Reliable Computing I

Lecture 5: Reliability Evaluation

Instructor: Mehdi Tahoori

Today’s Lecture

- Reliability evaluation
  - Permanent and temporary failures
- Combinatorial modeling
  - Series
  - Parallel
  - Series-parallel
  - Non-series-parallel
  - k-out-of-n
  - TMR vs. Simplex
  - Effects of voter, coverage
Evaluation Criteria

- A method of evaluation is required in order to compare the redundancy techniques and make subsequent design tradeoffs
- Modeling techniques are very vital means for obtaining reasonable predictions for system reliability and availability
  - Combinatorial: series/parallel, K-of-N, nonseries/nonparallel
  - Markov: time invariant, discrete time, continuous time, hybrid
  - Queuing
- Using these techniques probabilistic models of systems can be created and used to evaluate system reliability and/or availability

Basic Reliability Measures

- Reliability: durational (default)
  - \( R(t) = P\{\text{correct operation in duration (0,}t)\} \)
- Availability: instantaneous
  - \( A(t) = P\{\text{correct operation at instant } t\} \)
  - Applied in presence of temporary failures
  - A steady-state value is the expected value over a range of time.
- Transaction Reliability: single transaction
  - \( R_t = P\{\text{a transaction is performed correctly}\} \)
Mean time to …

- **Mean Time to Failure (MTTF):**
  - expected time the unit will work without a failure.

- **Mean time between failures (MTBF):**
  - expected time between two successive failures.
    - Applicable when faults are temporary.
    - The time between two successive failures includes repair time and then the time to next failure.

- **Mean time to repair (MTTR):**
  - expected time during which the unit is non-operational.

 Failures with Repair

- Time between failures: time to repair + time to next failure

- $MTBF = MTTF + MTTR$
- $MTBF$, $MTTF$ are same same when $MTTR \approx 0$
- Steady state availability = $MTTF / (MTTF+MTTR)$
Mission Time (High-Reliability Systems)

- Reliability throughout the mission must remain above a threshold reliability $R_{\text{th}}$.
- Mission time $T_M$: defined as the duration in which $R(t) \geq R_{\text{th}}$.
- $R_{\text{th}}$ may be chosen to be perhaps 0.95.
- Mission time is a strict measure, used only for very high reliability missions.

Two Basic cases

- We next consider two very important basic cases that serve as the basis for time-dependent analysis.

1. Single unit subject to permanent failure
   - We will assume a constant failure rate to evaluate reliability and MTTF.

2. Single unit with temporary failures
   - System has two states Good and Bad, and transitions among them are defined by transition rates.
   - Both of these are example of Markov processes.
Single Unit with Permanent Failure

- Assumption: constant failure-rate $\lambda$
- Reliability $R(t) = e^{-\lambda t}$
- $MTTF = \int_0^\infty R(t) dt = \int_0^\infty e^{-\lambda t} dt = \frac{1}{\lambda}$

  - Ex 1: a unit has MTTF $30,000$ hrs. Find failure rate.
    $\lambda = \frac{30,000}{3.3 \times 10^{-5}}$ hr
  - Ex 2: Compute mission time $T_M$ if $R_m = 0.95$.
    $e^{-\lambda T_M} = 0.95 \quad T_M = \frac{\ln(0.95)}{-\lambda} = 0.051/\lambda$
  - Ex 3: Assume $\lambda = 3.33 \times 10^{-5}$, and $R_m = 0.95$ find $T_M$.
    Ans: $T_M = 1538.8$ hrs
    (compare with MTTF = 30,000)

- Availability $A(t) = \frac{\lambda t}{\lambda + \mu}$
- Steady-state availability ($t \to \infty$) $A(t) = \frac{\mu}{\lambda + \mu}$
- Reliability: $R(t) = P\{\text{no failure in (0,t)}\} = e^{-\lambda t}$
- $MTTF = \frac{1}{\lambda}$
  - Same as permanent failure

Single Unit: Temporary Failures

- Temporary: intermittent, transient, permanent with repair

- $p_0(t) = p_0(0)e^{-(\lambda+\mu)t} + \frac{\mu}{\lambda+\mu}(1 - e^{-(\lambda+\mu)t})$
- $p_1(t) = 1 - p_0(t)$
- Availability $A(t) = p_0(t)$
- Steady-state availability ($t \to \infty$) $A(t) = \frac{\mu}{\lambda+\mu}$
- Reliability: $R(t) = P\{\text{no failure in (0,t)}\} = e^{-\lambda t}$
- $MTTF = \frac{1}{\lambda}$
  - Same as permanent failure
Combinatorial Modeling

- System is divided into non-overlapping modules
- Each module is assigned either a probability of working, \( P_i \), or a probability as function of time, \( R_i(t) \)
- The goal is to derive the probability, \( P_{sys} \), or function \( R_{sys}(t) \) of correct system operation

Assumptions:
- module failures are independent
- once a module has failed, it is always assumed to yield incorrect results
- system is considered failed if it does not satisfy minimal set of functioning modules
- once system enters a failed state, other failures cannot return system to functional state
- Models typically enumerate all the states of the system that meet or exceed the requirements of correctly functioning system

Combinatorial Reliability

- Objective is: Given a
  - systems structure in terms of its units
  - reliability attributes of the units
  - some simplifying assumptions
- We need to evaluate the overall reliability measure.
- There are two extreme cases we will examine first:
  - Series configuration
  - Parallel configuration
  - Other cases involve combinations and other configurations.
- Note that conceptual modeling is applicable to \( R(t) \), \( A(t) \), \( R(t) \). A system is either good or bad.
Series configuration

- Assume system has $n$ components, e.g. CPU, memory, disk, terminal
- All components should survive for the system to operate correctly

$$R_s = P(U_1 \text{ good} \cap U_2 \text{ good} \cap U_3 \text{ good})$$
$$= P(U_1 \text{ g}) P(U_2 \text{ g}) P(U_3 \text{ g})$$
$$= R_1 R_2 R_3$$

- Reliability of the system
$$R_{\text{series}}(t) = \prod_{i=1}^{n} R_i(t)$$ where $R_i(t)$ is the reliability of module $i$

Series configuration

- For exponential failure rate of each component
  If $R_i(t) = e^{-\lambda_i t}$
  then $R_s(t) = \prod e^{-\lambda_i t} = e^{-(\lambda_1 + \lambda_2 + \cdots + \lambda_n) t}$

$$R_{\text{series}}(t) = e^{-\sum_{i=1}^{n} \lambda_i t} = e^{-\lambda_{\text{system}} t}$$

Where $\lambda_{\text{system}} = \sum_{i=1}^{n} \lambda_i$ corresponds to the failure rate of the system

- System failure rate is the sum of individual failure rates:
  $$\lambda_s = \lambda_1 + \lambda_2 + \cdots + \lambda_n$$

- Mean time to failure:
  $$MTTF_{\text{series}} = \frac{1}{\sum_{i=1}^{n} \lambda_i}$$
“A chain is as strong as its weakest link”?

- Let us see for a 4-unit series system
  - Assume $R_1 = R_2 = R_3 = 0.95$, $R_4 = 0.75$
  - $R_S = 0.643$
- Thus a chain is slightly weaker than its weakest link!
- The plot gives reliability of a 10-unit system vs a single system. Each of the 10 units are identical.
- More units, less reliability

If $X_i$ = lifetime of component $i$ then

$$0 \leq E[X] \leq \min \{E[X_i]\}$$

Parallel Systems

- Assume system with spares
- As soon as fault occurs a faulty component is replaced by a spare
- Only one component needs to survive for the system to operate correctly
- Prob. of module $i$ to survive = $R_i$
- Prob. of module $i$ not to survive = $(1 - R_i)$
- Prob. of no modules to survive =
  $$ (1 - R_1)(1 - R_2) \ldots (1 - R_n) $$
- Prob [at least one module survives] =
  $$ 1 - \text{Prob [none module survives]} $$
- Reliability of the parallel system

$$ R_{\text{parallel}}(t) = 1.0 - \prod_{i=1}^{n} (1.0 - R_i(t)) $$

(c) 2013, Mehdi Tahoori
Parallel Systems

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

\[ = \ldots \]

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

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

Parallel Configuration: Example

- Problem: Need system reliability \( R_s = 1 - \epsilon \)
- How many parallel units are needed
  - If \( R_1 = R_2 = \ldots = R_m, \ R_m < R_s \)
- Solution: \( 1 - R_s = (1 - R_m)^x \)
  \[ \epsilon = (1 - R_m)^x \]
  \[ x = \frac{\ln \epsilon}{\ln(1 - R_m)} \]

Assume \( R_s = 0.9999 (\epsilon = 0.0001), \ R_m = 0.9 \)
gives \( x = 4. \)
Series-Parallel Systems

- Consider combinations of series and parallel systems
- Example, two CPUs connected to two memories in different ways

\[ R_{sys} = 1 - (1-R_a R_b) (1-R_c R_d) \]
\[ R_{sys} = (1-(1-R_a)(1-R_c))(1-(1-R_b)(1-R_d)) \]

Non-Series-Parallel-Systems

- Often a “success” diagram is used to represent the operational modes of the system

- Reliability of the system can be derived by expanding around a single module m

\[ R_{sys} = R_m \ P(\text{system works} \mid m \ \text{works}) + (1-R_m) \ P(\text{system works} \mid m \ \text{fails}) \]

where the notation \( P(s \mid m) \) denotes the conditional probability “s given m has occurred”
Non-Series-Parallel-Systems

For complex success diagrams, an upper-limit approximation on $R_{sys}$ can be used.

An upper bound on system reliability is:

$$R_{sys} \leq 1 - \prod (1 - R_{path_i})$$

$R_{path}$ is the serial reliability of path $i$.

- The above equation is an upper bound because the paths are not independent.
- That is, the failure of a single module affects more than one path.
Non-Series-Parallel-Systems

Example

Reliability block diagram (RBD) of a system

\[ R_{33s} \leq 1 - (1 - R_A R_B R_C R_D)(1 - R_A R_E R_D)(1 - R_E R_C R_D) \]
\[ R_{33s} \leq 2R_m^2 + R_m^4 - R_m^6 - 2R_m^7 + R_m^8 \]

k-out-of-n Systems

Assumption:
- we have \( n \) identical modules with statistically independent failures.
- k-out-of-n system is operational if
  - k of the \( n \) modules are good.
- System reliability then is
  \[ R_{k/n} = \sum_{i=k}^{n} \binom{n}{i} p^i (1-p)^{n-i} \]
  - Where \( p \) is the probability that one unit is good
  - \( R_{k/n} \) is the summations of the probabilities of all good combinations
  - \( \binom{n}{i} = \frac{n!}{i!(n-i)!} \): choose i good systems out of n
Triple Modular Redundancy

2-out-of-3 system

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

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

\[ = 3R^2 - 2R^3 \]

- Where \( R \) is the reliability of a single module.
- This assumes that the voter is perfect
  - a reasonable assumption if the voter complexity is much less than an individual module.

TMR vs. Simplex

- System reliability vs. module reliability

What is the conclusion?
TMR vs. Simplex: MTTF

- Compare reliability of simplex and TMR systems

\[ R_{\text{simplex}}(t) = e^{-\lambda t} \]

MTTF\(_{\text{simplex}} = \int e^{-\lambda t} \, dt = \frac{1}{\lambda} \]

\[ MTTF = \int_0^\infty R_{\text{TMR}}(t) \, dt \]

\[ R_{\text{TMR}}(t) = e^{-3\lambda t} + \left( \frac{3}{2} \right) e^{-2\lambda t} \left( 1 - e^{-\lambda t} \right) \]

\[ MTTF_{\text{TMR}} = \frac{3}{2\lambda} - \frac{2}{3\lambda} = \frac{5}{6\lambda} \]

MTTF\(_{\text{simplex}} > MTTF_{\text{TMR}}\]
TMR vs. Simplex: Mission Time

- Mission time
  \[ R_{Th} = 3e^{-2\lambda t_m} - 2e^{-3\lambda t_m} \]
- A numerical solution for \( t_m \) can be obtained iteratively
  - \( \lambda = \frac{1}{\text{year}} \), A.R. \( = 0.95 \)
  - MTTF
    - single: 1 yr, 0.05
    - TMR: 0.83, 0.145
- Thus TMR mission time is much better.

TMR vs. Simplex: Availability

- Temporary faults: steady state
  \[ A_{TMR} = 3A^2 - 2A^3, \quad A = \frac{\mu}{\lambda + \mu} \]
  - \( \lambda = 0.01 \Rightarrow A = 0.9901 \)
  - \( \Rightarrow \bar{A} = 0.01 \)
  - \( A_{TMR} = 0.9997 \Rightarrow \bar{A}_{TMR} = 0.0003 \)
- Thus TMR can greatly reduce down-time in presence of temporary faults
TMR vs. Simplex: Summary

- Instead of MTTF, look at mission time
- Reliability of K-out-of-N systems very high in the beginning
  - spare components tolerate failures
- Reliability sharply falls down at the end
  - system exhausted redundancy, more hardware can possibly fail
- Such systems useful in aircraft control
  - very high reliability, short time
  - 0.99999 over 10 hour period

System with Backup: Effect of Coverage

- Failure detection is not perfect
  - Reconfiguration may not succeed
    - Attach a coverage "c"

\[
R_i = P\{U_i \text{ good}\} + 
    P\{U_i \text{ hastaken over } U_1 \text{ failed}\} \cdot P\{U_1 \text{ failed}\} 
  = R_i \cdot R_j \cdot C(1 - R_i) 
\]

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

- General case, n-1 spares

\[
R_s = R_m \cdot \sum_{i=0}^{n-1} C^i (1 - R_m)^i 
\]
System with Backup: Effect of Coverage

- If coverage is 100%, then given low module reliability, can increase system reliability arbitrarily.
- With low coverage, reliability saturates.

<table>
<thead>
<tr>
<th>$R_m$</th>
<th>0.9</th>
<th>0.7</th>
<th>0.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>$R_a = 0.9$</td>
<td>0.989</td>
<td>0.908</td>
<td>0.748</td>
</tr>
<tr>
<td>$R_a = 0.9$, $u \leq 2$</td>
<td>0.999</td>
<td>0.988</td>
<td>0.931</td>
</tr>
<tr>
<td>$R_a = 0.9$, $u &gt; 4$</td>
<td>0.999</td>
<td>0.996</td>
<td>0.990</td>
</tr>
<tr>
<td>$R_a = 0.8$, $u \leq 2$</td>
<td>0.972</td>
<td>0.888</td>
<td>0.700</td>
</tr>
<tr>
<td>$R_a = 0.8$, $u &gt; 4$</td>
<td>0.978</td>
<td>0.918</td>
<td>0.812</td>
</tr>
<tr>
<td>$R_a = 0.8$, $u = \infty$</td>
<td>0.978</td>
<td>0.921</td>
<td>0.833</td>
</tr>
</tbody>
</table>

Effect of Voter

- Previous expression for reliability assumed voter 100% reliable.
- Assume voter reliability $R_v$.

$$R_{IMVP} = R_v \left( R_m^3 + \frac{3}{2} R_m^2 (1 - R_m) \right)$$
TMR+Spares

- TMR core, n-3 spares (assume same failure rate)
- System failure when all but one modules have failed.
  - If we start with 3 in the core and 2 spares, the sequence is:
    - 3+2 \rightarrow 3+1 \rightarrow 3+0 \rightarrow 2+0 \rightarrow failure
- Reliability of the system then is
  \[ R_s = R_{sw}[1-nR(1-R)^{n-1}-(1-R)^n] \]
  - Where R is reliability of a single module and R_{sw} is the reliability of the switching circuit overhead.
  - R_{sw} should depend on total number of modules n, and relative complexity of the switching logic.
- Let us assume that R_{sw}=(R^a)^n,
  - where a is measure of relative complexity, generally a <<1
  \[ R_s = R^n[1-nR(1-R)^{n-1}-(1-R)^n] \]