

Lecture 4 - Probability Tools and Techniques

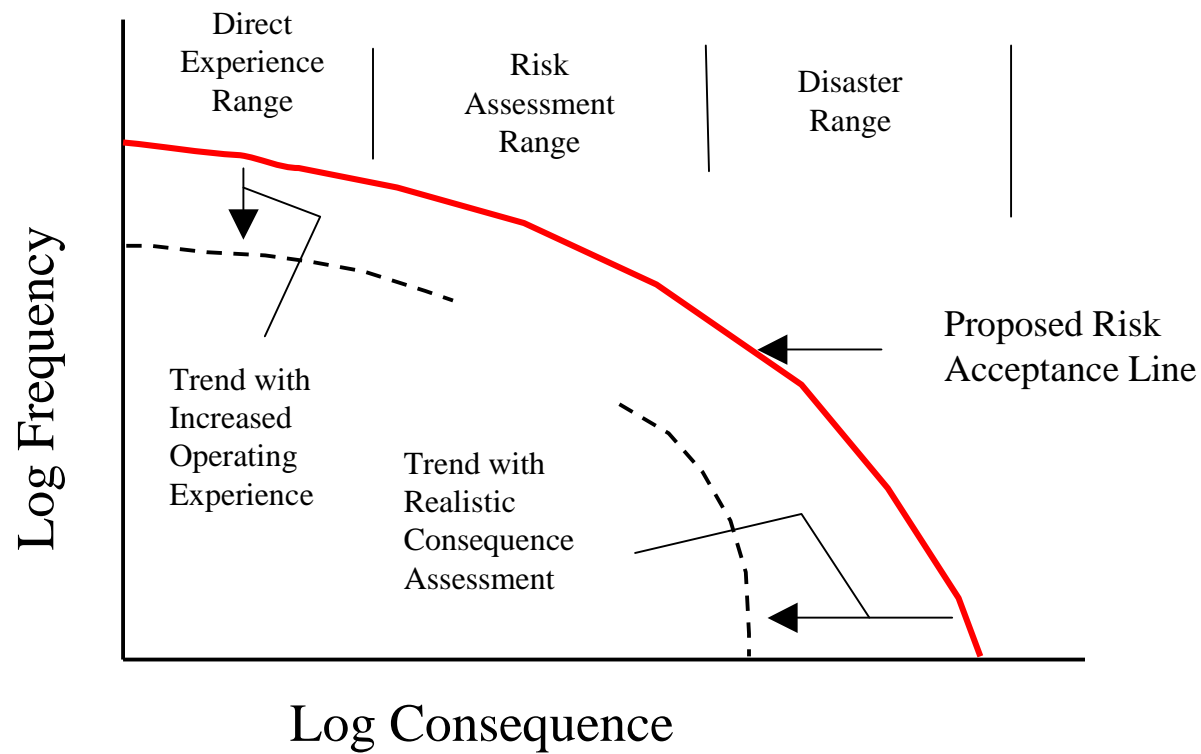
Material from D. Meneley is gratefully acknowledged

Outline

1. General
2. Definitions and Rules
3. Continuous and Standby Systems
4. Bayes Theorem
5. Reliability Equations
6. Probability Distribution Functions
7. Common Cause Failures
8. System Reliabilities
9. Fault Tree Analysis

Typical Technology Risk Profile

Risk \sim frequency x consequence



What is Your Chance of Being Killed by a Meteorite?

- **Fact:** About 4 rocks of ~2 km diameter hit the earth in 10^6 years
- **Fact:** Impact energy of a 2 km chunk is 10^5 Megatons -- it likely would be sufficient if the rock hit within 10^3 km of your chair, or within an area of 3×10^6 km².
- **Fact:** surface area of the earth is $\sim 5 \times 10^8$ km².
- Chance of you being killed $\sim 4 \times .006 \times 10^{-6} = 2 \times 10^{-8}$ /yr.
- So why worry about improbable events? You are going to get it eventually, in any case

Goals of Probabilistic Safety Analysis

- To quantify the radiological risk inherent in a plant design
 - in comparison with a regulator's acceptance line
 - The plant owner's acceptance line
 - The peoples' acceptance line
 - Provide input to severe accident management guidelines and emergency response
- To quantify the risk inherent in a particular failure sequence
 - To assess the need for improvement or relaxation in related equipment and operating procedures
 - To inform management and regulators of components and systems performance against standards

Techniques of PSA

- Analysts usually use a combination of event trees and fault trees.
- Success and failure alternatives are defined for each major system involved in the event.
- Basic theorems of probability are utilized to assess the performance of each component failure, using success/failure modes
- Branch probabilities calculated using direct experience data where it is available, estimates from similar components as required

Definitions and Rules -- 1

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

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

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

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

The intersection of two events is denoted by:

$$A_1 \cap A_2 \quad \underline{\text{or}} \quad A_1 A_2 \quad \underline{\text{or}} \quad A_1 \text{ .AND. } A_2$$

Note: this does not mean A_1 multiplied by A_2 .

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

Note: $P(A_1 | A_2)$ denotes the conditional probability of event A_1 given that event A_2 has occurred.

Definitions and Rules -- 2

The union of two events is denoted:

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

Note: this does not mean A_1 plus A_2 .

So, the probability of A1 or A2 failing is given by:

$$P(A_1 + A_2) = P(A_1) + P(A_2) - P(A_1A_2)$$

Note: third term usually is neglected (small)

Decomposition of an Event:

$$P(A_1) = P(A_1 | A_2)P(A_2) + P(A_1 | \bar{A}_2)P(\bar{A}_2)$$

This follows from combining the union rule with the product rule.

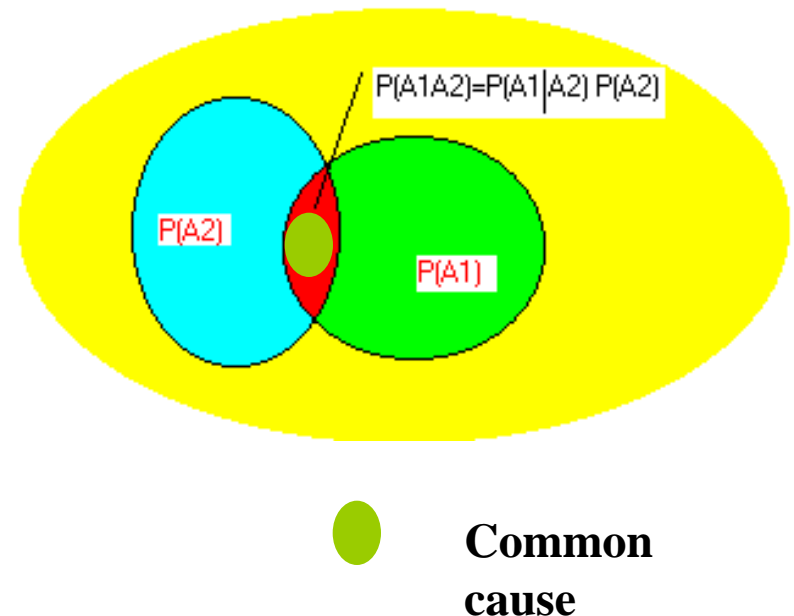
Intersection Example

Probability of Two Shutoff Rods Failing

$$P(A1) = P(A2) = 0.001$$

If rods are independent, $P(A1A2) = (0.001)^2 = 10^{-6}$

Suppose there is a common cause failure 10% of the time, then
 $P(A1) = P(A2) = 0.0009$ (random)
+ 0.0001 (common cause)



Two Shutoff Rods – with Common Cause Failure

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

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

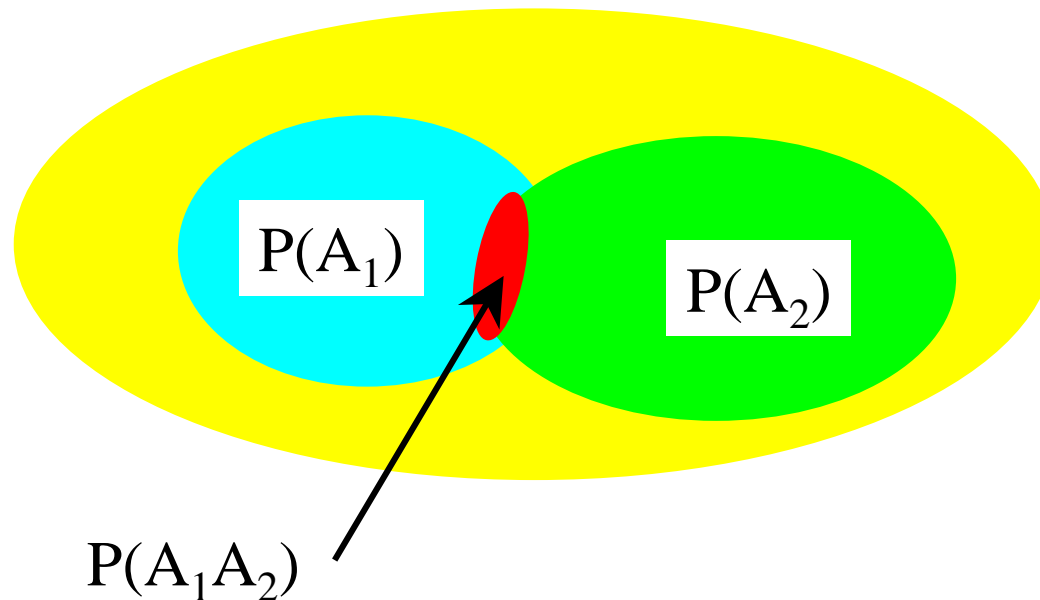
A 10% common cause probability has increased the combined failure by a factor of 100!

Union Example

Probability of Getting Heart or a Four from a Card Deck

Think of the probability of choosing a heart or a four from a card deck:

$$\begin{aligned} & \mathbf{P(\text{heart .OR. four})} \\ &= \mathbf{P(\text{heart}) + P(\text{four}) - P(\text{heart and four})} \\ &= \mathbf{13/52 + 4/52 - 1/52 = 4/13} \end{aligned}$$



Throwing Dice

Take two dice. What is the probability that die 1 shows a six OR die 2 shows a six?

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

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

The next slide shows the identical result obtained by setting up a simple Table of Combinations.

Table of Combinations - Two Dice

Die 1	Die 2	Number of Cases Showing '6'
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 '6'		11

Another Way

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

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

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

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

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

Numbers - Independent Events

$P(\text{at least one six})$

$= 1 - P(\text{no sixes})$

$= 1 - [1 - P(\text{six for die 1})][1 - P(\text{six for die 2})]$

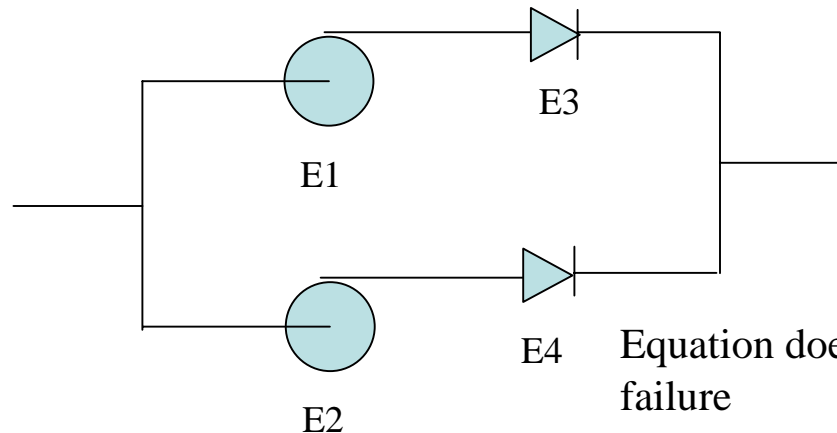
$= 1 - [1 - 1/6][1 - 1/6] = 1 - 25/36 = 11/36$

Standby Example

Probability of Two Pump System Startup

One auxiliary feedwater pump can provide 100% of the required flow. At time of demand both standby pump (E1, E2) are sent a start signal. Each pump has a start failure probability P_1 ; each check valve (E3, E4) has a probability of failure to open P_2 , what is the probability of system failure? Work it out:

$$P_{SYS}(\text{failure}) = [P_{E1} \cdot \text{OR} \cdot P_{E3}] \cdot \text{AND} \cdot [P_{E2} \cdot \text{OR} \cdot P_{E4}]$$
$$= (P_{E1} + P_{E3}) * (P_{E2} + P_{E4})$$



Generalization of Rule for Intersection of N Events

$$P(A_1 A_2 A_3 \dots A_N) = P(A_1)P(A_2 | A_1) \dots P(A_N | A_1 A_2 \dots A_{N-1})$$

If the events are independent:

$$P(A_1 A_2 A_3 \dots A_N) = P(A_1)P(A_2) \dots P(A_N)$$

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

Generalization of Rule for Union of N Events

$$P(A_1 + A_2 + A_3 + \dots + A_N) \leq \sum_{n=1}^N P(A_n) - \sum_{n=1}^{N-1} \sum_{m=n+1}^N P(A_n A_m) \\ + \dots + (-1)^{N-1} P(A_1 A_2 \dots A_N)$$

If the events are independent, then

$$1 - P(A_1 + A_2 + A_3 + \dots + A_N) = \prod_{n=1}^N [1 - P(A_n)]$$

Upper and lower bounds can be derived as follows:

$$1 - P(A_1 + A_2 + A_3 + \dots + A_N) = \sum_{n=1}^N P(A_n)$$

$$\text{and } P(A_1 + A_2 + A_3 + \dots + A_N) \geq \sum_{n=1}^N P(A_n) - \sum_{n=1}^{N-1} \sum_{m=n+1}^N P(A_n A_m)$$

Generalization for Rare Independent Events

$$P(A_1 + A_2 + A_3 + \dots + A_N) \approx \sum_{n=1}^N P(A_n)$$

and $P(A_1 A_2 A_3 \dots A_N) = P(A_1)P(A_2) \dots P(A_N)$

Used in reliability calculations

Why bother?

Examples drive theory and understanding, not the reverse.

Often using $P(\text{.NOT. } A) = P(\bar{A})$ is more useful.

Which would you use for for 24 shutoff rods? -- for 1000 dice?

The requirement for precision is quite low in most probability calculations, so that it often is possible to use simpler approximations or bounding values

Continuous and Standby Systems

Examples of systems that operate continuously

HTS pump motor

Containment air coolers

Reactor control system

Examples of systems that operate in standby mode

Shutdown, stepback

ECC initiation

Containment box-up

Auxiliary feedwater system

Backup HT feed pump

Emergency diesel-generators

Note: standby systems are on demand and may have a short or long mission time

Mixed Systems - e.g. ECC

Initiation – demand

Switch from High Pressure ECC to Medium Pressure ECC to
Low Pressure ECC – demand

Shutdown - demand

MPECC and LPECC Operation – continuous

Heat exchangers, pumps

Mission time

The Bayes Equation - 1

Using *Axiom 3*; $P(A_n B) = P(B)P(A_n | B) = P(A_n)P(B | A_n)$

Here, A_n denotes the n th of N mutually exclusive hypotheses or events, while B is some other hypothesis or event.

Using *Axiom # 2*, $\sum_{n=1}^N P(A_n | B) = 1$

Multiplying by $P(B)$ and using *Axiom # 1*, we get $P(B) = \sum_{n=1}^N P(A_n B)$

Substituting from the first equation above, $P(B) = \sum_{n=1}^N P(B | A_n)P(A_n)$

The last equation is the *extension rule* of probabilities.

The Bayes Equation - 2

Substituting once again gives the final form of the Bayes equation:

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

If we know that B is true, and if we know the full set of probabilities $P(B | A_n)$ then we can calculate the conditional probability of A_n given the added knowledge B.

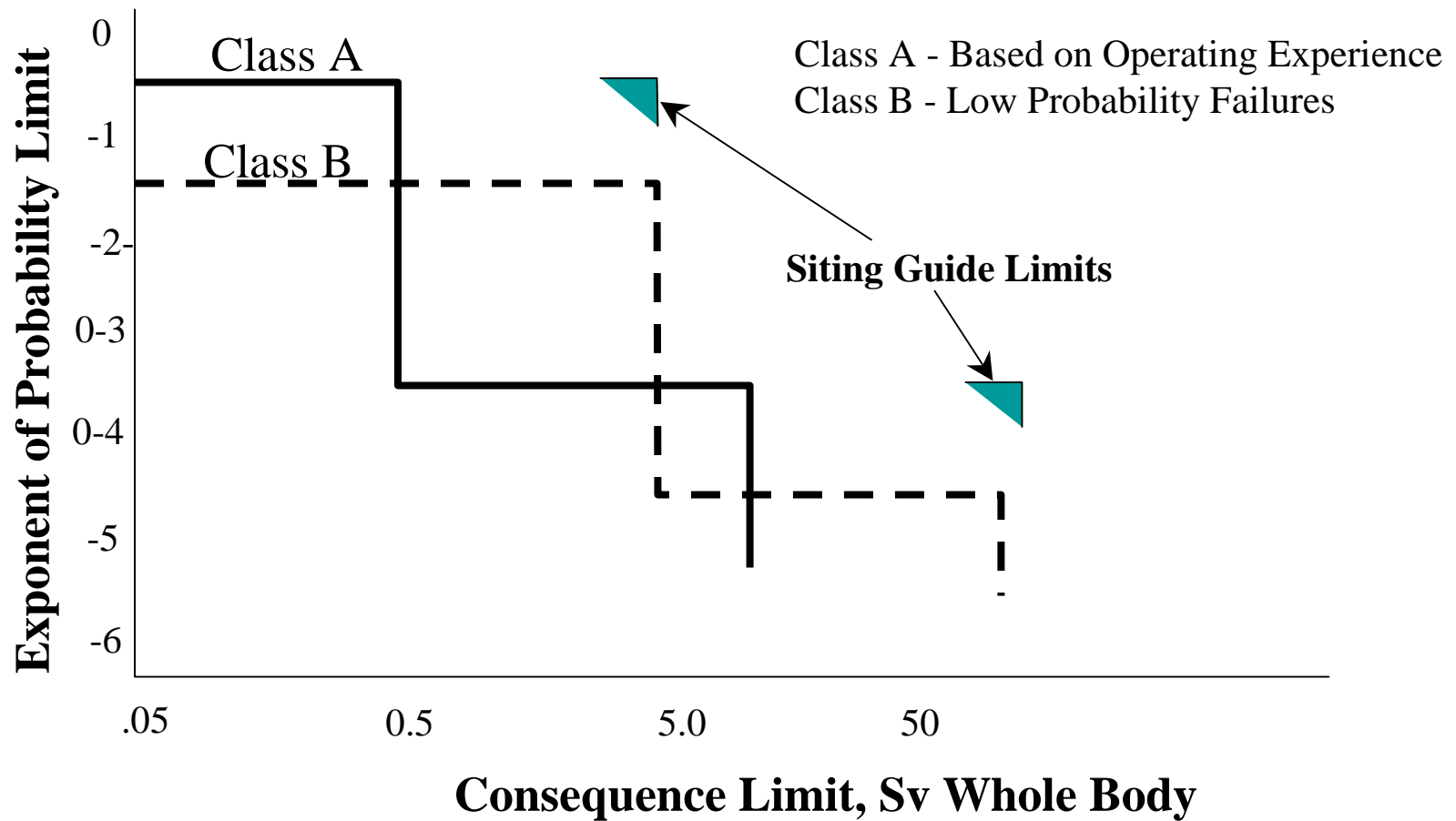
Serious Process Failure with Offsite Consequences

CANDU Power Plants

Postulate Number	1	2	3	4	5
Postulated frequency	3E-1	3E-2	3E-3	3E-4	3E-5
Probability of zero events in 400 operating years. Probability=(1-frequency) ⁴⁰⁰	0	5E-6	0.30	0.89	.99
UNIFORM PRIOR DISTRIBUTION					
Probability of postulate	0.2	0.2	0.2	0.2	0.2
Probability of postulate given zero events	0	2E-6	0.14	0.41	0.45
ESTIMATED PRIOR DISTRIBUTION					
Probability of postulate	0	0.1	0.5	0.3	0.1
Probability of postulate given zero events	0	1E-6	0.29	0.52	0.19

Conclusion: Operating history shows that CANDU is much safer than is required by the Siting Guide rules.

Possible Change in Licensing Limits



Demand Systems

- The probability of a system (e.g. a switch) failing [.NOT.D] on demand 'n' when it has worked [W] for 'n-1' times is denoted:

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

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

- Using *Axiom #3* and assuming all demand events are identical and independent (i.e. failure is not caused by 'wear-out'), then

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

- And so

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

- Probability of a repairable system failing sometime in n demands is n times larger.

Example of Demand System -- Light Switch

- The switch fails randomly with demand probability of 10^{-4} . It is used, on average, 20 times per week. The probability of its failure on the 3120th demand (after 3 years) is

$$10^{-4}(1-10^{-4})^{3119} = 0.732 \times 10^{-4}$$

- The probability that the switch will fail once (and be repaired immediately), sometime during three years, is 3120 times larger, or 0.228.
- We will have more to say about all of this as time goes on.

Systems Continuously Operating without Repair

- The analogy to a demand system, for a system in continuous operation, is:

$$f(t)dt = \lambda(t)dt[1 - F(t)]$$

where $f(t)dt \equiv$ the probability of failure in dt about t ,

$\lambda(t) =$ the conditional failure (hazard) rate,

$\lambda(t)dt \equiv$ the prob. of failure in dt given survival to time t ,

$[1 - F(t)] \equiv$ the probability of system survival up to time t .

- $f(t)$ is the failure probability density in the interval dt about t .
- Assuming eventual failure of the device, its reliability $R(t)$ is defined as $R(t) = 1 - F(t)$

Continuous Operation -- 2

$$R(t) = \int_0^\infty f(t') dt' - \int_0^t f(t') dt' = \int_t^\infty f(t') dt'$$

$$\text{and so } f(t) = -\frac{dR(t)}{dt} = \frac{dF(t)}{dt}$$

Recalling the definition of the conditional failure rate,

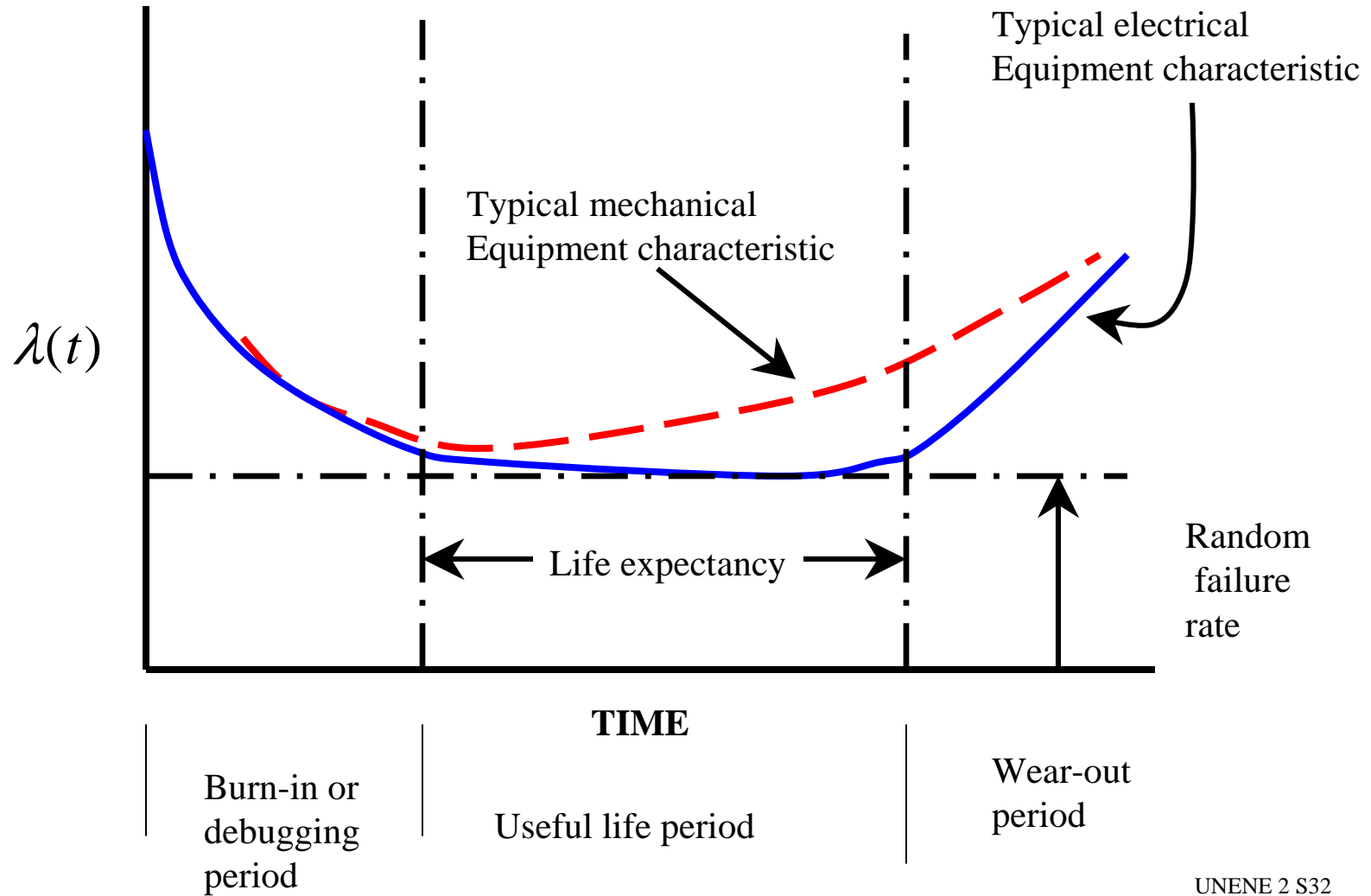
$$\text{and because } R(0) = 1, \quad \underline{R(t) = \exp\left[-\int_0^t \lambda(t') dt'\right]}$$

$$\text{and also } \underline{f(t) = \lambda(t) \exp\left[-\int_0^t \lambda(t') dt\right]}$$

Summary of Relevant Equations

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	$R(t)$	$\int_t^\infty f(\tau)d\tau$	$1 - F(t)$	$\exp[-\int_0^t f(\tau)d\tau]$
Cumulative failure probability	$F(t)$	$\int_0^t f(\tau)d\tau$	$1 - R(t)$	$1 - \exp[-\int_0^t f(\tau)d\tau]$
Failure probability density	$f(t)$	$dF(t)/dt$	$-dR(t)/dt$	$\lambda R(t)$

Mean Time to Failure



Availability

Availability = Reliability + effect of repair

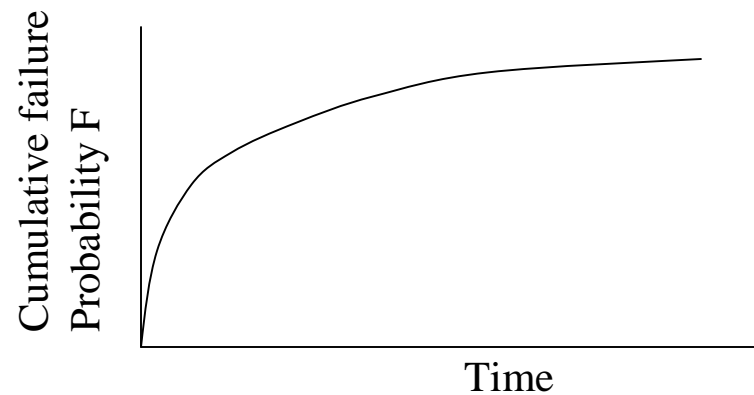
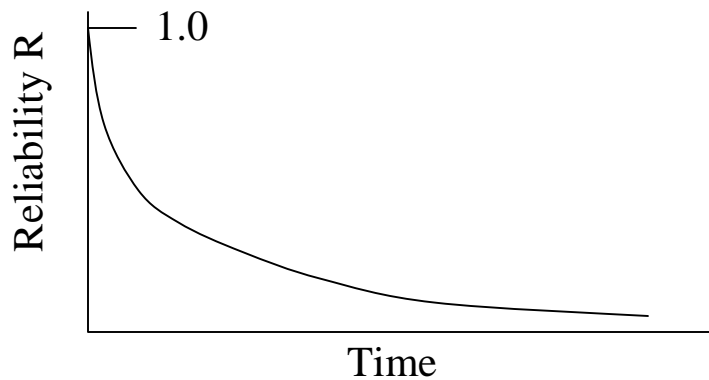
$$R(t) \leq A(t) \leq 1$$

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

Continuous operation no repair:

Assuming λ constant (random failures):

$$\langle F \rangle = \lambda t \text{ simplification of } 1 - \exp(-\lambda t)$$

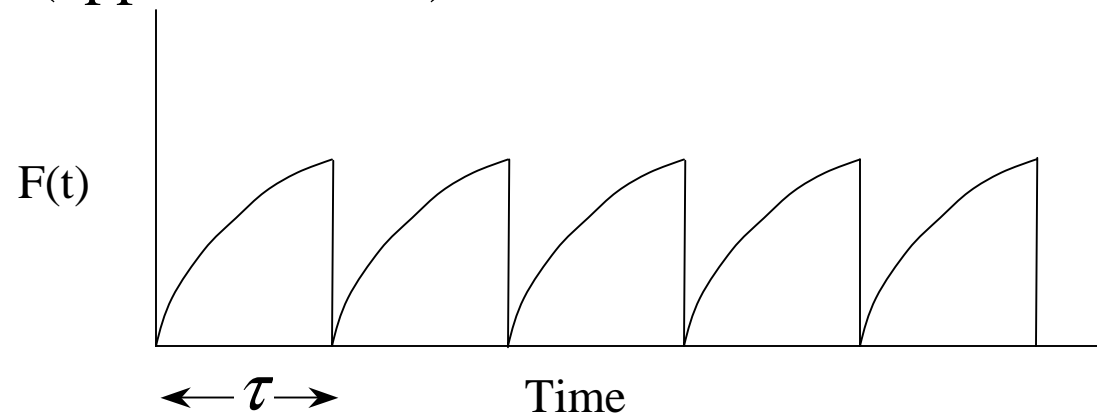


Standby Component With Testing

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

$$\text{Average } \langle F \rangle = 1 + (1/\lambda\tau)(\exp(-\lambda\tau) - 1)$$

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



If mean time to repair $\ll \tau$

Example – One Shutoff Rod

Suppose $\lambda = 0.002$ / year

Want Unavailability \equiv $\equiv (1-A) \equiv F \leq 10^{-3}$ (per demand)
 $= \lambda\tau/2$

So $\tau \leq 1$ year

What other choices do you have?

Meeting Reliability Targets

- Increase repair frequency τ until $\langle F \rangle$ meets the target, or
- Increase test frequency and fix if it fails on test

- What are two good reasons that you may not want to take either of these steps?

- What else can you do?

Probability Distribution Functions

- Discrete
 - Binomial distribution
 - Poisson distribution
- Continuous – Erlangian, Weibull, Exponential, Gamma, and so on.
- Many other options are appropriate to particular situations

Binomial Distribution

- Consider Bernoulli trials wherein $P(\bar{D})$ is constant for each trial. The possible outcomes of a set of trials 'n' correspond to the different terms in the binomial expansion of:
- Introduce a discrete random variable 'r' defined as the number of demands for which the system fails. Now, $[P(D) + P(\bar{D})]^n = 1$

$$P(r) = \binom{n}{r} [P(\bar{D})]^r [P(D)]^{n-r} = \frac{n!}{r!(n-r)!} [P(\bar{D})]^r [P(D)]^{n-r}$$

- For this distribution, mean $m = nP(\bar{D})$
standard deviation $\sigma^2 = nP(\bar{D})P(D)$
- This equation is used for a component that operates on demand and can be fully repaired immediately after failure. Then r is the number of failures in n demands and P(r) is the probability that the component will fail on r demands.

Example -- Light Switch

- Demand failure rate 10^{-4} per demand
- Probability that switch will fail exactly twice in 1000 operations -- plug the numbers into the binomial equation; the result is 0.0045.
- Probability that the switch fails twice or more in 1000 operations can be found from the equation:

$$P(> x) = 1 - \sum_{r=0}^x P(r)$$

- The answer in this example is 0.0047.

Poisson Distribution

- This is similar to the binomial distribution, but it describes systems that undergo transition *randomly and irreversibly* from one state with n occurrences of an event to another with $(n+1)$ occurrences. The distribution is obtained from a power series expansion to obtain:

$$P(r) = \frac{e^{-\mu} \mu^r}{r!}$$

- Where μ is the most probable number of occurrences of the event.
- The Poisson distribution is most useful for analyzing a system with many identical components that, upon failure, cause irreversible transitions in the system.

Example -- Fuel Assembly Failure

- A reactor has 200 fuel assemblies each of which can fail if the fuel cladding fails. If each assembly fails independently and randomly, calculate the probability of 3 assemblies failing if, on the average, 1% of the assemblies are known to fail.
- Plug in the numbers -- the answer is 0.18

Erlangian and Exponential Distributions

- The Erlangian distribution is the time-dependent form of the Poisson distribution, and the Exponential distribution is simply a special case of the Erlangian form.
- It arises in cases of random failures where the hazard rate λ is constant. It is valid for an integer number of failures.
- Then, the probability of r failures is $P(r, t) = \frac{e^{-\lambda t} (\lambda t)^r}{r!}$

$$f(t) = \lambda P(r-1, t) = \frac{\lambda (\lambda t)^{r-1} e^{-\lambda t}}{(r-1)!}, \quad \lambda > 0, \quad r \geq 1$$

- When $r=1$, the exponential distribution is obtained, so

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

The Gamma Distribution

- This is the general case including both Erlangian and exponential functions. The probability density obeys the equation

$$f(t) = \frac{\lambda(\lambda t)^{r-1} e^{-\lambda t}}{\Gamma(r)}, \quad \lambda > 0, \quad r > 0$$

- This distribution is appropriate for systems subject to an environment of repetitive random shocks generated in a Poisson distribution, so the failure probability depends on the **age** of the device.

More and More Distributions

- This discussion could go on for a very long time.
- You can grasp the idea - the analyst uses experimental data as a guide to the appropriate failure probability distribution.

Data Sources and Data Analysis

- A complex topic -- well beyond the scope of this course.
- Good information on historical failures of components and systems provides the only legitimate basis for probabilistic analyses.
- High precision within a narrow range of system states is occasionally necessary, but most often a full range of experience, at somewhat lower accuracy, is preferred.
- Engineers who hope to contribute usefully to the field of failure data collection and analysis must live with the equipment, not in the office.
- Two special items will be addressed: human error and common-cause/common mode failures.

Human Error

- When human error is discussed the subject quickly turns to ‘operator error’. But in general all errors are ‘Human’ in some sense.

MACHINES ARE TOO STUPID TO MAKE MISTAKES

- Accident investigations often reach the conclusion that the whole structure of the institutions involved in an accident were guilty to some degree, or contributed in ignorance to the eventual failure - - for example, the two major space shuttle accidents.
- Professional engineers have been given a special responsibility in this are, as stated in the PEO Charter.

An Example of Human Error

- Air Canada DC-9 rolls for takeoff at Pearson airport
- Speed reaches “point of no return” and pilot starts rotation.
- Chunks of rubber spin from main tires and clog one engine
- Pilot is 1.5-2.5 seconds late in starting emergency reverse procedure
- Pilot aims to the left to avoid airport beacon towers
- Plane rolls off runway and glides into gully at end of runway.
- Conclusion of investigation: **Pilot error.**
- Fact: Retread tires were beyond their service life, and other known problems contributed.

Examples Common Cause and Common Mode Failures

- **Common cause:** external events - fire, earthquake, explosion, etc.
- **Common mode:** common cause acting on a set of identical components. McCormick gives the following list.
 - Design defects
 - Fabrication, manufacturing, and quality control variations
 - Test, maintenance and repair errors
 - Human errors
 - Environmental variations (contamination, high temperature, etc.)
- How do we distinguish ‘human error’ as separate from the other common modes? Do we need to say more about proper assignment of blame? Possible additions to McCormick’s list:
 - Extreme performance pressure combined with resource shortages
 - Management neglect of safety warnings and recommendations
 - aging

Treatment of Common Cause Failures

- For a series of intersecting events, the *single-failure* upper bound can be used, i.e.:

$$P(A_1 A_2 \dots A_N) \leq \min[A_1, A_2 \dots A_N]$$

- Similarly, a *double failure bound* is given by:

$$P(A_1 A_2 \dots A_N) \leq \min[\text{prob's of all double combinations}]$$

- Double bounds may be determined by considering all common causes c_m plus an additional ‘design environment’ term c_0 :

$$P(A_1 A_2) = P(A_1)P(A_2) + \sum_{m=1}^M P(A_1 A_2 | c_m)P(c_m)$$

- The design environment is always present, so $c_0 \sim 1$

Reliability of Simple Systems

- Next we will look at calculation of reliability of a few simple systems, as preparation for looking at some real example cases.
- Analyze systems comprised of a set of components
- Mainly use the exponential distribution function, which is appropriate for analysing random failures.

Reliability of Simple Systems

- Use reliability block diagrams (with “system operation” indicated by successful transmission of a signal from input to output of a system).
- Examine various methods for determining the overall system’s reliability - decomposition method, signal flow graphs, and cut- sets
- Finally, we will do a quick study of M-out-of-N systems used to obtain very high reliability, such as in CANDU shutdown systems.

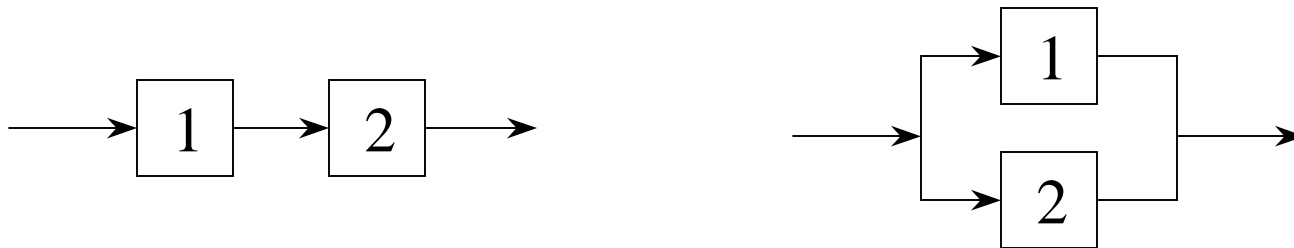
Series and Active-Parallel Units

- First, consider independent units.
- For two units in series, *Axiom #3* (product rule) applies:

$$R_{sys}(t) = R_1(t)R_2(t)$$

- For two units in parallel, the rule of union applies:

$$R_{sys}(t) = R_1(t) + R_2(t) - R_1(t)R_2(t)$$



Series & Active Parallel - Continued

- For N independent units in series,

$$R_{sys}(t) = \prod_{n=1}^N R_n(t) = \exp\left[-\sum_{n=1}^N \int_0^t \lambda_n(\tau) d\tau\right]$$

- For N independent units in active-parallel,

$$1 - R_{sys}(t) = \prod_{n=1}^N [1 - R_n(t)]$$

- Example: calculate reliability for a system of 2n units, in two parallel chains of n units each.

Answer:
$$R_{sys}(t) = [R(t)]^n + [R(t)]^n - [R(t)]^{2n}$$

M-out-of-N Systems in Active-Parallel Operation

- Out of N parallel units, only M are needed to make the system function. It is assumed here that repair or testing of any of the $N-M$ units can be completed without affecting system operation. Nonetheless, we will see that repair and testing can and do have an effect on system reliability.
- Three system states can be identified:
 - State 0 M units in operation, $(N-M)$ are in standby, and no units are under repair.
 - State n M units in operation, $(N-M-n)$ in standby, and n units are under repair
 - State $N-M+1$ The system is failed and is under repair.
- Here, we will consider only the first two states.

M-out-of-N -- 2

- Using the binomial theorem, because each of the N identical units is in one of two possible conditions - it is either operable or it is not. Then, as we have seen earlier,

$$P(r) = \binom{n}{r} [P(\bar{D})]^r [P(D)]^{n-r} = \frac{n!}{r!(n-r)!} [P(\bar{D})]^r [P(D)]^{n-r}$$

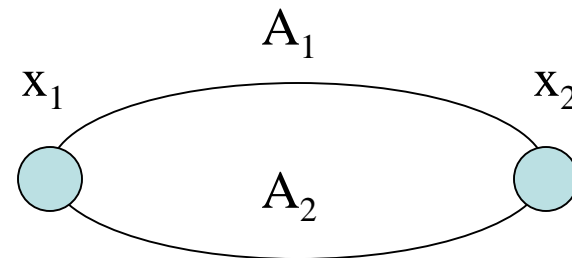
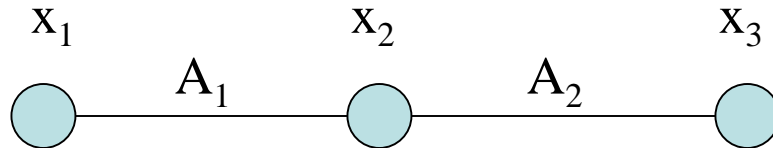
- Changing to reliability notation the same equation is seen as:

$$R_{sys}(t) = \sum_{n=M}^N \frac{N!}{n!(N-n)!} [R(t)]^n [1-R(t)]^{N-n}$$

- A simple example of the use of this logic is given on page 14 of your Chapter 4 lecture notes. We will discuss that case.
- A bit further on we will come back to the actual case of the design of SDS1 and SDS2.

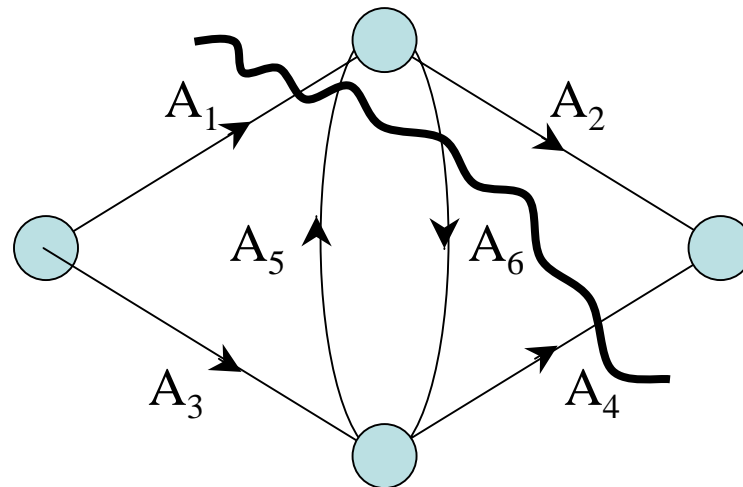
Signal Flow Graphs

- These diagrams are fully equivalent to the block diagrams we have already seen, but they do sometimes simplify the visualization of the “cut sets” that are our next topic.
- These figures show signal flow graphs for two units operating in series and in active-parallel.



Cut-Set Method for Finding System Reliability

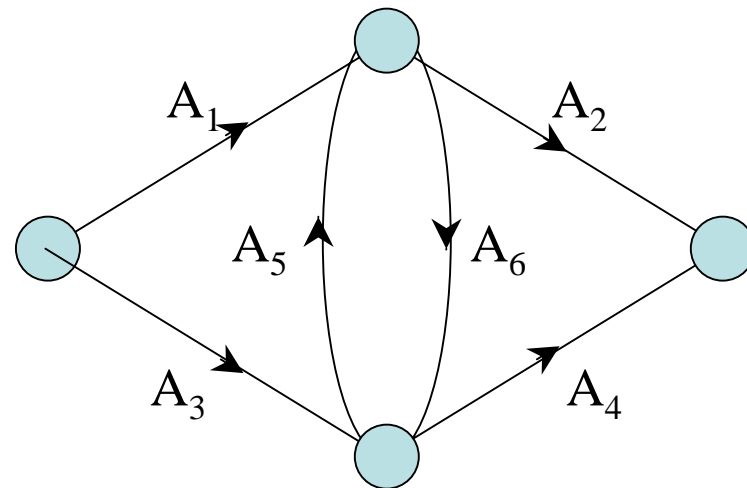
- **Defined:** *cut set* is a set of system events that, if they all occur, will cause system failure.
- **Defined:** A *minimal cut set* is a cut set that has no other cut set as a subset. Otherwise, if any event is removed from a minimal cut set, the system will not fail.



Cut Sets -- 2

- The wavy line in the figure defines one event, $C_1=A_1A_5A_6A_4$.
- Other cut sets are

- $C_2=A_1A_3$
- $C_3=A_2A_4$
- $C_4=A_1A_5A_3$
- $C_5=A_2A_6A_4$
- $C_6=A_3A_5A_6A_2$
- $C_7=A_1A_5A_4$
- $C_8=A_3A_6A_2$ etc.



- The minimal cut sets are seen to be C_2 , C_3 , C_7 , and C_8 .

Cut Sets 3

- Consider a general system for which all minimal cut sets are denoted by C_n , $n=1$ to N . Then, the system unreliability is:

$$F_{\text{sys}} = P(C_1 + C_2 + C_3 + \dots + C_N)$$

- To evaluate F_{sys} we first need to reduce the minimal cutsets C_n to a form involving all the events A_i . This can be done by utilizing the algebra for events - Boolean algebra. The main rules of this algebra are listed on the next slide.

Commutative law	$XY = YX$
	$X + Y = Y + X$
Associative law	$X(YZ) = (XY)Z$
	$X + Y + Z = (X + Y) + Z$
Idempotent law	$XX = X$
	$X + X = X$
Absorption law	$X((X + Y)) = XX + XY = X$
	$X + XY = X$
Distributive law	$X(Y + Z) = XY + XZ$
	$(X + Y)(X + Z) = X + YZ$
Complementation	$X\bar{X} = \phi$ (null event)
	$X + \bar{X} = \Omega$ (universal event)
De Morgan theorems	$\overline{(\bar{X}\bar{Y})} = \bar{X} + \bar{Y}$
	$\overline{(\bar{X} + \bar{Y})} = \bar{X} + \bar{Y}$
Unnamed but frequently useful relationships	$(X + \bar{X}Y) = X + Y$
	$\bar{X}(X + \bar{Y}) = \bar{X}\bar{Y}$

Cut Sets 4 - The Rules of Boolean Algebra

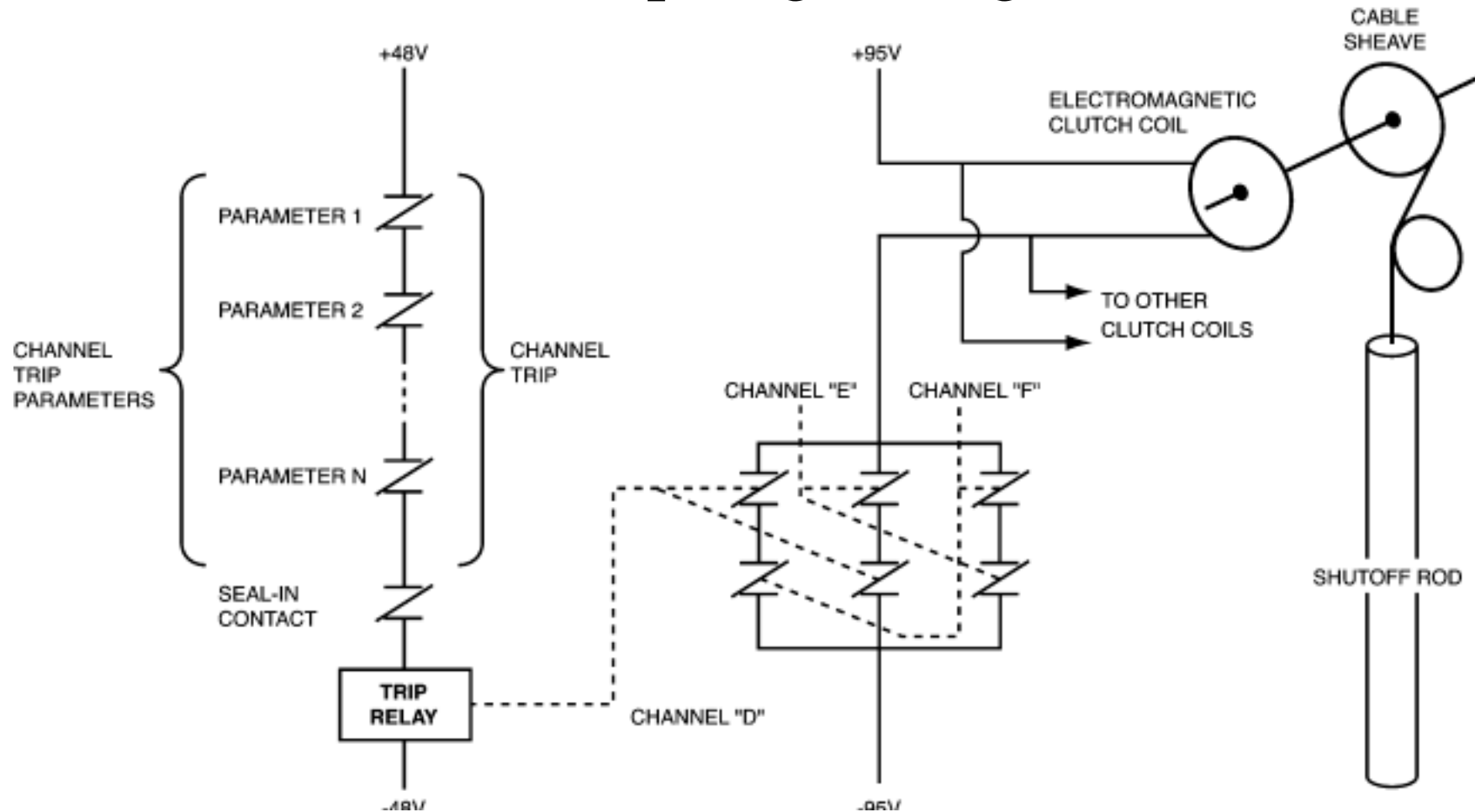
Cut Sets 5

- Boolean algebra rules are useful in several ways:
 - Commutative and associative laws are similar to ordinary algebra.
 - Idempotent law allows cancellation of redundancies of the same event.
 - Absorption simplifies union events - if X has occurred then $(X+Y)$ also has.
 - Distributive laws are used often in fault tree analysis
 - De Morgan theorems useful for system success rather than failure analysis.
- Large cut sets as occur in the analysis of reactor safety can be analyzed reasonably only using computer codes -- otherwise the tasks are too tedious.
- It is sufficient to know that one of the ways to evaluate a large fault tree numerically is to first determine the minimal cut sets and then calculate the system failure probability.

CANDU Shutdown Systems

- The reliability requirement for these systems is stated clearly in plant operating licenses -- the system's expected future unavailability must not exceed 10^{-3} per demand. Design and testing requirements are also given.
- In addition to being very reliable in shutting down the reactor on demand from instrumentation, the systems must be highly reliable to NOT shut the reactor down spuriously.
- At least two measured parameters must be installed on each trip chain to initiate shutdown in response to exceeding safety limits
- To the extent possible the systems must be designed to fail in the direction of safety.

SDS1 Trip Logic Diagram



SDS2 Trip Logic

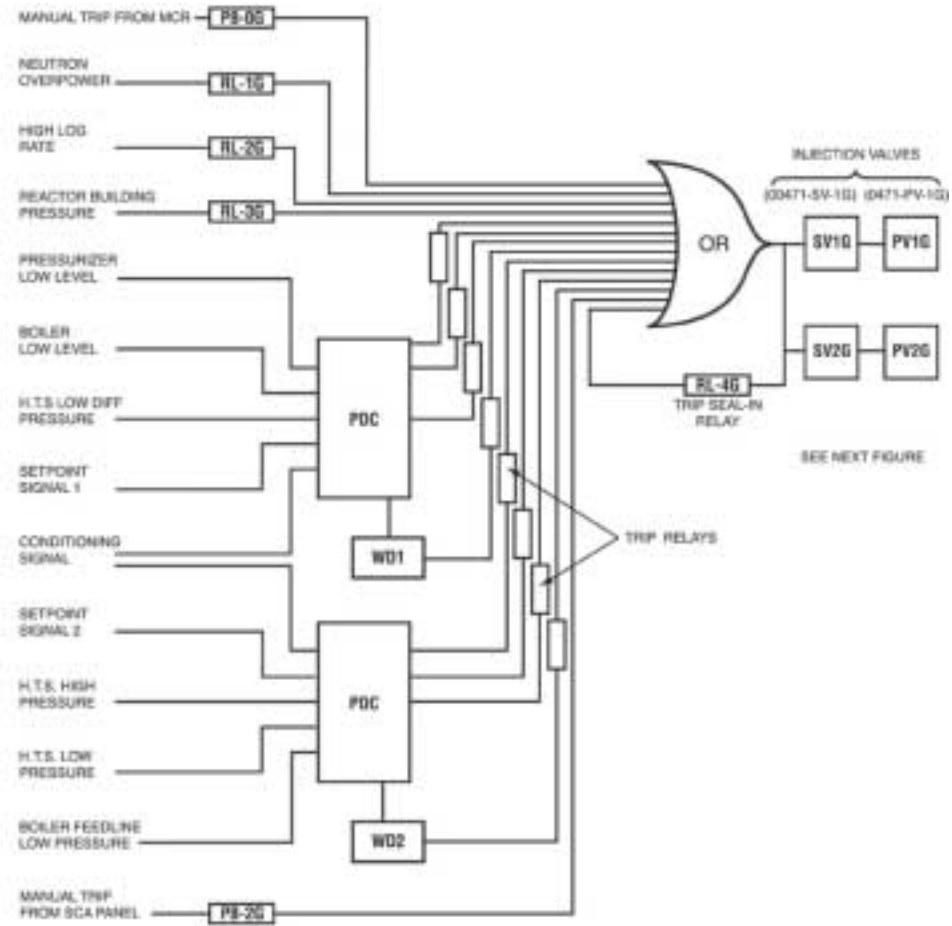


FIGURE 4.3 — CHANNEL "G" TRIP CHAIN

SDS2 Injection Logic

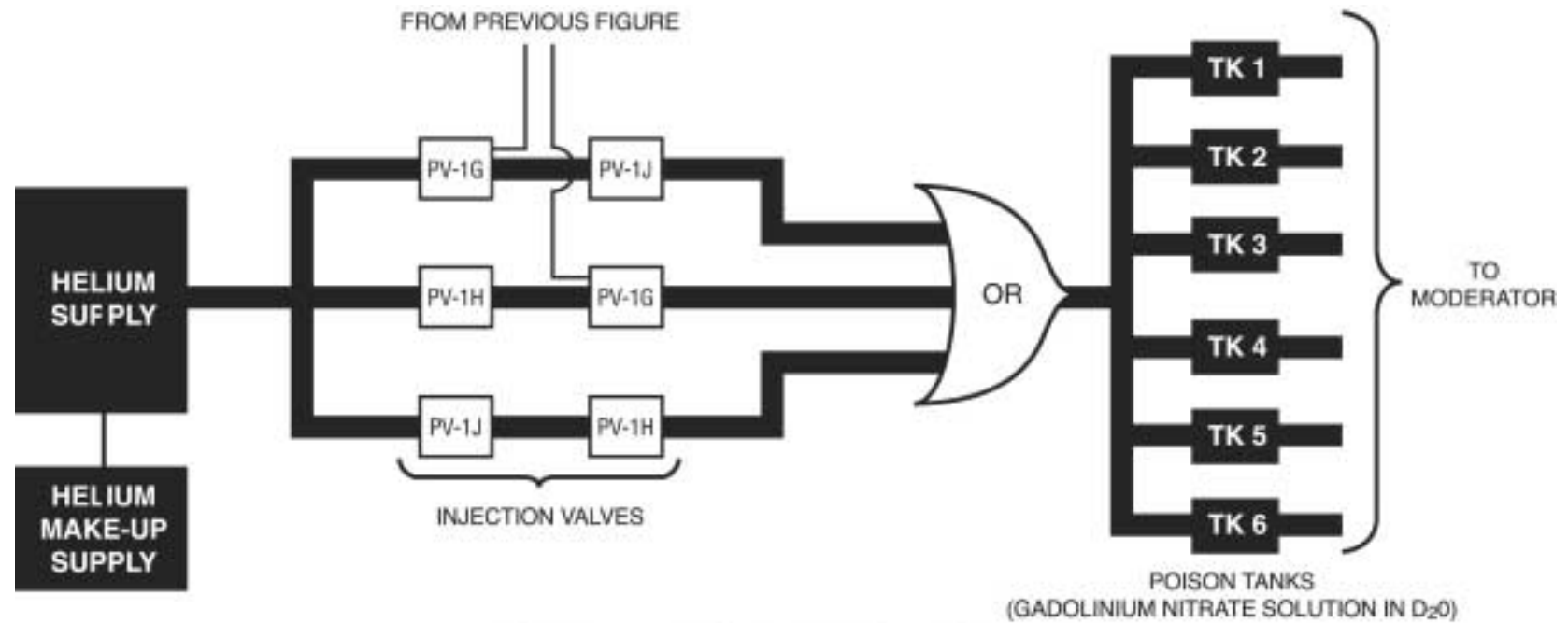


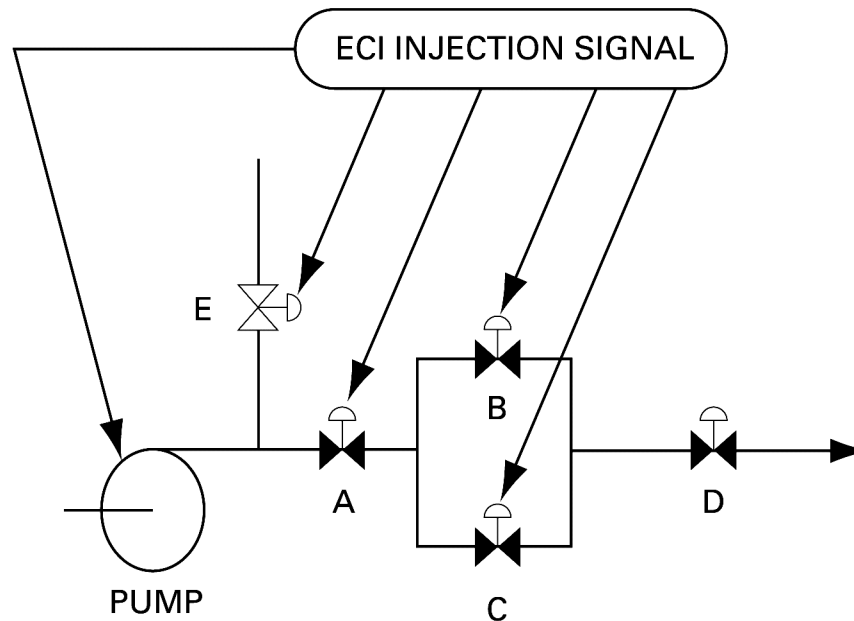
FIGURE 4.4 — SDS2 INJECTION LOGIC

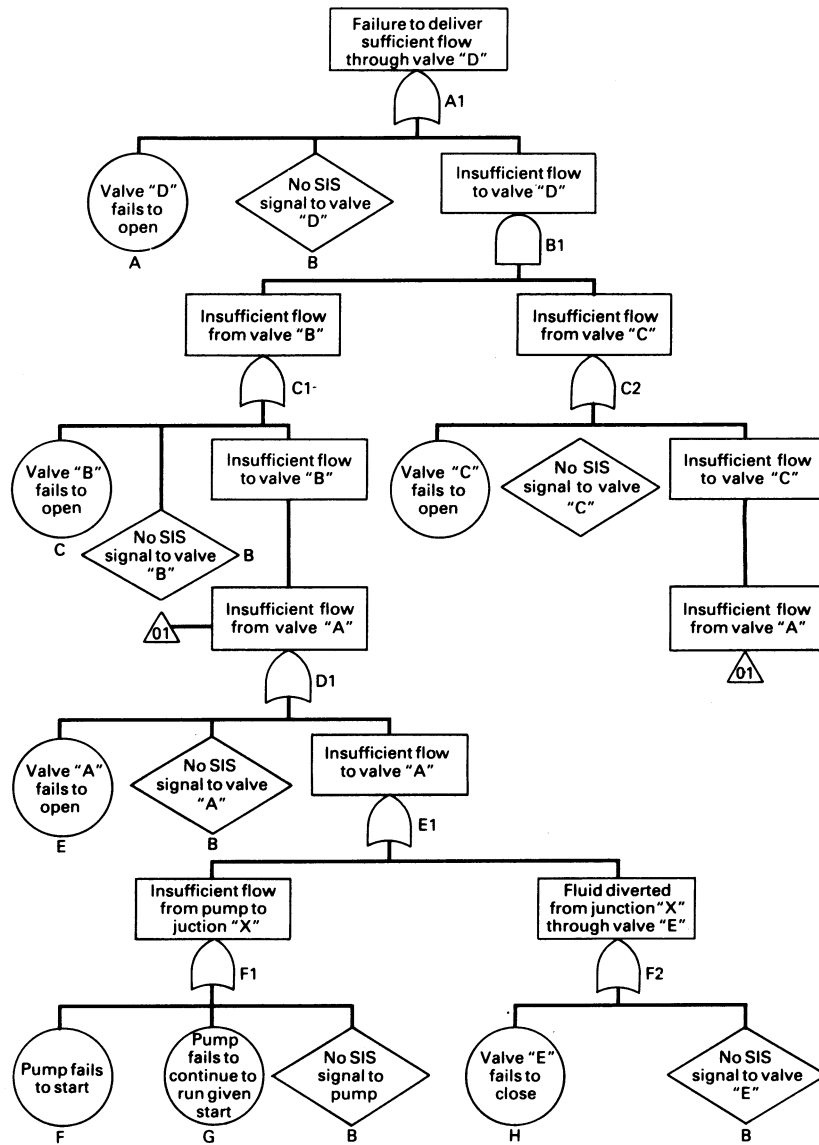
Fault Tree Analysis for Reliability

- Event sequence diagrams usually used in accident analysis can include only the major event branches such as special safety system operation or failure.
- Engineering design and maintenance decisions must be based on examination of the behaviour of systems and components in much finer detail.
- Fault trees offer a systematic method for detailed examination of the potential failure modes of these complex systems, and can provide estimates of the resulting branching probabilities of major systems in the event sequence diagrams.
- ---- Brief discussion of the fault tree example shown in the prepared notes of Chapter 4 of this course.----

A Simple Emergency Coolant Injection System

- Actions for necessary for success:
 - Start pump
 - Close valve 'E'
 - Open valves 'A' and 'D'
 - C





Initial Fault Tree for a Simple Emergency Coolant Injection System

$$\begin{aligned}
A1 &= A + B = B1 \\
B1 &= C1 \cdot C2 \\
C1 &= C + B + D1 \\
C2 &= D + B + D1 \\
D1 &= E + B + E1 \\
E1 &= F1 + F2 \\
F1 &= F + G + B \\
F2 &= H + B
\end{aligned}$$

By substitution,

$$\begin{aligned}
E1 &= (F + G + B) + (H + B) \\
D1 &= E + B + (F + G + B) + (H + B) \\
C2 &= D + B + E + B + (F + G + B) + (H + B) \\
C1 &= C + B + E + B + (F + G + B) + (H + B) \\
B1 &= (C + B + E + B + (F + G + B) + (H + B)) \cdot (D + B + E + B + (F + G + B) + (H + B)) \\
A1 &= (C + B + E + B + (F + G + B) + (H + B)) \cdot (D + B + E + B + (F + G + B) + (H + B))
\end{aligned}$$

Simplifying,

$$\begin{aligned}
A1 &= A + B + (C + B + E + B + F + G + H + B) \cdot (D + B + E + B + F + G + B) \\
&= A + B + (C + B + E + B + F + G + H + B) \cdot (D + B + E + F + G + H)
\end{aligned}$$

Multiplying,

$$\begin{aligned}
A1 &= A + B + CD + CB + CE + CF + CG + CH + BD + BB + BE + BF + BG + BH + ED \\
&\quad + EF + EG + EH + FC + FB + FE + FG + FH + GD + GB + GE + GF + GG + GH + HD + HB
\end{aligned}$$

Using identity "X.X=X",

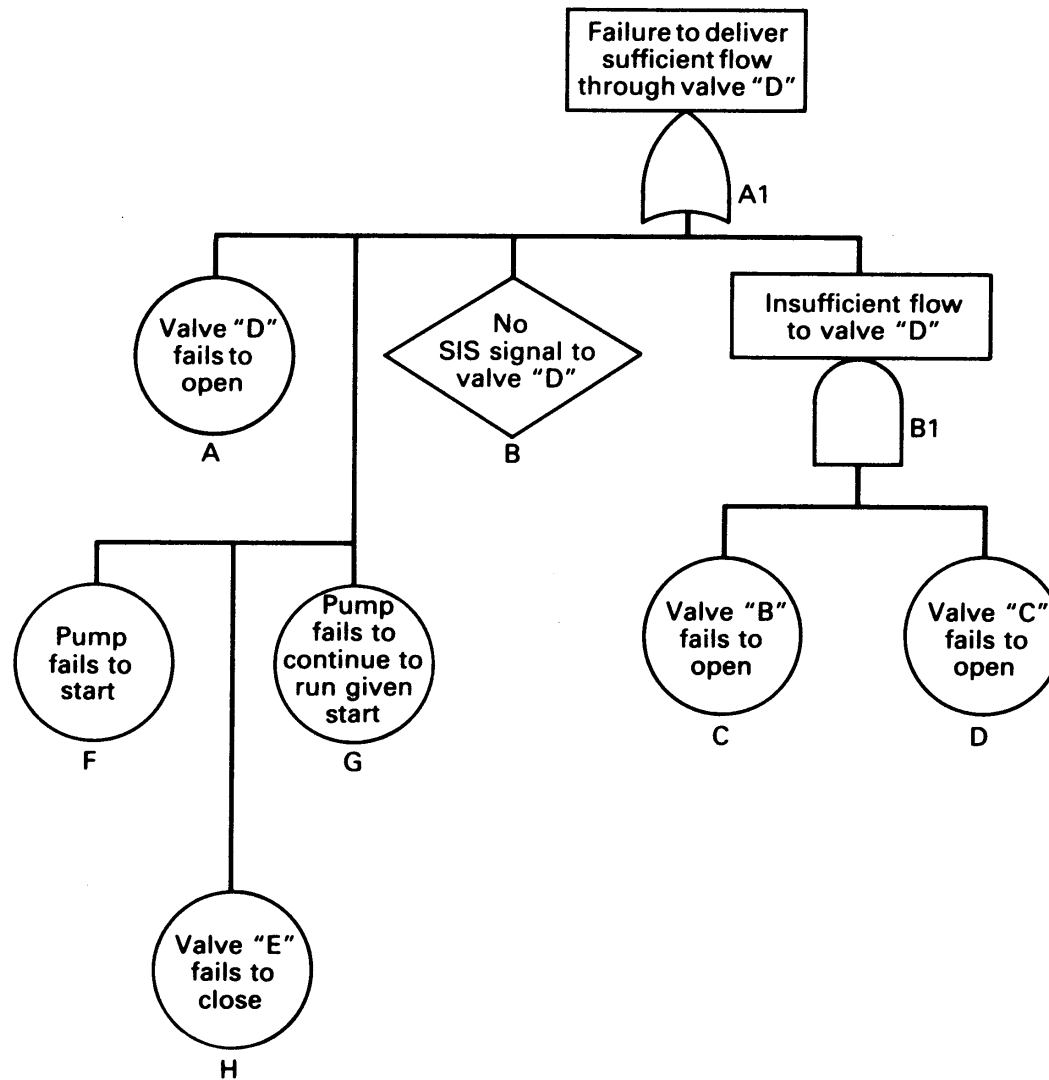
$$\begin{aligned}
A1 &= A + B + CD + CB + CE + CF + CG + CH + BD + B + BE + BF + BG + BH + ED + \\
&\quad + FE + F + FG + FH + GD + GB + GE + GF + G + GH + HD + HB + HE
\end{aligned}$$

Using identity "X+(X.Y)=X",

$$A1 = A + B + E + F + G + H + CD$$

Boolean Reduction of Initial Fault Tree for Simple ECI System

Min-cut Fault Tree for Injection System



Success Tree Equivalent to Min-Cut Fault Tree

