Probabilistic Calculations

22.39 Elements of Reactor Design, Operations, and Safety

Lectures 10-11

Fall 2006

George E. Apostolakis
Massachusetts Institute of Technology

General Formulation

$$X_T = \varphi(X_1, \ldots X_n) \equiv \varphi(\underline{X})$$

$$\mathbf{X_T = 1 - \prod_{1}^{N} (1 - M_i) \equiv \coprod_{1}^{N} M_i}$$

$$X_T = \sum_{i=1}^{N} M_i - \sum_{i=1}^{N-1} \sum_{j=i+1}^{N} M_i M_j + \ldots + (-1)^{N+1} \prod_{i=1}^{N} M_i$$

X_T : the TOP event indicator variable

M_i : the ith minimal cut set or accident sequence

TOP-event Probability

$$P(X_T) = \sum_1^N P(M_i) + \ldots + (-1)^{N+1} P\left(\prod_1^N M_i\right)$$

$$P(X_T) \cong \sum_1^N P(M_i)$$ **Rare-event approximation**

The question is how to calculate the probability of M_i

$$P(M_i) = P(X_k^i \ldots X_m^i)$$

$$P(A/B) \equiv \frac{P(AB)}{P(B)}$$

Conditional probability:

Independent events:

$$P(A/B) = P(A)$$

$$P(AB) = P(A)P(B)$$

MinCutSet Probability

$$P(M) = P(X_1X_2X_3) = P(X_1)P(X_2X_3 / X_1) =$$
$$= P(X_1)P(X_2 / X_1)P(X_3 / X_1X_2)$$

For independent events:

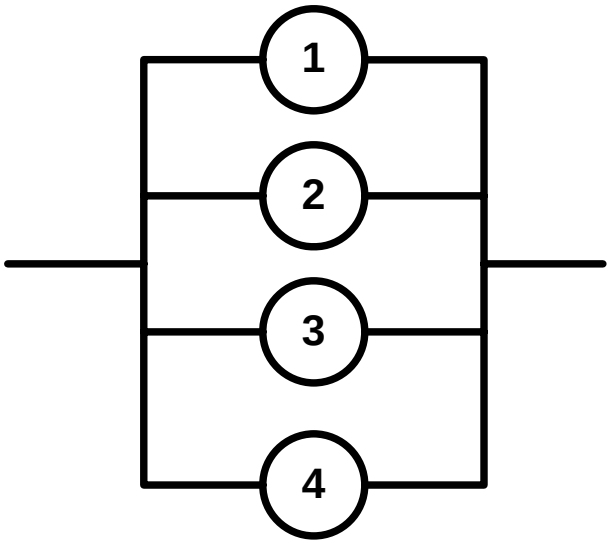
$$P(M) = P(X_1X_2X_3) = P(X_1)P(X_2)P(X_3)$$

For accident sequences, we must include the initiating-event frequency per year:

$$fr(M) = fr(IEX_1X_2) = fr(IE)P(X_1X_2 / IE) = fr(IE)P(X_1 / IE)P(X_2 / IEX_1)$$

$$fr\left(X_T\right) \equiv \text{CDF} \cong \sum_{1}^{N} fr\left(M_i\right)$$

Example: 2-out-of-4 System



$M_1 = X_1 X_2 X_3$ $M_2 = X_2 X_3 X_4$

$M_3 = X_3 X_4 X_1$ $M_4 = X_1 X_2 X_4$

$$X_T = 1 - (1 - M_1)(1 - M_2)(1 - M_3)(1 - M_4)$$

$$X_T = (X_1 X_2 X_3 + X_2 X_3 X_4 + X_3 X_4 X_1 + X_1 X_2 X_4) - 3X_1 X_2 X_3 X_4$$

2-out-of-4 System (cont'd)

$$P(X_T = 1) = P(X_1 X_2 X_3 + X_2 X_3 X_4 + X_3 X_4 X_1 + X_1 X_2 X_4) - 3P(X_1 X_2 X_3 X_4)$$

Assume that the components are independent and nominally identical with failure probability q. Then,

$$P(X_T = 1) = 4q^3 - 3q^4$$

Rare-event approximation: $P(X_T = 1) \cong 4q^3$

Overview

- **We need models for:**
  - **The frequency of initiating events.**
  - **The probability that a component will fail on demand.**
  - **The probability that a component will run for a period of time given a successful start.**

Initiating Events: The Poisson Distribution

- Used typically to model the occurrence of initiating events.
- Discrete Random Variable: Number of events in (0, t)
- The rate λ is assumed to be constant; the events are independent.
- The probability of exactly k events in (0, t) is (pmf):

$$\Pr[k] = e^{-\lambda t}\frac{(\lambda t)^k}{k!}$$

$k! \equiv 1*2*\ldots*(k-1)*k \qquad 0! = 1$

$$m = \lambda t \qquad \sigma^2 = \lambda t$$

Example of the Poisson Distribution

- *A component fails due to "shocks" that occur, on the average, once every 100 hours. What is the probability of exactly one replacement in 100 hours? Of no replacement?*

- $\lambda\ t = 10^{-2}*100 = 1$
- $\Pr[1\ \text{repl.}] = e^{-\lambda t} = e^{-1} = 0.37 = \Pr[\text{no replacement}]$
- **Expected number of replacements: 1**

$$\Pr[2\text{repl}] = e^{-1}\frac{1^2}{2!} = \frac{e^{-1}}{2} = 0.185$$

$$\Pr[k \le 2] = 0.37 + 0.37 + 0.185 = 0.925$$

Reliability and Availability

- **Reliability: Probability of successful operation over a period (0, t).**
- **Availability: Probability the item is working at time t.**

- **Note:**
  - **In industrial applications, the term "reliability" includes the probability that a safety system will start successfully and operate for a period (0, t).**
  - **The term "unavailability" usually refers to maintenance.**

Failure while running

- **T: the time to failure of a component (continuous random variable).**
- **$F(t) = P[T < t]$: failure distribution (unreliability)**
- **$R(t) \equiv 1-F(t) = P[t < T]$: reliability**
- **m: mean time to failure (MTTF)**
- **f(t): failure density, $f(t)dt = P\{$failure occurs between t and $t+dt\} = P\ [t < T < t+dt]$**

The Hazard Function or Failure Rate

$$h(t) \equiv \frac{f(t)}{R(t)} = \frac{f(t)}{1 - F(t)} \qquad F(t) = 1 - \exp\left(- \int_0^t h(s) ds \right).$$

The distinction between h(t) and f(t) :

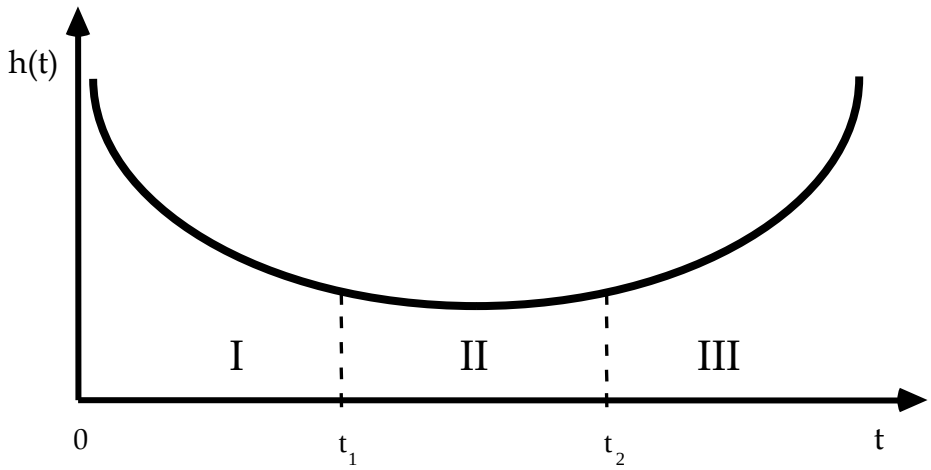
f(t)dt: unconditional probability of failure in (t, t +dt),

$$f(t)dt = P\ [t < T < t+dt]$$

h(t)dt: conditional probability of failure in (t, t +dt) given that the component has survived up to t.

$$h(t)dt = P\ [t < T < t+dt / \{ t < T \}]$$

The "Bathtub" Curve



I	Infant Mortality
II	Useful Life
III	Aging (Wear-out)

The Exponential Distribution

- f(t) = $\lambda e^{-\lambda t}$ $\lambda > 0$ $t > 0$ (failure density)

- $F(t) = 1 - e^{-\lambda t}$ $R(t) = e^{-\lambda t}$

- h(t) = λ constant (no memory; the *only* pdf with this property) $\Rightarrow$ useful life on bathtub curve

$F(t) \cong \lambda t$ for $\lambda t < 0.1$ (*another* rare-event approximation)

$$m = \frac{1}{\lambda} = \sigma$$

Example: 2-out-of-3 system

Each sensor has a MTTF equal to 2,000 hours. What is the unreliability of the system for a period of 720 hours?

- ***Step 1: System Logic.***

$$X_T = (X_A X_B + X_B X_C + X_C X_A) - 2X_A X_B X_C$$

Example: 2-out-of-3 system (2)

Step 2: Probabilistic Analysis.

For nominally identical components:

$P(X_T) = 3q^2 - 2q^3$

$$q = F(t) = 1 - e^{-\lambda t} \qquad \lambda = 5x10^{-4} \quad hr^{-1}$$

System Unreliability:

$$F_T(t) = 3\left(1 - e^{-\lambda t}\right)^2 - 2\left(1 - e^{-\lambda t}\right)^3$$

Rare event approximation:

$$F_T(t) \cong 3(\lambda t)^2 - 2(\lambda t)^3$$

A note on the calculation of the MTTF

$$MTTF = \int_0^\infty R(t)dt$$

Proof

$$MTTF = \int_0^\infty tf(t)dt = \int_0^\infty t(-\frac{dR}{dt})dt = -\int_0^\infty tdR =$$

$$= -tR_0^\infty + \int_0^\infty R(t)dt = \int_0^\infty R(t)dt$$

A note on the calculation of the MTTF (cont.)

since

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

and

$$R(t \to \infty) \to 0 \quad \text{faster} \quad \text{than} \quad t \to \infty$$

MTTF Examples

Single exponential component:

$$\mathbf{MTTF} = \int_0^\infty \mathbf{e}^{-\lambda t}\mathbf{dt} = \frac{\mathbf{1}}{\boldsymbol{\lambda}}$$

Series system:

$$\mathrm{MTTF} = \int_0^\infty dt e^{-m\lambda t} = \frac{1}{m\lambda} \equiv \frac{1}{\lambda_{system}}$$

1-out-of-2 system :

$$\mathrm{MTTF} = \int_0^\infty dt\left(2e^{-\lambda t} - e^{-2\lambda t}\right) = \frac{3}{2\lambda}$$

2-out-of-3 system :

$$\mathrm{MTTF} = \int_0^\infty R_T(t)dt = \int_0^\infty [1-3(1-e^{-\lambda t})^2 + 2(1-e^{-\lambda t})^3]dt = \frac{5}{6\lambda}$$

MTTF Examples: 2-out-of-3 System

Using the result for $F_T(t)$ on slide 15, we get

$$\text{MTTF} = \int_0^\infty R_T(t)dt = \int_0^\infty [1 - 3(1 - e^{-\lambda t})^2 + 2(1 - e^{-\lambda t})^3]dt$$

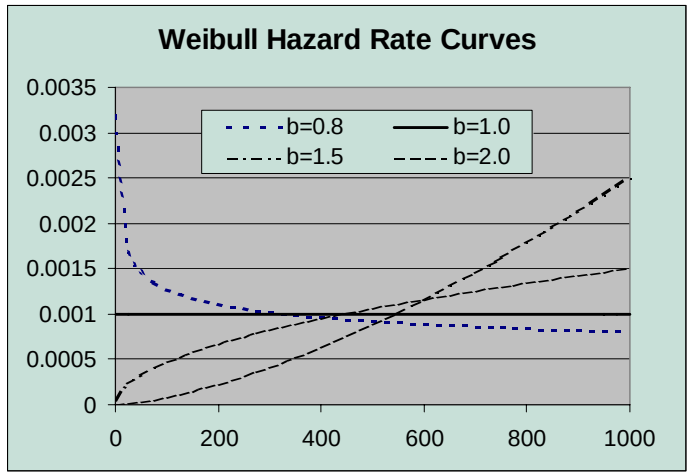
$$\text{MTTF} = \frac{1}{2\lambda} + \frac{1}{3\lambda} = \frac{5}{6\lambda}$$

The MTTF for a single exponential component is: $\frac{1}{\lambda}$

$\Rightarrow$ The 2-out-of-3 system is slightly worse.

The Weibull failure model

Adjusting the value of b, we can model any part of the bathtub curve.



$$h(t) = b\lambda^{b} t^{b-1}$$

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

For b = 1 ⇒ the exponential distribution.

The Model of the World

- ***Deterministic, e.g., a mechanistic computer code***
- ***Probabilistic (Aleatory), e.g., $R(t/\lambda) = exp(-\lambda t)$***
- ***Both deterministic and aleatory models of the world have assumptions and parameters.***
- ***How confident are we about the validity of these assumptions and the numerical values of the parameters?***

The Epistemic (state-of-knowledge) Model

- **Uncertainties in assumptions are not handled routinely. If necessary, sensitivity studies are performed.**
- **Parameter uncertainties are reflected on appropriate probability distributions.**
- **For the failure rate: $\pi(\lambda)\, d\lambda$ = Pr(the failure rate has a value in $d\lambda$ about λ)**

Unconditional (predictive) probability

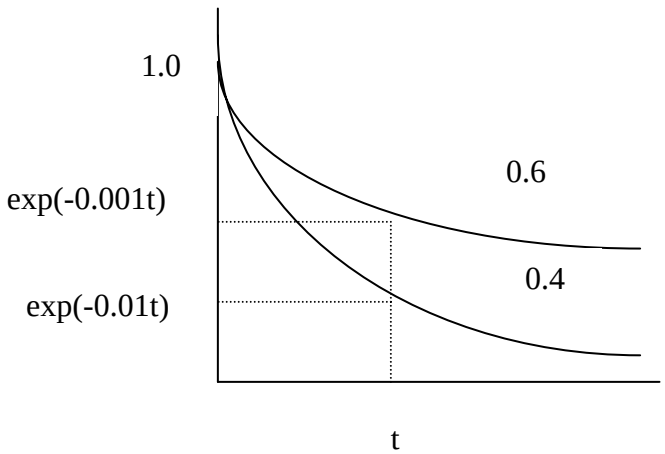
$$R(t) = \int R(t/\lambda)\pi(\lambda)d\lambda$$

Communication of Epistemic Uncertainties: The discrete case

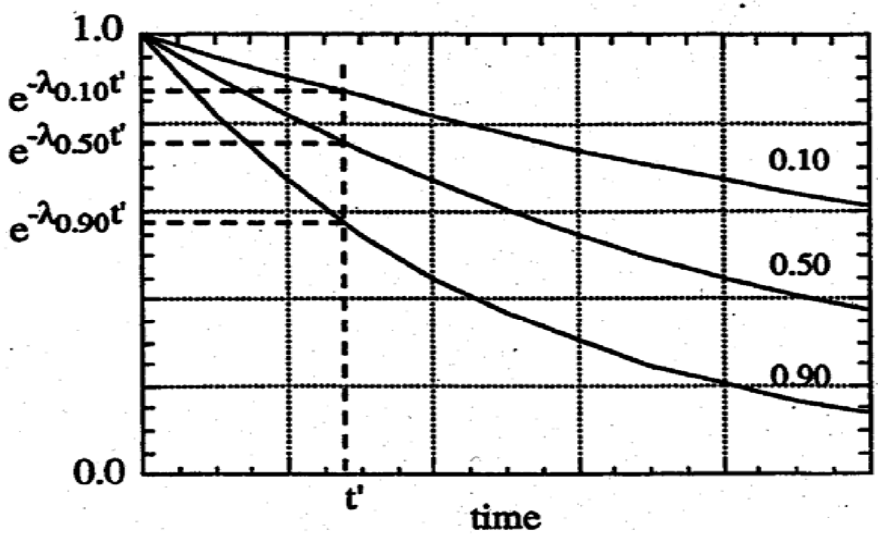
Suppose that $P(\lambda = 10^{-2}) = 0.4$ and $P(\lambda = 10^{-3}) = 0.6$

Then, $P(e^{-0.001t}) = 0.6$ and $P(e^{-0.01t}) = 0.4$

$R(t) = 0.6\ e^{-0.001t} + 0.4\ e^{-0.001t}$



Communication of Epistemic Uncertainties: The continuous case



Courtesy of US NRC.

The lognormal distribution

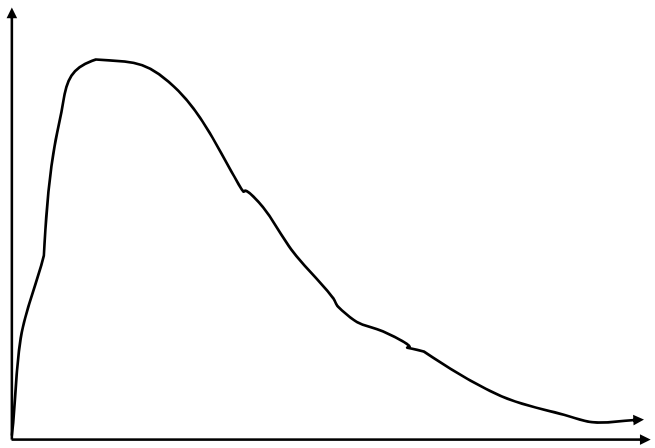
- **It is very common to use the lognormal distribution as the epistemic distribution of failure rates.**

$$\pi(\lambda) = \frac{1}{\sqrt{2\pi}\sigma\lambda}\exp\left[-\frac{(\ln\lambda-\mu)^2}{2\sigma^2}\right] \qquad m = \exp\left[\mu+\frac{\sigma^2}{2}\right]$$

$$\lambda_{95} = e^{\mu+1.645\sigma} \qquad \text{median}: \lambda_{50} = e^{\mu}$$

$$\lambda_{05} = e^{\mu-1.645\sigma}$$

$$EF = \frac{\lambda_{95}}{\lambda_{50}} = \frac{\lambda_{50}}{\lambda_{05}} = \sqrt{\frac{\lambda_{95}}{\lambda_{05}}}$$



$$Y = \ln\lambda$$

Y is normally distributed with mean μ and standard deviation σ

Component/Primary Failure Modes	Assessed Values	
	Lower Bound	Upper Bound
Mechanical Hardware		
Pumps		
Failure to start, Q_d:	3×10^{-4}/d	3×10^{-3}/d
Failure to run, λ_o: (Normal Environments)	3×10^{-6}/hr	3×10^{-4}/hr
Valves		
Motor Operated		
Failure to operate, Q_d:	3×10^{-4}/d	3×10^{-3}/d
Plug, Q_d:	3×10^{-5}/d	3×10^{-4}/d
Solenoid Operated		
Failure to operate, Q_d:	3×10^{-4}/d	3×10^{-3}/d
Plug, Q_d:	3×10^{-5}/d	3×10^{-4}/d
Air Operated		
Failure to operate, Q_d:	1×10^{-4}/d	1×10^{-3}/d
Plug, Q_d:	3×10^{-5}/d	3×10^{-4}/d
Check		
Failure to open, Q_d:	3×10^{-5}/d	3×10^{-4}/d
Relief		
Failure to open, Q_d:	3×10^{-6}/d	3×10^{-5}/d
Manual		
Plug, Q_d:	3×10^{-5}/d	3×10^{-4}/d
Pipe		
Plug/rupture		
$\leq$ 3" diameter, λ_o:	3×10^{-11}/hr	3×10^{-8}/hr
> 3" diameter, λ_o:	3×10^{-12}/hr	3×10^{-9}/hr
Clutches		
Mechanical		
Failure to engage/ disengage	1×10^{-4}/d	1×10^{-3}/d
Electrical Hardware		
Electrical Clutches		
Failure to operate, Q_d:	1×10^{-4}/d	1×10^{-3}/d

Courtesy of US NRC.

(Continued)

Component/Primary Failure Modes	Assessed Values	
	Lower Bound	Upper Bound
Motors		
Failure to start, Q_d:	1×10^{-4}/d	1×10^{-3}/d
Failure to run (Normal Environments), λ_o:	3×10^{-6}/hr	3×10^{-5}/hr
Transformers		
Open/shorts, λ_o:	3×10^{-7}/hr	3×10^{-6}/hr
Relays		
Failure to energize, Q_d:	3×10^{-5}/d	3×10^{-4}/d
Circuit Breaker		
Failure to transfer, Q_d:	3×10^{-4}/d	3×10^{-3}/d
Limit Switches		
Failure to operate, Q_d:	1×10^{-4}/d	1×10^{-3}/d
Torque Switches		
Failure to operate, Q_d:	3×10^{-5}/d	3×10^{-4}/d
Pressure Switches		
Failure to operate, Q_d:	3×10^{-5}/d	3×10^{-4}/d
Manual Switches		
Failure to operate, Q_d:	3×10^{-6}/d	3×10^{-5}/d
Battery Power Supplies		
Failure to provide proper output, λ_s:	1×10^{-6}/hr	1×10^{-5}/hr
Solid State Devices		
Fails to function, λ_o:	3×10^{-7}/hr	3×10^{-5}/hr
Diesels (complete plant)		
Failure to start, Q_d:	1×10^{-2}/d	1×10^{-1}/d
Failure to run, λ_o:	3×10^{-4}/hr	3×10^{-2}/hr
Instrumentation		
Failure to operate λ_o:	1×10^{-7}/hr	1×10^{-5}/hr

Courtesy of US NRC.

(a) All values are rounded to the nearest half order of magnitude on the exponent.

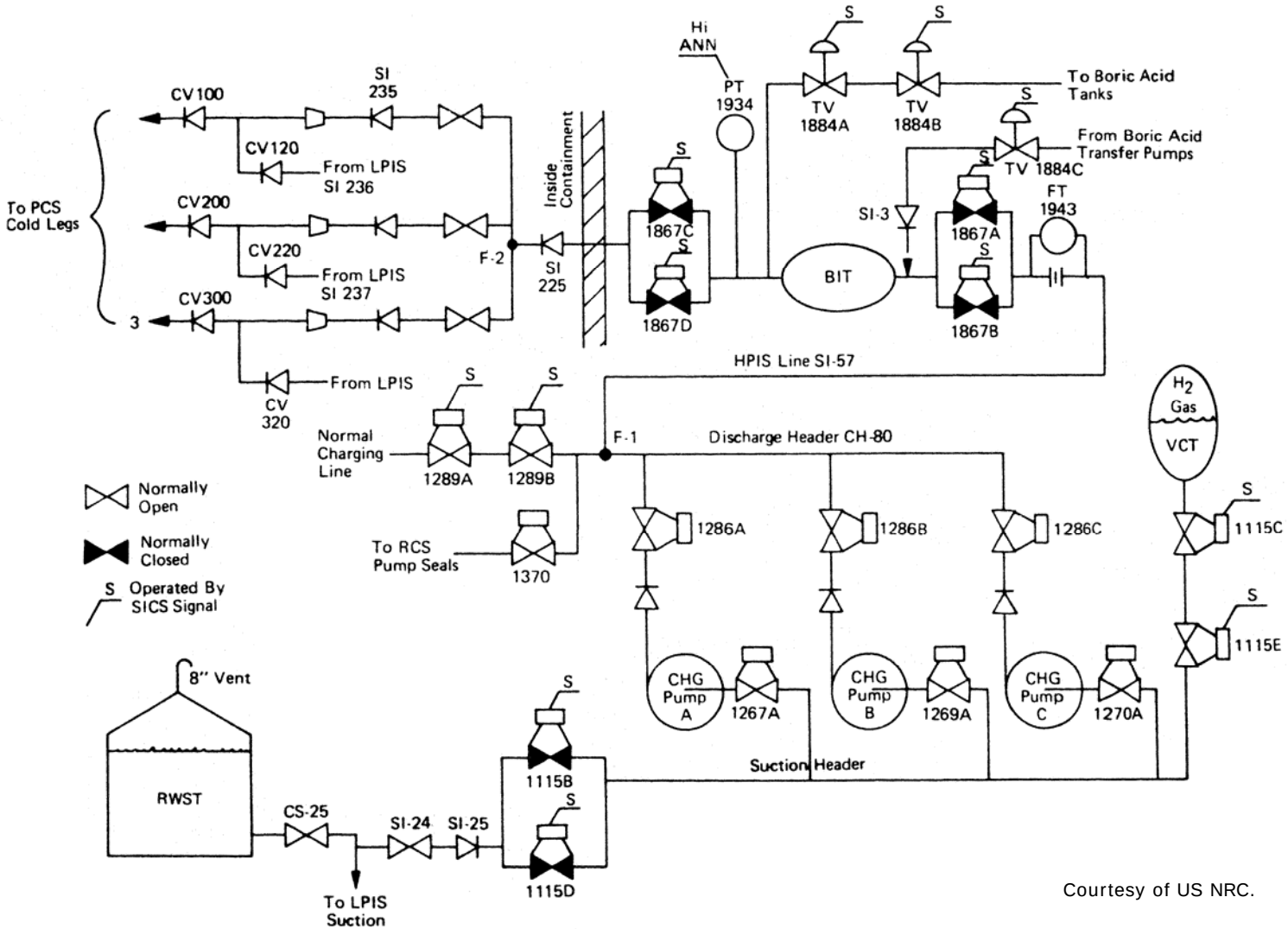
(b) Derived from averaged data on pumps, combining standby and operate time.

(c) Approximated from plugging that was detected.

(d) Derived from combined standby and operate data.

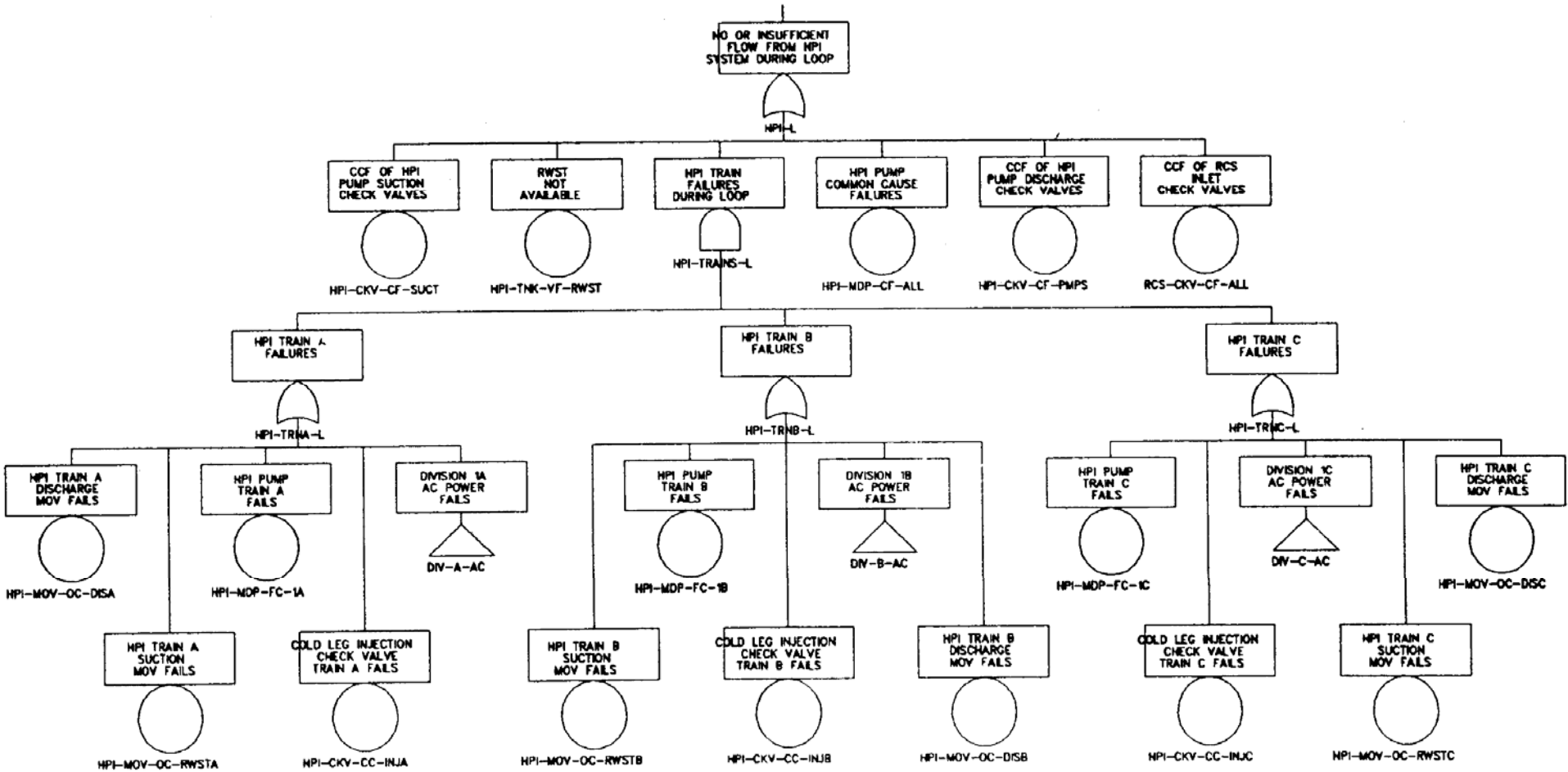
(e) Derived from standby test on batteries, which does not include load.

SIMPLIFIED SYSTEM DIAGRAM



Courtesy of US NRC.

HIGH PRESSURE INJECTION DURING LOOP 1-0F-3 TRAINS FOR SUCCESS



Courtesy of US NRC.

HPIS Analysis (1-out-of-3)

- **In the RSS HPIS, the three pump trains have a common suction line from the RWST. The South Texas Project design has separate suction lines for the three trains, as the fault tree shows.**

- $Q_{total} = Q_{singles} + Q_{doubleFail's} + Q_{test\&maint} + Q_{CCF}$

- **<u>Representative single failures (single-element mcs)</u>:**
  - **Check valve SI 225 fails to open**
  - **Check valve SI-25 fails to open**
  - **RWST discharge line ruptures**
  - **Other**

- $Q_{singles} = 1.1 \times 10^{-3}$ **("point estimate")**

HPIS: Double Failures

- **Representative double failures (double-element mcs):**
  - **RWST supply MOVs 1115B and 1115D fail to open**
  - **Born Injection Tank (BIT) inlet MOVs 1867A and 1867B fail to open**
  - **BIT discharge MOVs 1867C and 1867D fail to open**
  - **Service water pumps; cooling water pumps; BIT cooling system**
  - **other**
- **Q(MOVs 1867C and 1867D fail to open) = $P(X_1)\ P(X_2)$**

where $P(X_i)$ is a lognormal with median 1.9×10^{-2} and EF = 3

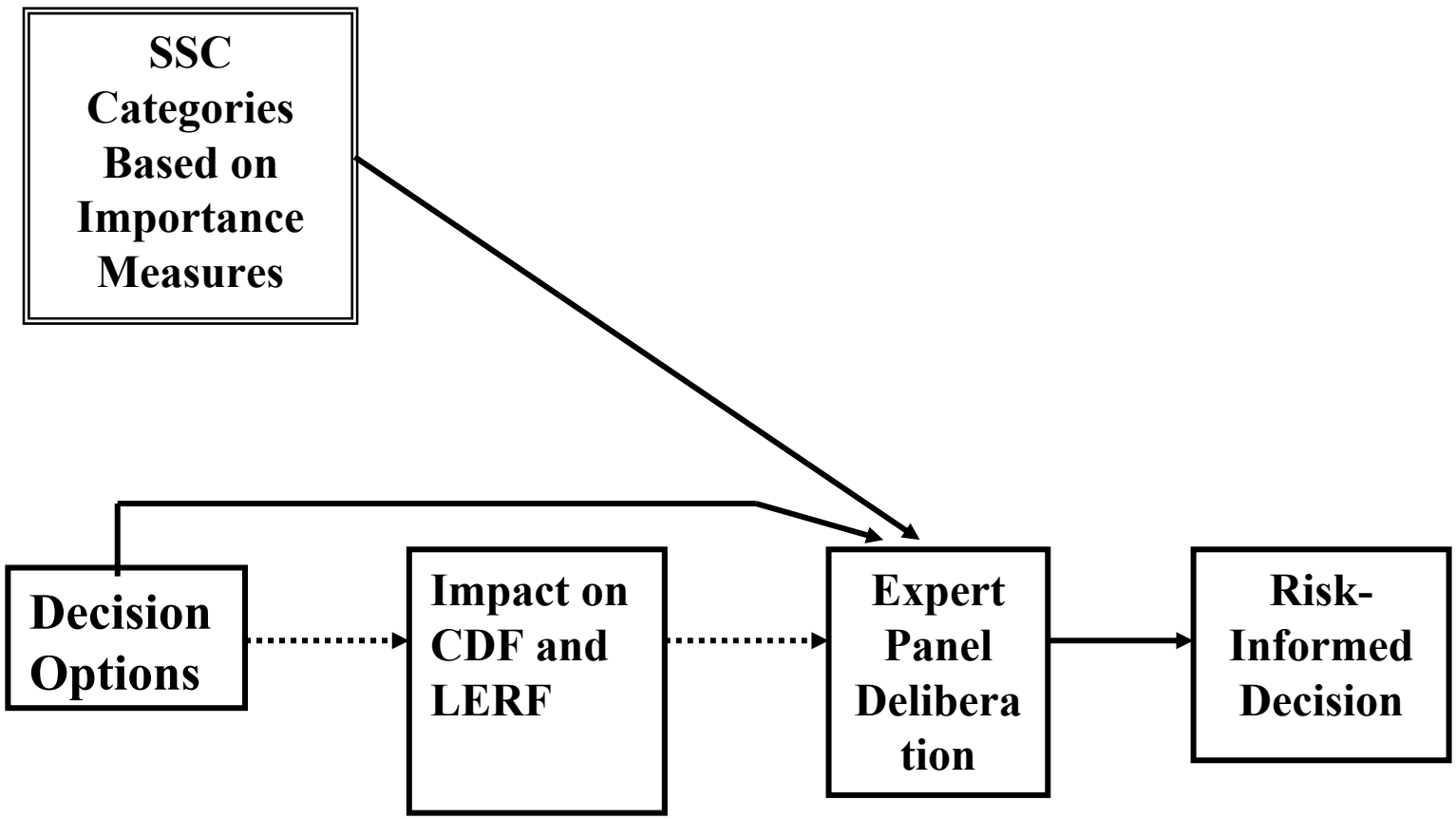
- **$Q_{doubleFail's} = 2.5 \times 10^{-3}$ ("point estimate")**

HPIS: Other Contributions

- $Q_{test\&maint}$ is negligible because of the 1-out-of-3 redundancy (if one train is out, double failures must occur for the system to fail).
- Q_{CCF}(MOVs 1867C and 1867D fail to open) = $\beta P(X_1)$ = = $0.075 \times 1.9 \times 10^{-2} = 1.4 \times 10^{-3}$

- Monte Carlo simulation yields (RSS):
  - $Q_{total,median} = 8.6 \times 10^{-3}$
  - $Q_{total,upper} = 2.7 \times 10^{-2}$
  - $Q_{total,lower} = 4.4 \times 10^{-3}$

In some important cases, ΔCDF and ΔLERF cannot be calculated.



Fussell-Vesely Importance Measure

$$FV_i = \frac{\Pr[\bigcup_k M_k^{(i)}]}{R^0} = \frac{R^0 - R^{-i}}{R^0} = 1 - \frac{R^{-i}}{R^0}$$

R^0 The base-case risk metric (CDF or LERF) = $\Pr[\bigcup_k M_k]$

$M_k^{(i)}$ The k^{th} accident sequence containing event i

R^{-i} The risk metric (CDF or LERF) with the i^{th} component up (unavailability equal to zero)

Risk Reduction Worth (RRW)

$$RRW_i = \frac{R^0}{R^{-i}}$$

$$FV_i = \frac{R^0 - R^{-i}}{R^0} = 1 - \frac{R^{-i}}{R^0} = 1 - \frac{1}{RRW_i}$$

- FV_i is the fractional decrease in the risk metric when event i is always true (component i is always available; its unavailability is set equal to zero).

- This importance measure is particularly useful for identifying improvements to the reliability of elements which can most reduce risk.

F-V Ranking

Loss Of Offsite Power Initiating Event	0.831
DIESEL GENERATOR B FAILS	0.437
DIESEL GENERATOR A FAILS	0.393
COMMON CAUSE FAILURE OF DIESEL GENERATORS	0.39
OPERATOR FAILS TO RECOVER OFFSITE POWER (SEAL LOCA)	0.388
RCP SEALS FAIL W/O COOLING AND INJECTION	0.344
OPERATOR FAILS TO RECOVER OFFSITE POWER BEFORE BATTERY DEPLETION	0.306

Risk Achievement Worth (RAW)

$$RAW_i = \frac{R^{+i}}{R^0}$$

R^{+i} **The risk metric (CDF or LERF) with the i^{th} component always down (its unavailability is set equal to 1)**

RAW presents a measure of the "worth" of the basic event in "achieving" the present level of risk and indicates the importance of maintaining the current level of reliability for the basic event.

RAW Ranking

Loss Of Offsite Power Initiating Event	51,940
Steam Generator Tube Rupture Initiating Event	41,200
Small Loss Of Coolant Accident Initiating Event	40,300
CONTROL ROD ASSEMBLIES FAIL TO INSERT	3,050
COMMON CAUSE FAILURE OF DIESEL GENERATORS	271
RPS BREAKERS FAIL TO OPEN	202

Comments on Importance Measures

- Importance measures are typically evaluated for individual SSCs, not groups.
- The various categories of risk significance are determined by defining threshold values for the importance measures. For example, in some applications, a SSC is in the "high" risk-significant category when FV $\geq$ 0.005 and RAW $\geq$ 2.0.
- Importance measures are strongly affected by the scope and quality of the PRA. For example, incomplete assessments of risk contributions from low-power and shutdown operations, fires, and human performance will distort the importance measures.