PRA & PSA

- Probability Risk Assessment
  - PRA
- Probability Safety Assessment
  - PSA
- Fault Tree Analysis
  - FTA
- Event Tree Analysis
  - ETA
**PRA & PSA**

- **Probability Risk/Safety Assessment**
  - general term for risk assessments that use probability models to represent the likelihood of different risk levels
  
  - reliability assessment methods used to analyze systems which are considered critical

  - PSA normally deals with issues of safety
  - PRA may deal with non-safety issues
Definitions

- **Variability**
  - true heterogeneity or diversity
  - example: drinking water
    » for different people the risk from consuming the water may vary
    » could be caused by different body weight, exposure duration & frequency
Definitions

- **Uncertainty**
  - caused by lack of knowledge
  - example: drinking water
    » risk assessor is certain that different people consume different amounts of water
    » BUT may be uncertain about how much variability there is
Definitions

- **Random Variable** $X$
  - a function that assigns a real number $X(s)$ to each sample point $s$ in sample space $S$
  - e.g. coin toss, number of heads in a sequence of 3 tosses
  -

<table>
<thead>
<tr>
<th>$s$</th>
<th>hhh</th>
<th>hht</th>
<th>hth</th>
<th>htt</th>
<th>thh</th>
<th>tht</th>
<th>tth</th>
<th>ttt</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X(s)$</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

- $X$ is a random variable taking on values in the set

$$S_X = \{0,1,2,3\}$$
Definitions

- Cumulative Distribution Function (cdf)
  - The cdf of a random variable $X$ is defined as the probability of the event $\{X \leq x\}$

$$F_X(x) = P(X \leq x) \text{ for } -\infty < x < +\infty$$

$$F_X(x) = \text{prob. of event } \{s: X(s) \leq x\}$$

$$F_X(x) = \text{is a probability, i.e. } 0 \leq F_X(x) \leq 1$$

$$F_X(x) \text{ is monotonically non-decreasing, i.e. if } x_1 \leq x_2 \text{ then } F_X(x_1) \leq F_X(x_2)$$

$$\lim_{x \to \infty} F_X(x) = 1 \quad \lim_{x \to -\infty} F_X(x) = 0$$
Definitions

- Probability Density Function (pdf)
  - The pdf of a random variable is the derivation of $F_X(x)$
    \[
    f_X(x) = \frac{dF_X(x)}{dx}
    \]
  - Since $F_X(x)$ is a non-decreasing function,
    \[
    f_X(x) \geq 0
    \]
  - The pdf represents the “density” of probability at point $x$
Definitions

- **cdf vs. pdf**
  - Adult body weight (males and females combined)
  - Arithmetic mean 71.7kg, std = 15.9kg
  - Source: Finley et.al. 1994
**Definitions**

- **Expectation of a random variable**
  - in order to completely describe the behavior of a random variable, an entire function, namely the cdf or pdf, must be given
  - however, sometime we are just interested in parameters that summarize information

\[ E(X) = \int_{-\infty}^{\infty} xf_X(x) \, dx \]

i.e. mean time to failure = expected lifetime of the system
PRA & PSA

- Fault Tree Analysis
  - most widely used method in system reliability analysis
  - this is a top down approach
  - typical components are AND and OR
example: (source Relax Software Corp.)
**PRA & PSA**

- **Event Tree Analysis**
  - visual representation of all events which can occur in a system
  - example: (source Relax Software Corp.)

![Event Tree Analysis Diagram](image)
Reliability of Series System

- Any one component failure causes system failure
- Reliability Block Diagram (RBD)

\[
R(t)_{\text{series}} = \prod_{i=1}^{n} R_i(t)
\]

\[
= \prod_{i=1}^{n} e^{-\lambda_i t}
\]

\[
= e^{-(\sum_{i=1}^{n} \lambda_i)t}
\]
Reliability of Series System

Thus

\[ \lambda_{\text{series}} = \sum_{i=1}^{n} \lambda_i \]

Mean time to failure of series system:

\[ MTTF_{\text{series}} = \frac{1}{\sum_{i=1}^{n} \lambda_i} \]

Thus the MTTF of the series system is much smaller than the MTTF of its components.

If \( X_i \equiv \text{lifetime of component } i \) then

\[ 0 \leq E[X] \leq \min \{E[X_i]\} \]
Reliability of Parallel System

- All components must fail to cause system failure
- Reliability Block Diagram (RBD)

  1
  \[ \begin{array}{c}
  2 \\
  \vdots \\
  n \\
  \end{array} \]

  - assume mutual independence
$X$ is lifetime of the system

$$X = \max \{ X_1, X_2, \ldots, X_n \} \quad \text{n components}$$

$$R(t)_{\text{parallel}} = 1 - \prod_{i=1}^{n} Q_i(t)$$

$$= 1 - \prod_{i=1}^{n} (1 - R_i(t))$$

$$\geq 1 - (1 - R_i(t))$$

Assuming all components have exponential distribution with parameter $\lambda$

$$R(t) = 1 - (1 - e^{-\lambda t})^n$$
\[E(X) = \int_0^\infty [1 - (1 - e^{-\lambda t})^n] dt\]

\[= \ldots\]

\[= \frac{1}{\lambda} \sum_{i=1}^n \frac{1}{i}\]

\[\approx \frac{\ln(n)}{\lambda}\]

from previous page

\[Q(t)_{\text{parallel}} = \prod_{i=1}^n Q_i(t)\]  \hspace{1cm} \text{Product law of unreliability}
**Stand-by Redundancy**

- When primary component fails, standby component is started up.
- Stand-by spares are cold spares => unpowered
- Switching equipment assumed failure free

Let $X_i$ denote the lifetime of the $i$-th component from the time it is put into operation until its failure.

System lifetime:

$$X_{sys} = \sum_{i=1}^{n} X_i$$
**Stand-by Redundancy**

- **MTTF**

\[ E(X) = \frac{n}{\lambda} \]

- gain is linear as a function of the number of components, unlike the case of parallel redundancy
- added complexity of detection and switching mechanism
**M-of-N System**

Starting with N components, we need any M components operable for the system to be operable.

Example: TMR

\[
R_{\text{TMR}}(t) = R_1(t)R_2(t)R_3(t) + R_1(t)R_2(t)(1 - R_3(t)) + R_1(t)(1 - R_2(t))R_3(t) + (1 - R_1(t))R_2(t)R_3(t)
\]

Where \( R_i(t) \) is the reliability of the i-th component

If \( R_i(t) = R_1(t) = R_2(t) = R_3(t) = R(t) \) then

\[
R_{\text{TMR}}(t) = R^3(t) + 3R^2(t)(1 - R(t)) = R^3(t) + 3R^2(t) - 3R^3(t) = 3R^2(t) - 2R^3(t)
\]
M-of-N System

The probability that exactly $j$ components are not operating is

$$\binom{N}{j} Q^j(t) R^{N-j}(t)$$

with

$$\binom{N}{j} = \frac{N!}{j!(N-j)!}$$

then

$$R_{MofN}(t) = \sum_{i=0}^{N-M} \binom{N}{i} Q^i(t) R^{N-i}(t)$$
Reliability Block Diagram

- **Series Parallel Graph**
  - a graph that is recursively composed of series and parallel structures.
  - therefore it can be “collapsed” by applying series and/or parallel reduction
  - Let $C_i$ denote the condition that component $i$ is operable
    » $1 = \text{up, } 0 = \text{down}$
  - Let $S$ denote the condition that the system is operable
    » $1 = \text{up, } 0 = \text{down}$
  - $S$ is a logic function of $C$’s
Reliability Block Diagram

- Example:

\[ S = (C_1 + C_2 + C_3)(C_4 C_5)(C_6 + C_7 C_8) \]

+ => parallel (1 of N)

. => series (N of N)
Example 2-of-3 system

\[ S = (C_1 C_2 + C_1 C_3 + C_2 C_3) \]

may abbreviate

\[ S = \frac{2}{3} (C_1 C_2 C_3) \]

draw as parallel

2-of-3
Fault Trees

- Fault Trees
  - dual of Reliability Block Diagram
  - logic failure diagram
  - think in terms of logic where
    » 0 = operating, 1 = failed
- AND Gate
  - all inputs must fail for the gate to fail
- OR Gate
  - any input failure causes the gate to fail
- k-of-n Gate
  - k or more input failures cause gate to fail