Reliability Analysis

- **Permanent faults**
  - Reliability decay
- **Temporary faults**
  - Often Steady state characterization
- **Design faults**
  - Reliability growth during testing & debugging

At space shuttle Challenger
Launch, 1986

Basic Reliability Measures

- **Reliability**: durational (default)
  \[ R(t)=P\{\text{correct operation in duration} \ (0,t)\} \]
- **Availability**: instantaneous
  \[ A(t)=P\{\text{correct operation at instant} \ t)\} \]
  If steady-state value, not a function of time.
- **Transaction Reliability**: single transaction
  \[ R_{t}=P\{\text{a transaction is performed correctly}\} \]
- For temporary faults, Availability or Transaction Reliability may be suitable measures.
Mean Time to Failure (MTTF)

- $T$: r.v. time to failure

$$MTTF = E(T) = \int_0^\infty t f(t) dt$$

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

$$= \left[-t R(t)\right]_0^\infty + \int_0^\infty R(t) dt$$

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

Note:

$$R(t) = 1 - P\{\text{failure in (0}, t)\}$$

$$= 1 - P\{0 \leq T \leq t\}$$

$$= 1 - F(t)$$

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

Note:

$$xe^{-x} \to 0 \text{ as } x \to 0$$

Failures with Repair

- MTTR for repairable systems is similarly defined.

- $MTBF = MTTF + MTTR$
  - MTBF, MTTR same when failure is permanent or $MTTR = 0$
  - Steady state availability = $MTTF / (MTTF+MTTR)$
Mission Time (High-Reliability Systems)

- Reliability throughout the mission must remain above $R_{th}$.
- Mission time $T_M$: duration in which $R(t) \geq R_{th}$.
- $R_{th}$ may be chosen to be perhaps 0.95.

![Graph showing reliability over time with mission time $T_M$.]

Basic Cases: Single Unit with Permanent Failure

- Failure rate: probability of failure/unit time
- Assumption: constant failure-rate

\[
\frac{dp_0(t)}{dt} = -\lambda \ p_0(t) \\
\]

- Burn-in: surviving units stronger
- Wearout: affect of aging

![Diagram showing failure rate over time with burn-in and wearout phases.]

\[
p_0(0) = 1
\]
Single Unit with Permanent Failure (2)

\[ \frac{dp_0(t)}{dt} = -\lambda p_0(t) \]
\[ p_0(0) = 1 \]

Solution: \[ p_0(t) = e^{-\lambda t} \]
\[ R(t) = e^{-\lambda t} \]

"Exponential reliability"

At \[ t = \frac{1}{\lambda}, R(t) = e^{-1} = 0.368 \]

---

Single Unit: Permanent Failure (3)

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

\[ MTTF = \int_0^\infty R(t)dt = \int_0^\infty e^{-\lambda t} dt \]
\[ = \left[ -\frac{e^{-\lambda t}}{\lambda} \right]_0^\infty \]
\[ = \frac{1}{\lambda} \]

- Ex 1: a unit has MTTF = 30,000 hrs. Find failure rate.
  \[ \lambda = 1/30,000 = 3.3 \times 10^{-5} / \text{hr} \]
- Ex 2: Compute mission time \( T_M \) if \( R_{th} = 0.95 \).
  \[ e^{\lambda T_M} = 0.95 \quad T_M = -\ln(0.95) / \lambda \]
  \[ = 0.05 / \lambda \]
- Ex 3: Assume \( \lambda = 3.33 \times 10^{-5} \) find \( T_M \).
  Ans: \( T_M = 1501.5 \) hrs
  (compare with MTTF = 30,000)
Generalization: Failure Rate

- \( z(t) = \alpha \lambda (\lambda t)^{\alpha-1} \)
  - leads to Weibull Distribution
  - \( f_T(t) = \alpha \lambda (\lambda t)^{\alpha-1} e^{-(\lambda t)^\alpha} \)
- \( \alpha \): shape parameter, 1 for constant rate
- \( \lambda \): scale parameter
- Often used to get a better fit, if needed, for rising or falling failure rates.

See links at: http://sd.znet.com/~sdsmpe/distr.htm

Single Unit: Temporary Failures(1)

- Temporary: intermittent, transient, permanent with repair

\[
\frac{dp_0(t)}{dt} = -\lambda p_0(t) + \mu p_1(t)
\]
\[
\frac{dp_1(t)}{dt} = +\lambda p_0(t) - \mu p_1(t)
\]
- can be solved by laplace transform etc.

\[
p_0(t) = p_0(0)e^{-(\lambda + \mu)t} + \frac{\mu}{\lambda + \mu}(1 - e^{-(\lambda + \mu)t})
\]
- Similarly

\[
p_1(t) =
\]
Single Unit: Temporary Failures (2)

- \( p_0(t) = p_0(0)e^{-(\lambda + \mu)t} + \frac{\mu}{\lambda + \mu}(1 - e^{-(\lambda + \mu)t}) \)
- Availability \( A(t) = p_0(t) \)
- steady-state probabilities exist

\[
t \to \infty, \quad p_0(t) = \frac{\mu}{\lambda + \mu}, \quad p_1(t) = \frac{\lambda}{\lambda + \mu}
\]

- Steady-state availability is \( \frac{\mu}{\lambda + \mu} \)

Single Unit: Temporary Failures (3)

- Reliability (durational)
  \[ R(t) = P\{\text{no failures in } (0, t)\} = P\{\text{in Good 0 at } t\} = e^{-\lambda t} \]
  same as permanent failure

- Thus MTTF = \( \frac{1}{\lambda} \)
- Mission time: also same
Combinatorial Reliability

- Conceptual modeling, applicable to R(t), A(t), R_i(t).
- **Series configuration**: all units are essential.
  - **Assumption**: statistically independent failures

\[
R_s = P\{U_1 \text{ good} \cap U_2 \text{ good} \cap U_3 \text{ good}\} = P\{U_1 \text{ g}\}P\{U_2 \text{ g}\}P\{U_3 \text{ g}\} = R_1R_2R_3
\]

In general \( R_s = \prod_{i=1}^{n} R_i \)

If \( R_i(t) = e^{-\lambda t} \)
then \( R_s(t) = e^{-(\lambda_1+\lambda_2+\cdots+\lambda_n)t} \)

i.e. failure rates add: \( \lambda_s = \lambda_1 + \lambda_2 + \cdots + \lambda_n \)

---

“A chain is as strong as it’s weakest link”

- Assume \( R_1 = R_2 = R_3 = 0.95, R_4 = 0.75 \)
- \( R_5 = 0.643 \)
- A 10-unit system vs a single system. Each of the 10 units are identical.
Combinatorial: Parallel

- **Parallel configuration:** at least one unit must be good. Represents an *ideal* redundant system.

\[
R_s = 1 - P\{\text{all units bad}\}
\]
\[
= 1 - P\{U_1 \text{bad} \cap U_2 \text{bad} \cap U_3 \text{bad}\}
\]
\[
= 1 - P\{U_1 \text{b.} \}P\{U_2 \text{b.} \}P\{U_3 \text{b.} \}
\]
\[
= 1 - (1 - R_1)(1 - R_2)(1 - R_3)
\]

In general \(R_s = 1 - \prod_{i=1}^{n} (1 - R_i)\)

\[i.e. \quad R_s = \prod_{i=1}^{n} R_i\]

Parallel Configuration: Example

Problem: Need system reliability \(R_s = 1 - \varepsilon\)

How many parallel units are needed
if \(R_1 = R_2 = \cdots = R_m, R_m < R_s\)?

Solution: \(1 - R_s = (1 - R_m)^x\)

\[
\varepsilon = (1 - R_m)^x
\]

\[
x = \frac{\ln \varepsilon}{\ln(1 - R_m)}
\]

Assume \(R_s = 0.9999 (\varepsilon = 0.0001)\),

\(R_m = 0.9\)

gives \(x = 4\).
“Coverage”

\[ R_s = P\{U_1 \text{ good}\} + P\{U_2 \text{ has taken over } |U_1 \text{ failed}\} P\{U_1 \text{ failed}\} = R_1 + R_2 C (1 - R_1) \]

where \( C = P\{\text{failure detected and successful switchover}\} \)

- Failure detection: requires concurrent detection.
  Need redundancy.
- Switchover:
  - good state loaded in \( U_2 \).
  - Process restarted

Imperfect Coverage

\[ R_s = R_1 + R_2 C (1 - R_1) \]

- Assuming \( R_1 = R_2 = 0.7 \)
- In general \( R_s = R_m \sum_{i=0}^{n-1} C^i (1 - R_m)^i \)

Graph: Two parallel modules

Coverage vs. Reliability

0.5 0.6 0.7 0.8 0.9 1

0 0.25 0.5 0.75 1

Reliability
**k-out-of-n Systems**

- n identical modules with statistical independent failures.
- Operational if k of the modules are good.

\[
R_{k/n} = \sum_{i=k}^{n} \binom{n}{i} p^i (1-p)^{n-i}
\]

**Triple Modular Redundancy**

- Popular high-reliability scheme: 2-out-of-3
- Majority voter
- Various implementations

\[
R_{TMR} = \sum_{i=2}^{3} \binom{3}{i} R^i (1-R)^{3-i}
\]

\[
= 3 R^2 (1-R) + R^3
\]

\[
= 3 R^2 - 2 R^3
\]
TMR: Permanent Failures

Let \( R = e^{-\lambda t} \)
\( R_{TMR}(t) = 3e^{2\lambda t} - 2e^{3\lambda t} \)

\[ MTTF = \int_{0}^{\infty} R_{TMR}(t) dt \]
\[ = \int_{0}^{\infty} (3e^{2\lambda t} - 2e^{3\lambda t}) dt \]
\[ = \frac{5}{6} \lambda \] (single module MTTF: \( \frac{1}{\lambda} \))

TMR – Single crossover point
Solving \( 3R^2 - 2R^3 = R \)
we get \( R_{cross} = 0.5 \).
TMR worse after \( R < 0.5 \!)

TMR

- Mission time
\[ R_{Th} = 3e^{-2\lambda t_m} - 2e^{-3\lambda t_m} \]
\( t_m \) = numerical solution

- \( Ex: \lambda = 1/\text{year}, R_{Th} = 0.95 \)

\[
\begin{array}{|c|c|c|}
\hline
\text{MTTF} & t_m & \\
\hline
\text{single} & 1 \text{yr} & 0.05 \\
\text{TMR} & 0.83 & 0.145 \\
\hline
\end{array}
\]

- Temporary faults: steady state
\[ A_{TMR} = 3A^2 - 2A^3, A = \frac{\mu}{\lambda + \mu} \]

- \( Ex: \frac{\lambda}{\mu} = 0.01 \Rightarrow A = 0.9901 \)
\[ \Rightarrow \overline{A} = 0.01 \]
\[ A_{TMR} = 0.9997 \Rightarrow \overline{A}_{TMR} = 0.0003 \]
TMR+Spares

- TMR core, n-3 spares (assume same failure rate)
- A: System failure when all but one modules have failed.
  \[ R_s = R_{sw} [1-nR(1-R)^{n-1}(1-R)^n] \]
- Let \( R_{sw} = (R^a)^n \), \( a: \) relative complexity \(<1\)
  \[ R_s = R^n [1-nR(1-R)^{n-1}(1-R)^n] \]
- Ex: \( R=0.9, a=10^{-2} \)
  We can see that \( n_{max}=4 \)

Can we do better?

TMR+Spare (2)

B: One of the last two fails, remove one arbitrarily.
  \[ R_s = R^n [1-0.5nR(1-R)^{n-1}(1-R)^n] \]

- Diagram showing TMR core, switching circuit, and disagreement detector.

- Graph showing reliability over modules for both schemes A and B.
Redundancy: Generalized Reliability Computation

- \( R_s = P\{\text{correct output}\} = P\{B_1 G \cap B_2 G \cap B_3 G\} + P\{B_3 G\} \sum_{i=1}^{n} P\{\text{failure mode } i\} \}
- P\{\text{failure mode } i\} \} = R_1 R_2 R_3 + R_3 \sum_{i=0}^{n} P_i C_i
- If \( R_3 = 1\) and a single failure mode dominates
  \( R_s = R_1 R_2 + P_i C \)

Generalized Reliability: Ex: Memory

- Approximation \( R_s = R_s R_3 + P_i C \)
- Ex: Memory system, total \( m \) bits/word, \( R_s \): reliability of a single word. One bit error correction capability. Assuming perfect error detection/correction
  \( R_{\text{word}} = R_b^m + [m(1 - R_b)R_b^{m-1}] \)
- Ex: One word is 8 bits data plus 4 check bits (1-bit correcting Hamming code). Assume \( R_b \) is \( 10^{-5} \) unit time,
  with redundancy: \( R_{\text{word}} = 1 - 6.6 \times 10^{-9} \)
  without redundancy: \( R_{\text{word}} = 1 - 7.9 \times 10^{-5} \)
- Note: actual soft error rate these days is very small.