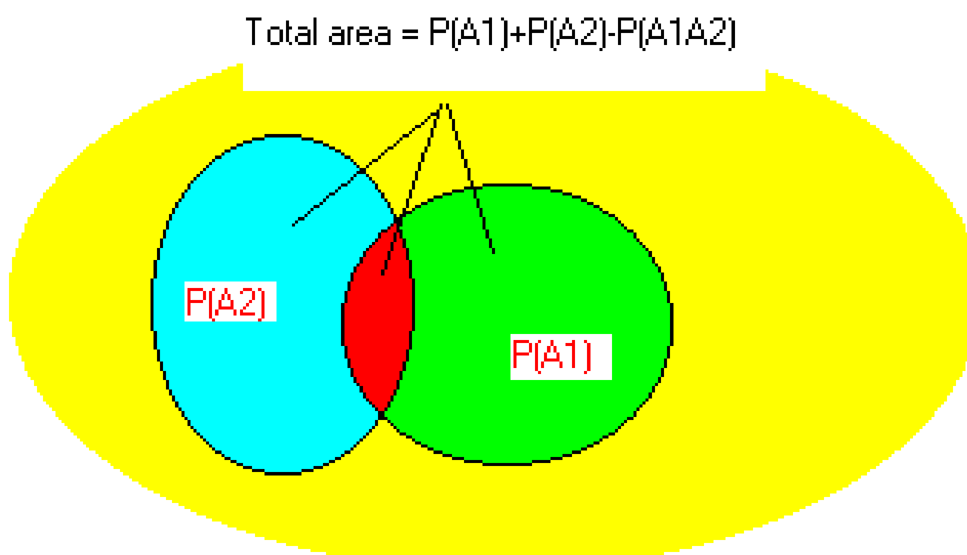
How worried should you be if you get a positive test for a rare disease?

Bayes with Unknown Statistics

- How to determine the frequency of an event which has not occurred
  - Take a number of possibilities for frequency
  - Assign (guess) a likelihood of each possibility being correct
  - Use Bayes theorem to see if your guesses are sensible
- Problem: bad guess = silly result

Probabilities for “OR”ed Events

- Take two dice. What is the probability that die 1 shows a six OR die 2 shows a six?
- Recall
  $P(A_1+A_2) = P(A_1) + P(A_2) - P(A_1A_2)$



Work it out...

- Since

  $P(A_1) = P(A_2) = 1/6$, and $P(A_1A_2) = 1/36$, then

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

Table of Combinations

Die 1	Die 2	Number of Cases showing 'six'
1	1,2,3,4,5,6	1
2	1,2,3,4,5,6	1
3	1,2,3,4,5,6	1
4	1,2,3,4,5,6	1
5	1,2,3,4,5,6	1
6	1,2,3,4,5,6	6
Total Combinations Showing 'six'		11

Another Way

P(at least one six) = 1 - P(no sixes)

Probability of no sixes for each die = [1 - the probability of getting a six]

Probability of getting no sixes for both dies = the product of the probability of getting no six for each die

P(no six for die 1) = 1 - P(six for die 1)

P(no six for die 2) = 1 - P(six for die 2)

P(no six for die 1 AND no six for die 2) =

[1 - P(six for die 1)][1 - P(six for die 2)]

Numbers

P(at least one six)

= 1 - P(no sixes)

= 1 - [1 - P(six for die 1)][1 - P(six for die 2)]

= 1 - [1- 1/6][1 - 1/6] = 1 - 25/36 = 11/36

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

Why bother?

- Examples drive theory and understanding, not the reverse
- Often using P(not A) or $P(\bar{A})$ is more useful
- Which would you use for 1000 dice?

Demand and Continuous

- Examples of **demand** systems
  - Shutdown, stepback
  - ECC initiation
  - Containment box-up
- Examples of **continuous** systems
  - HTS pump motor
  - Air coolers
  - Reactor control system

Mixed Systems – e.g., ECC

- Initiation – demand
- Switch from HPECI to MPECI to LPECI – demand
- Crash cooldown - demand
- MPECI and LPECI Operation – continuous
  - Heat exchangers, pumps
  - Limited mission time

Demand Systems

D_n = 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.

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

$$P(\bar{D}_n \; W_{n-1}) = P(\bar{D}_n | W_{n-1}) \quad P(W_{n-1}) \qquad (2)$$

So

$$\begin{aligned} P(D_1 D_2 D_3 \ldots D_{n-1} \; \bar{D}_n) &= P(\bar{D}_n | W_{n-1}) \; P(W_{n-1}) \\ &= P\;(\bar{D}_n | D_1 D_2 \ldots D_{n-1}) \;.\; P\;(D_{n-1} | D_1 D_2 \ldots D_{n-2}) \ldots P(D_2 | D_1) \; P(D_1) \end{aligned} \qquad (3)$$

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

$$P(D_1 D_2 \ldots D_{n-1} \bar{D}_n) = P(\bar{D}) \; [1 - P(\bar{D})]^{n-1} \qquad (4)$$

Failure Dynamics

$$f(t)dt = \text{probability of failure in the interval } dt \text{ at time } t$$

$$\begin{aligned} F(t) &= \text{accumulated failure probability} \\ &= \int_0^t f(t')dt' \end{aligned} \qquad (1)$$

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

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

Conditional Failure Rate - 1

$$f(t) = -\frac{dR(t)}{dt} = \frac{dF(t)}{dt} \qquad (1)$$

?(t) =failure rate at time t
given successful operation up to time t

$$\begin{aligned} f(t)dt &= ?(t)\ dt\ \ R(t) \\ \text{or}\quad f(t) &= ?(t)\ \ R(t) \\ &= -\frac{dR}{dt} \end{aligned} \qquad (1)$$

Conditional Failure Rate – 2

$$R(t) = \exp\left[-\int_0^t ?(t)dt\right] \qquad (1)$$

If l is constant (random failures)

$$R(t) = e^{-l t}$$

Summary of Terms

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 ?(t), R(t), F(t), and f(t)

Mean Time to Failure

$$MTTF = \frac{\int_0^\infty t f(t)\,dt}{\int_0^\infty f(t)\,dt} = \int_0^\infty t\, l\, e^{-l t}\,dt = \frac{1}{l}$$

(for random failures)

Typical Behaviour of λ

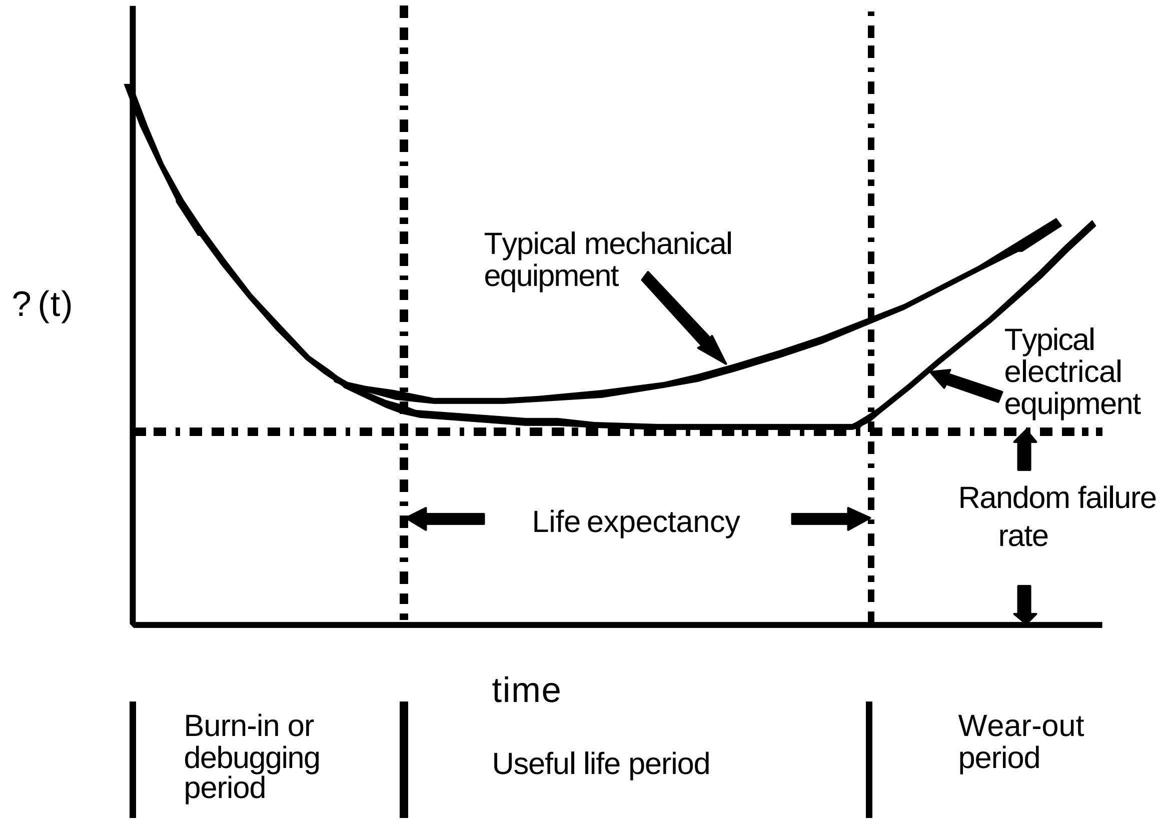


Figure 4-6 - Time dependence of conditional failure (hazard)rate [Source: Ref. 1, page 26]

Availability

Availability = Reliability + effect of repair

$R(t) \leq A(t) \leq 1$

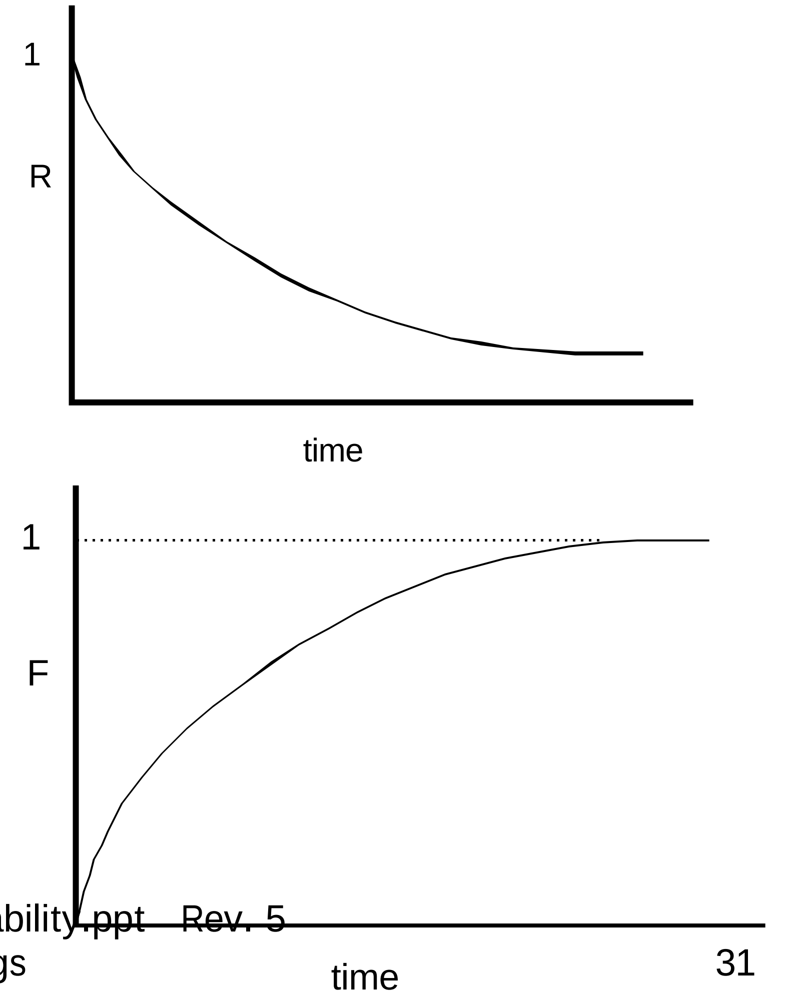
With no repair, $R(t) = A(t)$

Continuous Operation

For random failures

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

$F(t) = 1 - R(t)$



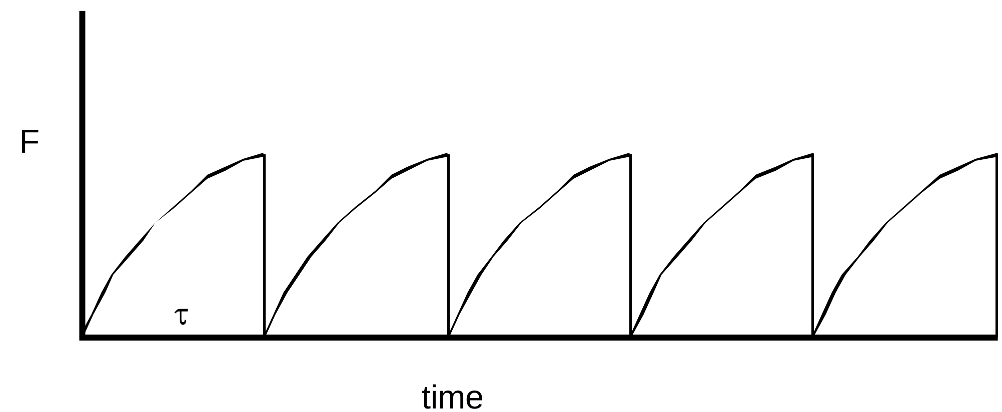
With Repair

In any time interval $0 < t < \tau$

between repairs

$F(t) = \lambda t$

Average is $\langle F \rangle = \lambda\tau/2$



Example – One Shutoff Rod

Suppose λ = 0.02 / year

Want Unavailability $\equiv \bar{A} \equiv$ (1-A) $\equiv$ F $\leq 10^{-3}$ (per demand)

$\bar{A} = \lambda\tau/2$

So $\tau \leq 1$ year

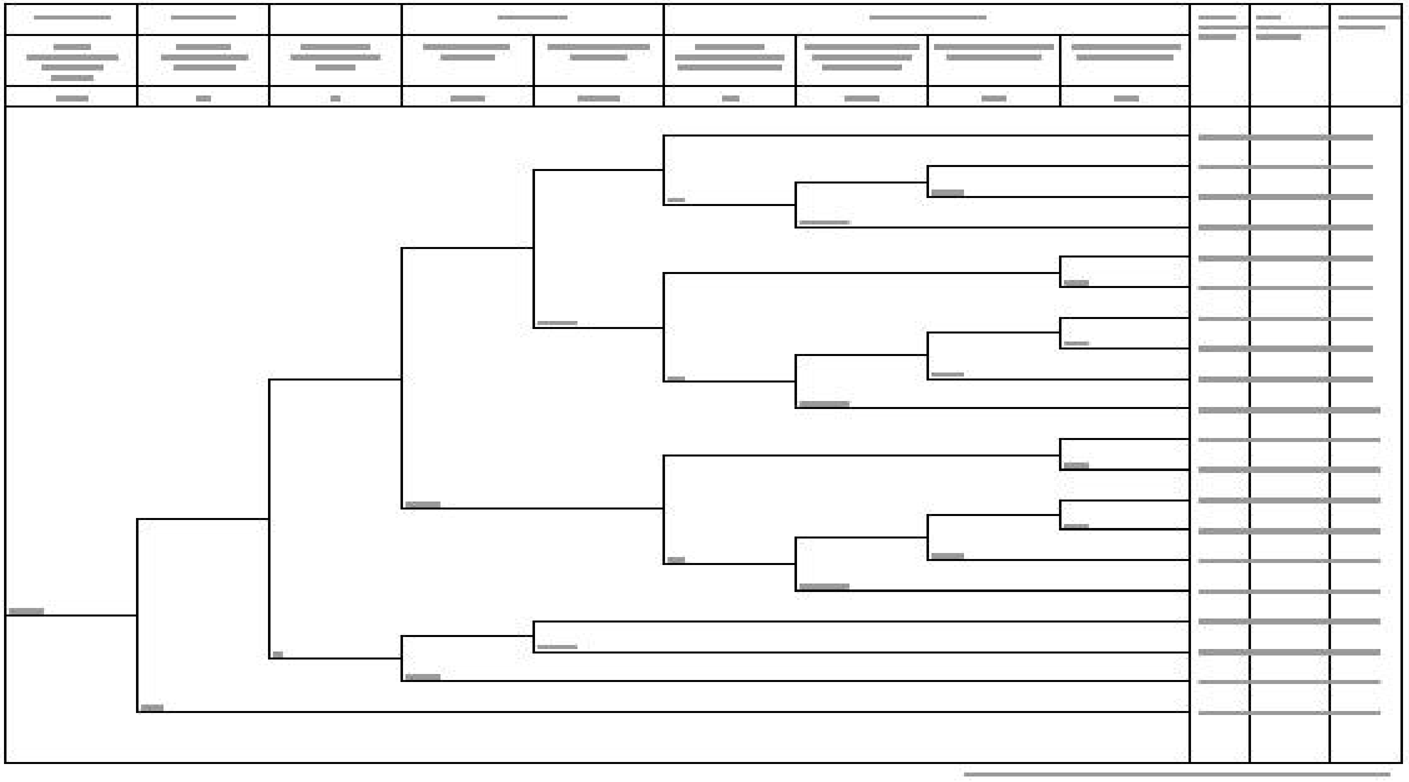
Meeting Reliability Targets

- Increase repair frequency τ until <F> meets the target
- Increase test frequency and fix if it fails on test

Event trees and Fault Trees

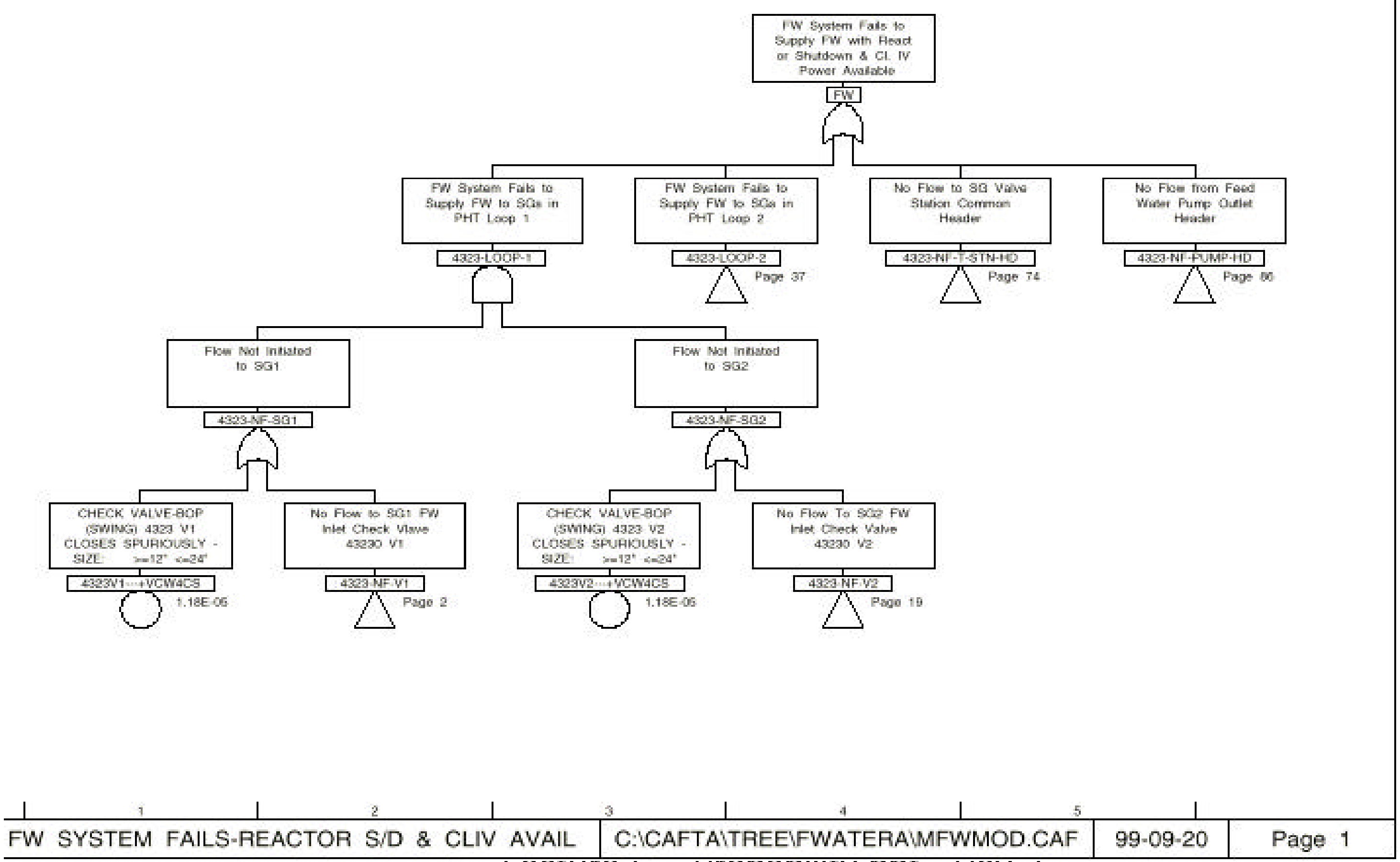
- Simplified treatment
- Fault tree – frequency of an initiating event
  - Focus on how an event can occur
- Event tree – frequency of core damage
  - Focus on mitigating systems, given an event

Event Tree



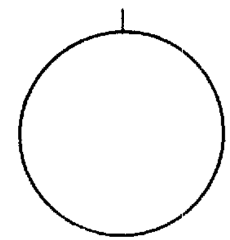
LARGE LOCA EVENT TREE FOR CANDU 6

Fault Tree

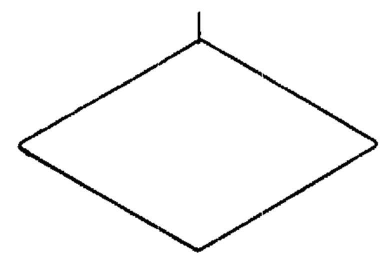

FW System Fails to Supply FW with React or Shutdown & Cl. IV Power Available
FW
FW System Fails to Supply FW to SGs in PHT Loop 1
4323-LOOP-1
FW System Fails to Supply FW to SGs in PHT Loop 2
4323-LOOP-2
Page 37
No Flow to SG Valve Station Common Header
4323-NF-T-STN-HD
Page 74
No Flow from Feed Water Pump Outlet Header
4323-NF-PUMP-HD
Page 86
Flow Not Initiated to SG1
4323-NF-SG1
Flow Not Initiated to SG2
4323-NF-SG2
CHECK VALVE-BOP (SWING) 4323 V1 CLOSES SPURIOUSLY - SIZE: >=12" <=24"
4323V1---+VCW4CS
1.18E-05
No Flow to SG1 FW Inlet Check Vlave 43230 V1
4323-NF-V1
Page 2
CHECK VALVE-BOP (SWING) 4323 V2 CLOSES SPURIOUSLY - SIZE: >=12" <=24"
4323V2---+VCW4CS
1.18E-05
No Flow To SG2 FW Inlet Check Valve 43230 V2
4323-NF-V2
Page 19
1
2
3
4
5
FW SYSTEM FAILS-REACTOR S/D & CLIV AVAIL
C:\CAFTA\TREE\FWATERA\MFWMOD.CAF
99-09-20
Page 1

Fault Tree Symbols - Events

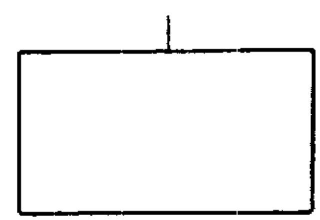
Basic Event



Undeveloped Event

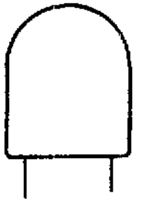


Intermediate or Top Event

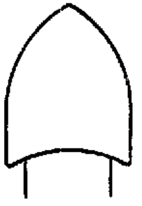


Fault Tree Symbols - Gates

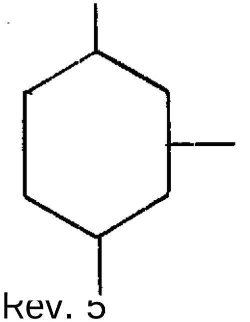
AND Gate



OR gate



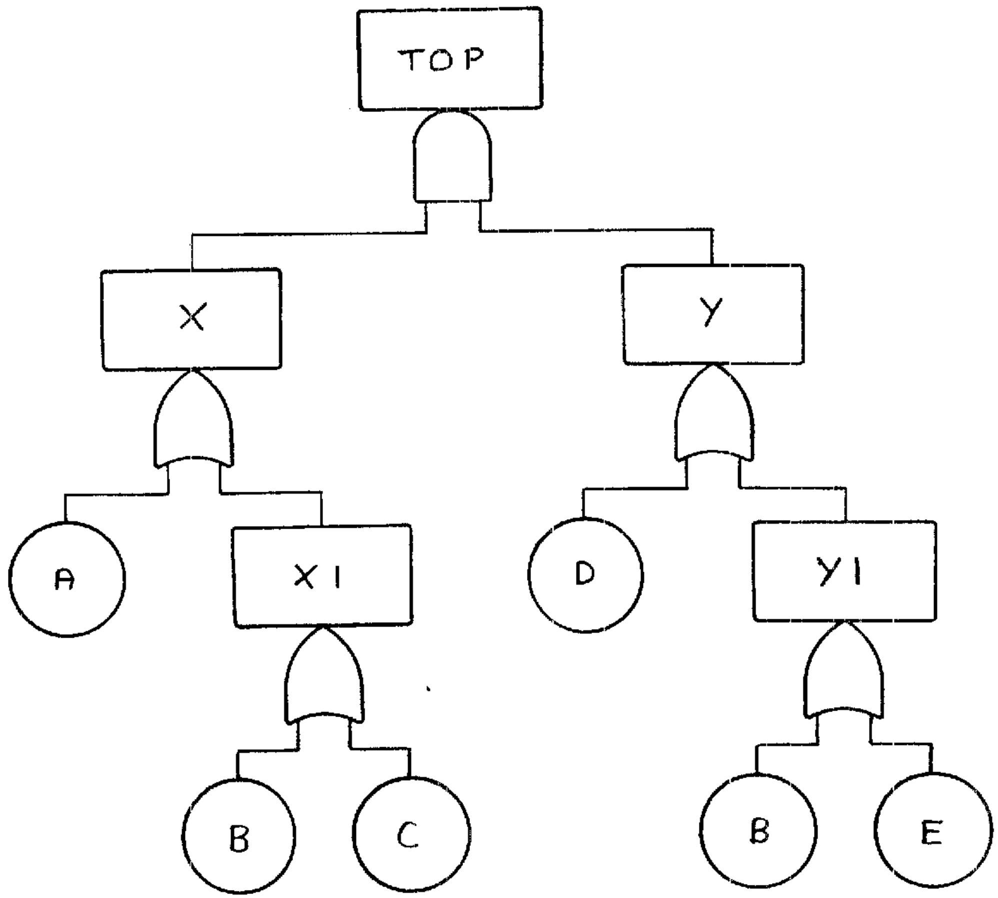
INHIBIT Gate



Steps in Creating a Fault Tree

- Define top event
  - E.g. system failure
- Write down the *immediate* causes of the top event
  - If more than one, decide whether they are joined by AND or OR gates
- For each of these lower events, expand them similarly
- Continue until you can no longer break the event down, or you know the probability of failure

Example Fault Tree



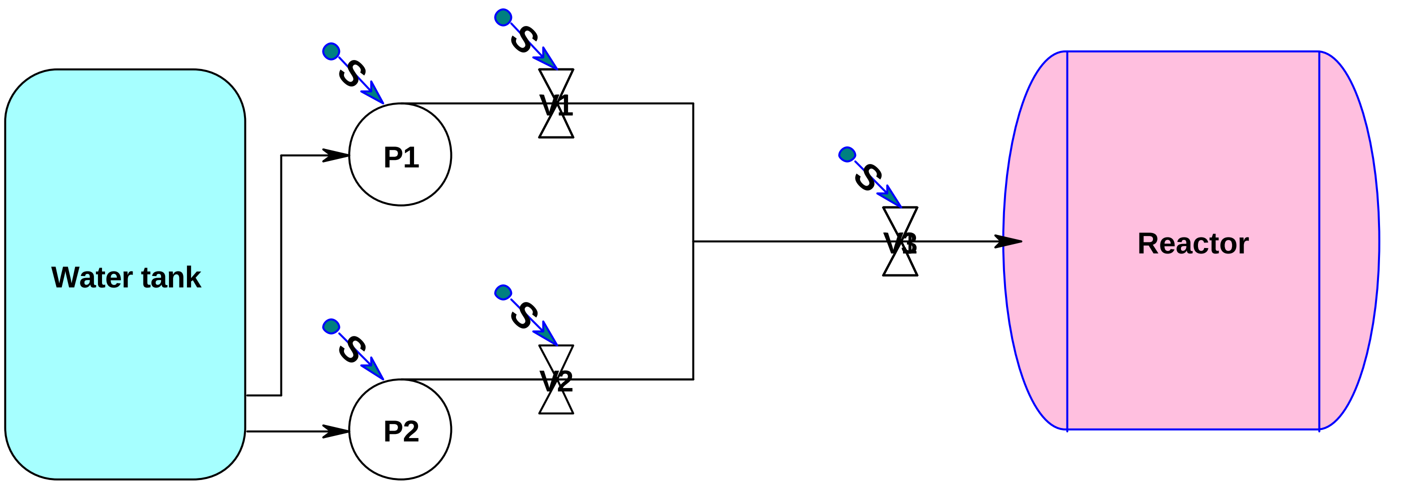
Evaluation

Top	$= X \bullet Y$
X	$= A+X1$
Y	$= D+Y1$
X1	$= B+C$
Y1	$= B+E$

Therefore:

X	$= A+B+C$
Y	$= D+B+E$
TOP	$= (A+B+C) \bullet (D+B+E)$
	$= AD+AB+AE+BD+BB+BE+CD+CB+CE$
	$= \underline{B+AD+CD+AE+CE}$

Develop a Fault Tree for This



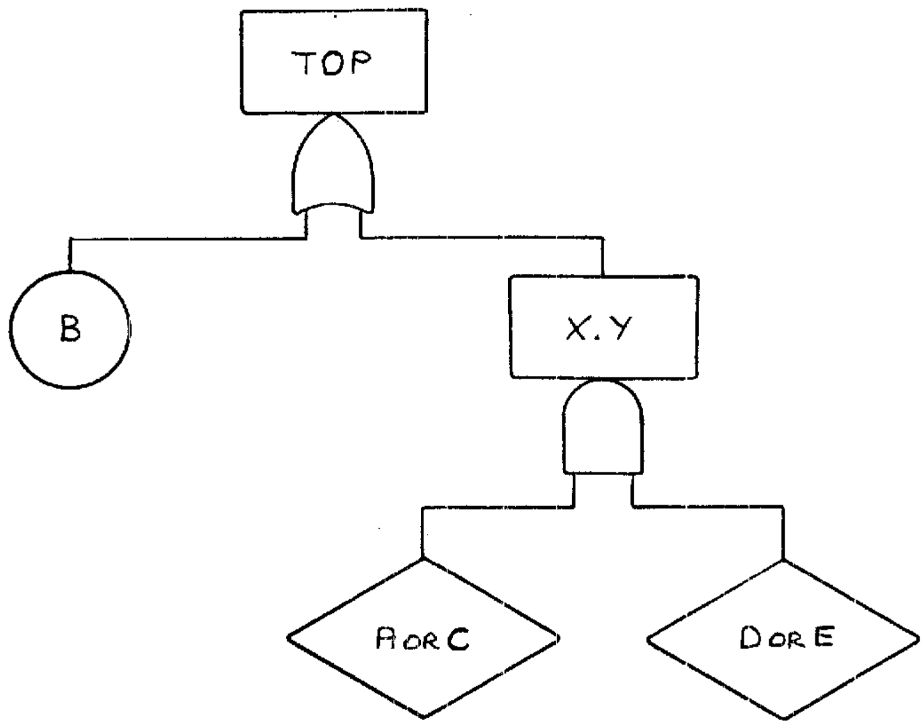
Demand failure probabilities for each component:

Pump (P): 0.01
Valve (V): 0.01
Signal (S): 0.001

Minimal Cut Set

- Cut set = any basic event or combination of basic events that will cause the top event to occur
- Minimal cut set = the smallest combination of events which, if they all occur, will cause the top event to occur

Minimal Cut Set Gives Reduced Fault Tree



Event Tree Exercise

- A LOCA in a CANDU calls on the following safety functions to prevent a release of radioactivity to the environment:
  - Shutdown (either of two shutdown systems)
  - Emergency Core Cooling
  - Containment (box-up and cooling)
- If ECC fails, the moderator can prevent fuel melting
- If the demand unavailability of each of the four safety systems is 10^{-3} and of the moderator is 10^{-2}, draw the event tree and determine:
  - The frequency of severe core damage
  - The frequency of a large release