Reliability, Redundancy, and Resiliency

- Review of probability theory
- Component reliability
- Confidence
- Redundancy
- Reliability diagrams
- Intercorrelated Failures
- System resiliency
- Resiliency in fixed fleets
Review of Probability

- Probability that $A$ occurs
  \[ 0 \leq P(A) \leq 1 \]
- Probability that $A$ does not occur
  \[ P(\overline{A}) \]
- Sum of all probable outcomes
  \[ P(A) + P(\overline{A}) = 1 \]
Review of Probability

- Probability of both A and B occurring
  \[ P(A) \cap P(B) = P(A)P(B) \]

- Probability of either A or B occurring
  \[ P(A) \cup P(B) = 1 - P(\overline{A})P(\overline{B}) \]
  \[ = 1 - [1 - P(A)][1 - P(B)] \]
  \[ = P(A) + P(B) - P(A)P(B) \]
Utility Theory

- Probability of an outcome does not determine utility of the outcome
- Use probability and utility to determine expected value of outcome

\[ EV = P(A)U(A) + P(\bar{A})U(\bar{A}) \]
Utility Example

- Maryland State Lottery - pick six numbers out of 49 (any order)

\[ P(\text{win}) = \frac{49!}{6!43!} = 1/13,983,816 \]

- Assume $10,000,000 jackpot

\[ EV = (7.151 \times 10^{-8})(10^7) + (1)(-1) = -$0.39 \]
Component Reliability

<table>
<thead>
<tr>
<th>Failure Rate $\lambda$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burn-in Failures</td>
</tr>
<tr>
<td>Operating Failures</td>
</tr>
<tr>
<td>End-of-life Failures</td>
</tr>
</tbody>
</table>

Time
Reliability Analysis

- Failure rate is defined as fraction of currently operating units failing per unit time

\[ \lambda(t) = -\frac{1}{R(t)} \frac{d}{dt} R(t) \]

- The trend of operating units with time is then

\[ \int_{0}^{t} \lambda(\tau) \, d\tau = -\int_{1}^{R(t)} \frac{dR(\tau)}{R(\tau)} \]
Reliability Analysis (continued)

• Evaluation of the definite integrals gives

\[ \int_0^t \lambda(\tau) \, d\tau = -\ln[R(t)] \]

• Assuming that \( \lambda \) is constant over the operating lifetime,

\[ R(t) = \exp\left[-\int_0^t \lambda(\tau) \, d\tau\right] = e^{-\lambda t} \]

• At \( t=1/\lambda \), 1/e of the original units are still operating (defined as mean time between failures)
Reliability Analysis (continued)

• Frequently assess component reliability based on reciprocal of failure rate $\lambda$:

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

where MTBF = mean time between failures

• For a mission duration of N hours, estimate of component reliability becomes

$$R(\text{mission}) = e^{-\frac{N}{MTBF}}$$
Verifying a Reliability Estimate

• Given a unit reliability of $R$, what is the probability $P$ of testing it 20 times without a failure?

• What is the probability $Q$ that you will see one or more failures?

- $R = 0.99$ - $P = 0.8179$ - $Q = 0.1821$
- $R = 0.95$ - $P = 0.3584$ - $Q = 0.6416$
- $R = 0.90$ - $P = 0.1216$ - $Q = 0.8784$
Confidence

• The confidence $C$ in a test result is equal to the probability that you should have seen worse results than you did

$$P(\text{observed and better outcomes}) + C = 1$$
Example of Confidence

• 100 vehicle flights with 1 failure
• Assume a reliability value of $R$

\[
R^{100} + 100R^{99}(1 - R) + C = 1
\]

• Trade off reliability with confidence values
Definition of Redundancy

- Probability of k out of n units working =
  (number of permutations of k out of n) \times
  P(k units work) \times P(n-k units fail)

\[ P\left(\begin{pmatrix} k \\ n \end{pmatrix}\right) = \frac{n!}{k!(n-k)!} P^k (1 - P)^{n-k} \]
Redundancy Example

3 parallel computers, each has reliability of 95%:

- Probability all three work
  \[ P(3) = P^3 = (0.95)^3 = 0.8574 \]

- Probability exactly two work
  \[ P(2) = 3P^2(1 - P) = 3(0.95)^2(0.05) = 0.1354 \]

- Probability exactly one works
  \[ P(1) = 3P(1 - P)^2 = 3(0.95)(0.05)^2 = 0.0071 \]

- Probability that none work
  \[ P(0) = (1 - P)^3 = (0.05)^3 = 0.0001 \]
Redundancy Example

3 parallel computers, each has reliability of 95%:

- Probability all three work
  \[ P(3) = 0.8574 \]

- Probability at least two work
  \[ P(3) + P(2) = 0.8574 + 0.1354 = 0.9928 \]

- Probability at least one works
  \[ P(3) + P(2) + P(1) = 0.9928 + 0.0071 = 0.9999 \]

- Probability that none work
  \[ P(0) = (1 - P)^3 = (0.05)^3 = 0.0001 \]
Reliability Diagrams

- Example of Apollo Lunar Module ascent engine
- Three valves in each of oxidizer and fuel lines
- One in each set of three must work
- \( R_v = 0.9 \rightarrow R_{\text{system}} = 0.998 \)

\[
R_{\text{system}} = \left[ 1 - (1 - R_v)^3 \right]^2
\]
Reliability Diagrams (how not to...) 

\[ R_{\text{system}} = \left[ 1 - (1 - R_v)^3 \right]^2 \]

\( R_v = 0.9 \rightarrow R_{\text{system}} = 0.998 \)

\[ R_{\text{system}} = \left[ 1 - (1 - R_v^2)^3 \right] \]

\( R_v = 0.9 \rightarrow R_{\text{system}} = 0.993 \)
Intercorrelated Failures

- Some failures in redundant systems are common to all units
  - Software failures
  - “Daisy-chain” failures
  - Design defects
- Following a failure, there is a probability $f$ that the failure causes a total system failure
Intercorrelated Failure Example

3 parallel computers, each has reliability of 95%, and a 30% intercorrelated failure rate:

- Probability all three work
  \[ P(3) = P^3 = (0.95)^3 = 0.8574 \]

- Probability exactly two work (one failure)
  \[ P(2) = 3P^2(1-P) = 3(0.95)^2(0.05) = 0.1354 \]
  - Probability the failure is benign (system works)
    \[ P(2_{\text{safely}}) = 0.7(0.1354) = 0.0948 \]
  - Probability of intercorrelated failure (system dies)
    \[ P(2_{\text{system failure}}) = 0.3(0.1354) = 0.0406 \]
Intercorrelated Failure Example

(continued from previous slide)

• Probability exactly one works (2 failures)

\[ P(1) = 3P(1 - P)^2 = 3(.95)(.05)^2 = .0071 \]

  - Probability that both failures are benign

\[ P(1_{safely}) = .7^2(.0071) = .0035 \]

  - Probability that a failure is intercorrelated

\[ P(1_{system\ failure}) = (1 - .7^2)(.0071) = .0036 \]
Redundancy Example with Intercorrelation

3 parallel computers, each has reliability of 95%, and a 30% intercorrelated failure rate:

- Probability all three work
  \[ P(3) = 0.8574 \]
- Probability at least two work
  \[ = 0.8574 + 0.0948 = 0.9522 \] (was 0.9928)
- Probability at least one works
  \[ = 0.9522 + 0.0035 = 0.9557 \] (was 0.9999)
System Reliability with 30% Intercorrelation

- P(1)
- P(2)
- P(3)
- P(4)
- P(2)intercorrelated
- P(3)intercorrelated
- P(4)intercorrelated
Concept of System Resiliency

- Initial flight schedule

- Hiatus period following a failure

- Backlog of payloads not flown in hiatus

- Surge to fly off backlog

- Resilient if backlog is cleared before next failure occurs (on average)
Resiliency Variables

- $r$ - nominal flight rate, flts/yr
- $d$ - down time following failure (yrs)
- $k$ - fraction of flights in backlog retained
- $S$ - surge flight rate/nominal flight rate
- $m$ - average/expected flights between failures
- $rd$ - number of missed flights
- $krd$ - number of flights in backlog
- $(S-1)r$ - backlog flight rate
Definition of Resiliency

\[ \frac{Srkd}{S-1} \leq m \]

Example for Delta launch vehicle

- \( r = 12 \) flts/yr
- \( d = 0.5 \) yrs
- \( k = 0.8 \)
- \( S = 1.5 \)
- \( m = 30 \)

\[ \frac{Srkd}{(S-1)} = 14.4 < 30 \text{ - system is resilient!} \]
Shuttle Resiliency

\[ r = 9 \text{ flts/yr} \]
\[ d = 2.5 \text{ yrs} \]
\[ k = 0.8 \]
\[ S = 0.67 \text{ (6 flts/yr)} \]
\[ m = 25 \]

System has negative surge capacity due to reduction in fleet size - cannot ever recover from hiatus without more extreme measures.
Modified Resiliency

\( k' \) - retention rate of all future payloads
(\( k' \leq S \) for \( S < 1 \))

• New governing equation for resiliency:

\[
\frac{S r k' d}{S - k'} \leq m
\]

• Implication for shuttle case:
\( k < 0.417 \) to achieve modified resiliency