Fault Tolerant Computing
CS 530
Reliability Analysis

Yashwant K. Malaiya
Colorado State University
Reliability Analysis: Outline

Reliability measures:
• Reliability, availability, Transaction Reliability,
• MTTF and R(t), MTBF

Basic Cases
• Single unit with permanent failure, failure rate
• Single unit with temporary failures

Combinatorial Reliability: Block Diagrams
• Serial, parallel. K-out-of-n systems
• Imperfect coverage

Redundancy
• TMR, spares
• Generalized
Reliability Analysis

• Permanent faults
  ▪ The unit will eventually fail. Thus reliability “decays”.

• Temporary faults
  ▪ Faults come and go. Often Steady state characterization is possible.
  ▪ Permanent faults subject to repair are modeled as temporary faults.

• Design faults
  ▪ Reliability growth occurs during testing & debugging. We will study this under “Software Reliability” later.
Why Mathematical Analysis?

- You can determine reliability by constructing a large number of copies of the target system, and collecting failure data. However, that would be infeasible except for special cases.
- Thus we need to be able to determine the reliability before a system is built, by using the information we have about the components and the proposed architecture.
Basic Reliability Measures

- **Reliability**: durational (default)
  \[ R(t) = P\{\text{correct operation in duration } (0,t)\} \]
  - This is the default definition of reliability.

- **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
  \[ R_t = P\{\text{a transaction is performed correctly}\} \]

- The term “Reliability” is sometimes used with a non-standard meaning.
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.
  - Approximately equal to
- **Mean time to repair (MTTR):** expected time during which the unit is non-operational.
Mean time to …

Average Rated Life for Various Types of Bulbs

<table>
<thead>
<tr>
<th>Type</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incandescent</td>
<td>750-2,000</td>
</tr>
<tr>
<td>Compact Fluorescent CFL</td>
<td></td>
</tr>
<tr>
<td>Plug-in</td>
<td>10,000-20,000</td>
</tr>
<tr>
<td>Screw-based</td>
<td>8,000-10,000</td>
</tr>
<tr>
<td>Halogen</td>
<td>2,000-4,000</td>
</tr>
<tr>
<td>LED</td>
<td>40,000-50,000</td>
</tr>
</tbody>
</table>

Mean Time to Failure (MTTF)

- There is a very useful general relation between MTTF and $R(t)$. Here $T$ is time to failure, which is a random variable.

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

Thus

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

Note:

\[
R(t) = 1 - P\{\text{failure in } (0, t)\} = 1 - P\{0 \leq T \leq t\} = 1 - F(t)
\]

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

or \( f(t) = -\frac{dR(t)}{dt} \)

Note:

\[
x e^{-x} \to 0 \text{ as } x \to \infty
\]

and $R(t)$ is generally of the form $e^{-at}$

Thus $tR(t) \to 0$ as $t \to \infty$. 

Worth Remembering!
Failures with Repair

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

**Diagram:**

- "failure" to "repair" to "good" to "repair" to "bad" to "repair" to "good"

- **MTBF = MTTF + MTTR**
  - MTBF, MTTF are the same same when MTTR ≈ 0
  - Steady state availability = \( \frac{MTTF}{MTTF + MTTR} \)
Downtime of Cloud Services

And the cloud provider with the best uptime in 2015 is .. Network World
Mission Time (High-Reliability Systems)

- Reliability throughout the mission must remain above a threshold reliability $R_{th}$.
- **Mission time** $T_M$: defined as the duration in which $R(t) \geq R_{th}$.
- $R_{th}$ 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.
Constant Failure Rate Assumption

- We will always assume a constant failure rate.
  - It keeps analysis simple.
  - During operating life, the failure rate is approximately constant.
- The Bath-Tub curve:
  - In the beginning the failure rate is high because the weaker devices fail due to “infant mortality”. Near the end the failure rate is again high due to “aging” or wear-out of devices.
Basic Cases: Single Unit with Permanent Failure

• Failure rate is the probability of failure/unit time
• Assumption: constant failure-rate $\lambda$

The state transition diagram & the differential equation represent What we call Markov Modeling.

$$\frac{dp_0(t)}{dt} = -\lambda\ p_0(t)$$ since the rate of leaving state 0 depends on probability of being in state 0

$p_0(0) = 1$ initial condition
Single Unit with Permanent Failure (2)

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

\[ p_0(0) = 1 \]

_Solution: \( p_0(t) = e^{-\lambda t} \)

_Since \( R(t) = p_0(t) \)

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

"The Exponential Reliability Law"

At \( t = \frac{1}{\lambda} \), \( R(t) = e^{-1} = 0.368 \)
Single Unit: Permanent Failure (3)

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

\[ A(t) \text{ is same as } R(t) \text{ in this case.} \]

\[ MTTF = \int_{0}^{\infty} R(t)dt = \int_{0}^{\infty} e^{-\lambda t} dt \]

\[ = \left[-\frac{e^{-\lambda t}}{\lambda}\right]_0^{\infty} \]

\[ = \frac{1}{\lambda} \]

- **Ex 1:** a unit has MTTF = 30,000 hrs. Find failure rate.
  \[ \lambda = \frac{1}{30,000} = 3.3 \times 10^{-5}/hr \]

- **Ex 2:** Compute mission time \( T_M \) if \( R_{th} = 0.95 \).
  \[ e^{-\lambda T_M} = 0.95 \]
  \[ T_M = -\frac{\ln(0.95)}{\lambda} \approx 0.051/\lambda \]

- **Ex 3:** Assume \( \lambda = 3.33 \times 10^{-5} \) and \( R_{th} = 0.95 \) find \( T_M \).
  Ans: \( T_M = 1538.8 \) hrs
  (compare with MTTF = 30,000)
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 we can get an expression for \( p_1(t) \), however it is not needed since \( p_1(t) = 1 - p_0(t) \).

Note state diagram & Differential equations for Markov modeling

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 \( A(t) = p_0(t) \)

Thus \( A(t) = p_0(0)e^{-(\lambda + \mu)t} + \frac{\mu}{\lambda + \mu} (1 - e^{-(\lambda + \mu)t}) \)

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

- Thus MTTF = \( \frac{1}{\lambda} \)

- Mission time: also same

Note that when we say **no failures in (0,t)**, even a brief failure is a failure. Thus R(t) may be too strict as a measure when brief failures may be acceptable.
Combinatorial Reliability

This is a part of classic reliability theory.

**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 $R(t)$, $A(t)$, $R_t(t)$. A system is either good or bad.
Series configuration: all units are essential. System fails if one of them fails.

• Assumption: statistically independent failures in units.

\[ R_S = P\{U_1 \text{ good}\} \cap P\{U_2 \text{ good}\} \cap P\{U_3 \text{ good}\} \]

\[ = P\{U_1 g\} \cap P\{U_2 g\} \cap P\{U_3 g\} \]

\[ = R_1 R_2 R_3 \]

In general \[ R_S = \prod_{i=1}^{n} R_i \]
Series configuration

If \( R_i(t) = e^{-\lambda_i t} \)

then \( R_s(t) = \prod e^{-\lambda_i t} = e^{-[\lambda_1 + \lambda_2 + \cdots + \lambda_n] t} \)

i.e. system failure rate is the sum of individual failure rates:

\[
\lambda_s = \lambda_1 + \lambda_2 + \cdots + \lambda_n
\]

This gives us a nice way to estimate the overall failure rate, when all the individual units are essential. This is the basis of the approach used in the popular "Military Handbook" MIL-HDBK-217 approach for estimating the failure rates for different systems.

The failure rates of individual units are estimated using empirical formulas. For example the failure rate of a VLSI chip is related to its complexity etc.
“A chain is as strong as it's weakest link”

Let us see for a 4-unit series system

- Assume $R_1 = R_2 = R_3 = 0.95$, $R_4 = 0.75$
  - $R_S = 0.95 \times 0.95 \times 0.95 \times 0.75 = 0.643$
- 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.

Do you agree?
Combinatorial: Parallel

- **Parallel configuration**: System is good when least one of the several replicated units is good. A parallel configuration represents an *ideal* redundant system, ignoring any overhead.

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

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

i.e. \( \overline{R_s} = \prod_{i=1}^{n} \overline{R_i} \)

Where \( \overline{R} \) represents 1-R, i.e. “unreliability”
Parallel Configuration: Example

Problem: Need system reliability \( R_s = 1 - \varepsilon \)
How many parallel units are needed
if \( R_1 = R_2 = \Lambda = R_m \), \( R_m < R_s \)?

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 \( x = 4 \).

Remember, we’re consider an ideal system

Sometimes it is more convenient to talk in terms of “unreliability”
An Example Problem

The failure rate for sub-units A1 and A2 is $\lambda_A$, for sub-units B1 and B2, the failure rate is $\lambda_B$, for sub-units C1 and C2, the failure rate is $\lambda_C$. You can assume independence of failures for sub-units. Find an expression for $R(t)$ and MTTF.

- $R(t) = [P\{A1 is good\}P\{A2 is good\} + P\{A1 is good\}P\{A2 is bad\} + P\{A1 is bad\}P\{A2 is good\}] \cap P\{B is good\}$
  
  $= [1 - P\{A1 is bad\}P\{A2 is bad\}] \cap P\{B is good\}$
  
  $= [1 - (1 - e^{-\lambda_A t})^2] e^{-\lambda_B t} = [2e^{-\lambda_A t} - e^{-2\lambda_A t}] e^{-\lambda_B t}$
  
  $= [2 - e^{-\lambda_A t}] e^{-(\lambda_A + \lambda_B)t}$

- $MTTF = \int_0^\infty R_1(t) dt = \int_0^\infty [2 - e^{-\lambda_A t}] e^{-(\lambda_A + \lambda_B)t} dt = 2 \int_0^\infty e^{-(\lambda_A + \lambda_B)t} dt - \int_0^\infty e^{-(2\lambda_A + \lambda_B)t} dt = \frac{2}{\lambda_A + \lambda_B} - \frac{1}{2\lambda_A + \lambda_B}$