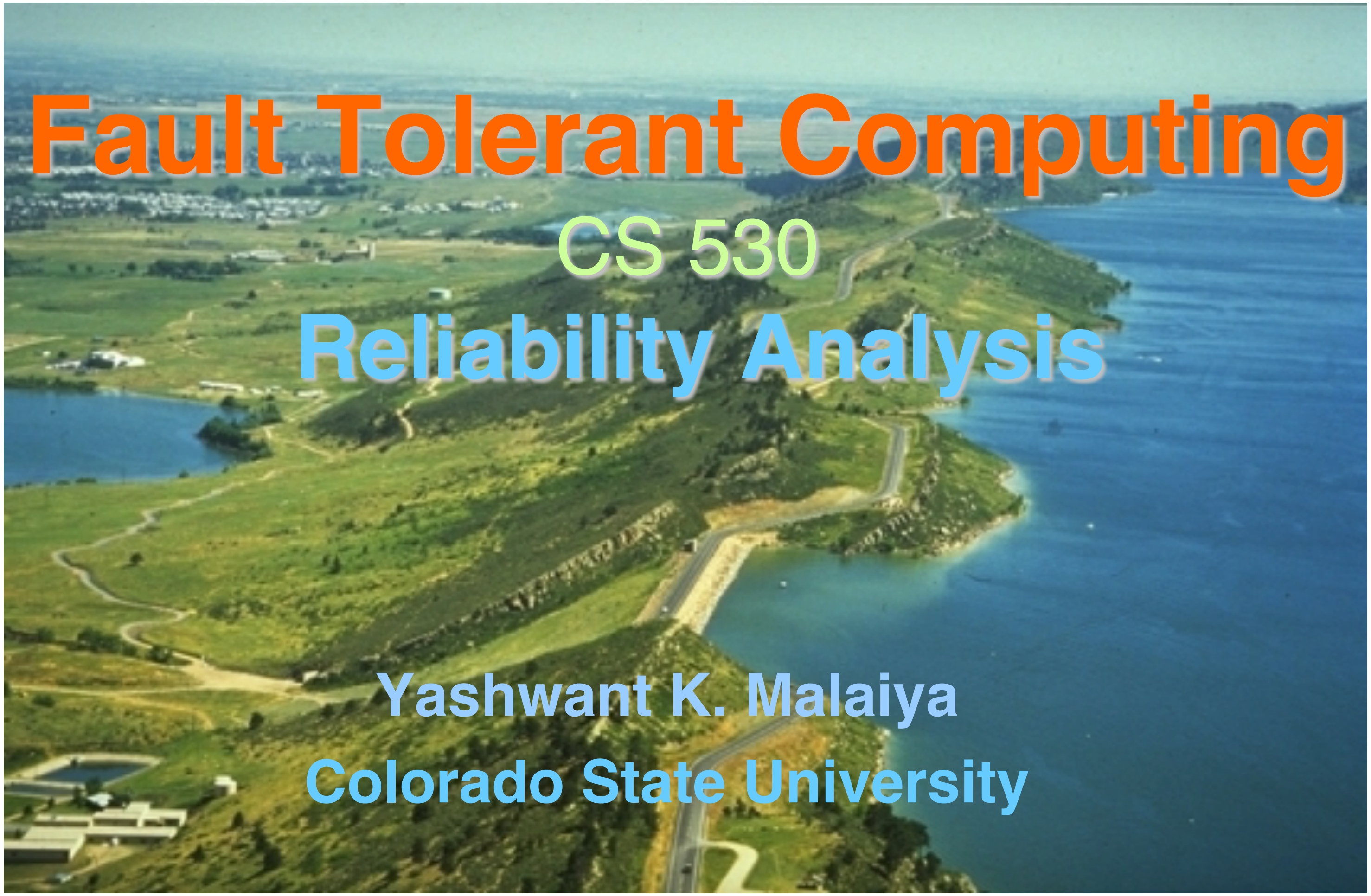


Fault Tolerant Computing

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

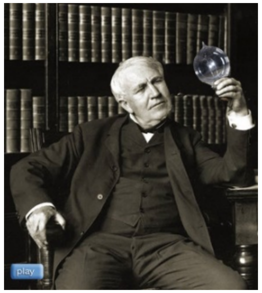
  $A(t)= P\{\text{correct operation at instant } t)\}$
  - Applied in presence of temporary failures
  - A steady-state value is the expected value over a range of time.
- **Transaction Reliability:** single transaction

  $R_t=P\{\text{a transaction is performed correctly}\}$
- 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

Type	Hours	
Incandescent	750-2,000	
Compact Fluorescent CFL		
Plug-in	10,000-20,000	
Screw-based	8,000-10,000	
Halogen	2,000-4,000	
LED	40,000-50,000 ?	

The Great Lightbulb Conspiracy: The Phoebus cartel engineered a shorter-lived lightbulb and gave birth to planned obsolescence IEEE Spectrum

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.

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

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

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

$$Thus \; \boxed{MTTF = \int_0^\infty R(t) dt}$$

Worth Remembering!

Note:

$$R(t) = 1 - P\{failure \; in \; (0,t)\}$$
$$= 1 - P\{0 \le T \le t\}$$
$$= 1 - F(t)$$
$$\therefore \frac{dF(t)}{dt} = -\frac{dR(t)}{dt}$$
$$or \;\; f(t) = -\frac{dR(t)}{dt}$$

Note:

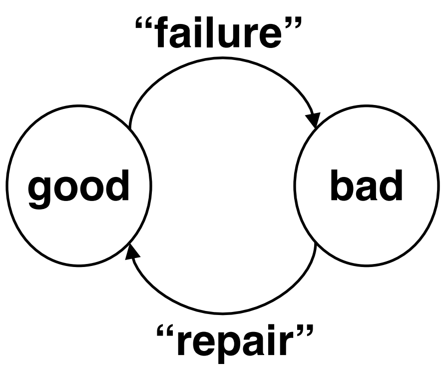
$xe^{-x} \to 0 \; as \; x \to \infty$

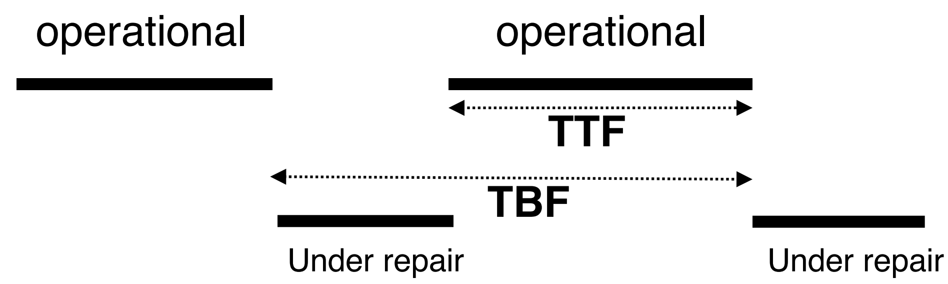
and R(t) is generally of the form e^{-at}

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

Failures with Repair

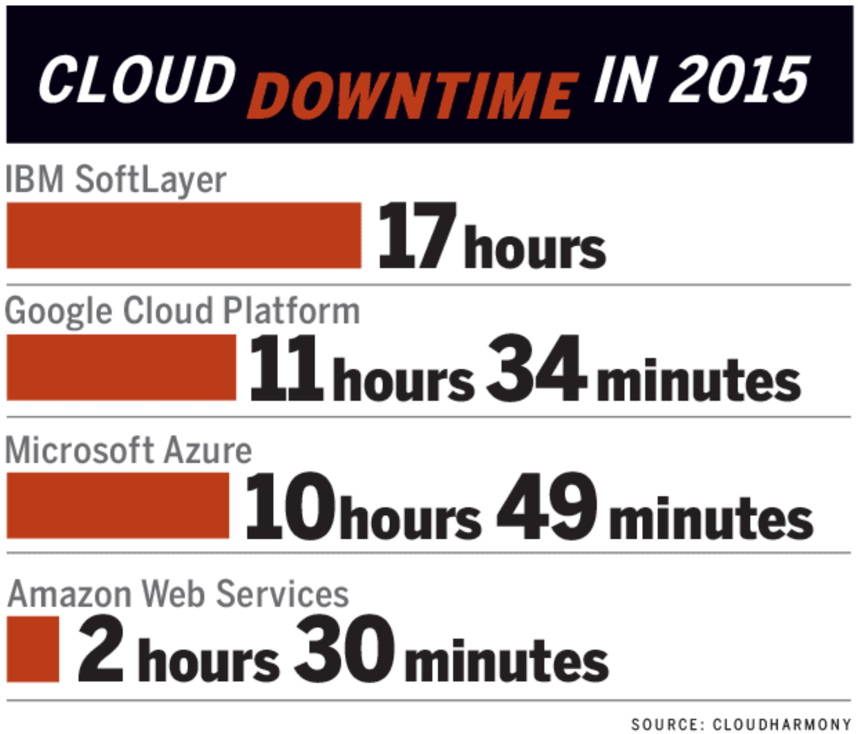
- **Time between failures: time to repair + time to next failure**





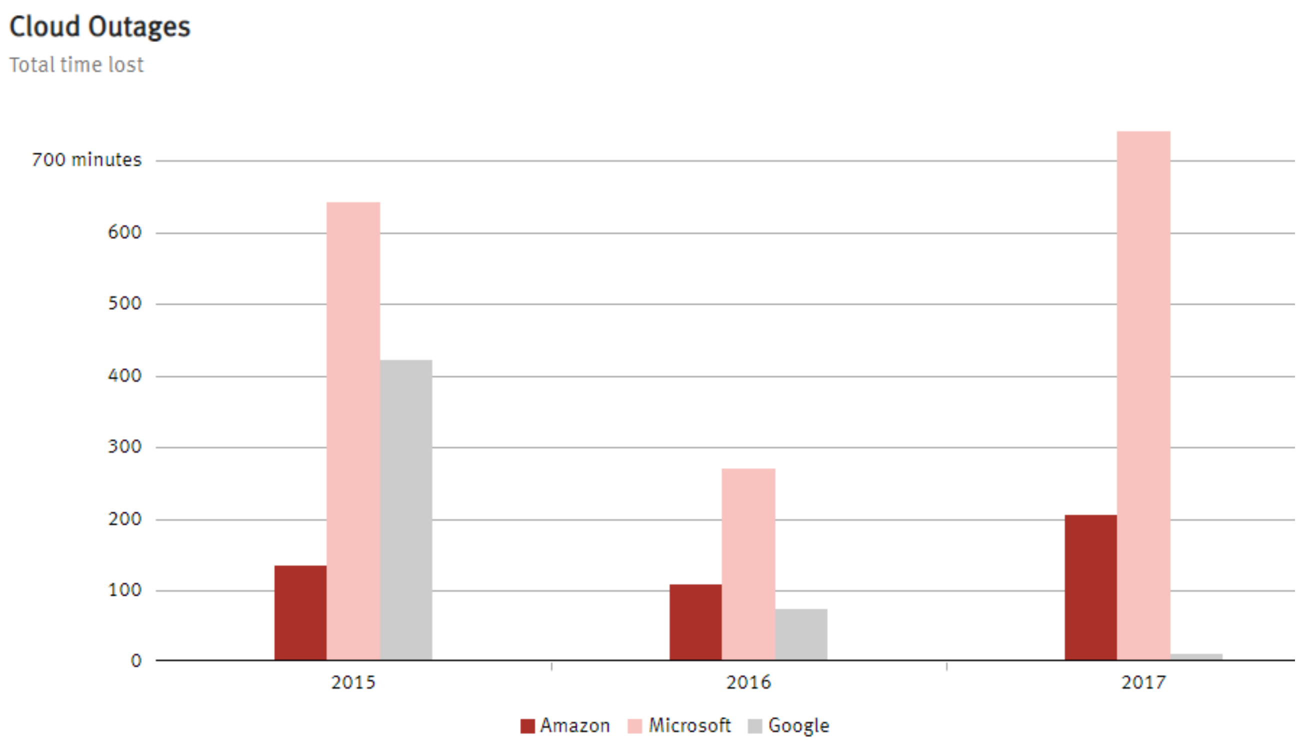
- **MTBF = MTTF + MTTR**
  - MTBF, MTTF are same same when MTTR ≈0
- **Steady state availability = MTTF / (MTTF+MTTR)**

Downtime of Cloud Services



And the cloud provider with the best uptime in 2015 is .. Network World

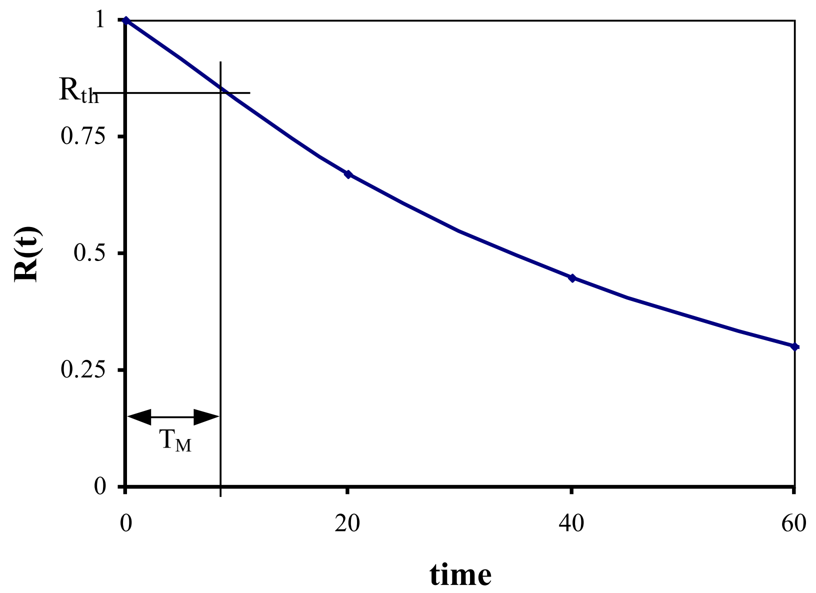
Downtime of Cloud Services



https://www.theinformation.com/articles/how-aws-stacks-up-against-rivals-on-downtime?shared=cMitFeGtWn4
https://www.geekwire.com/2019/google-really-run-reliable-cloud-service-even-sources-skeptical/

Mission Time (High-Reliability Systems)

- Reliability throughout the missic 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

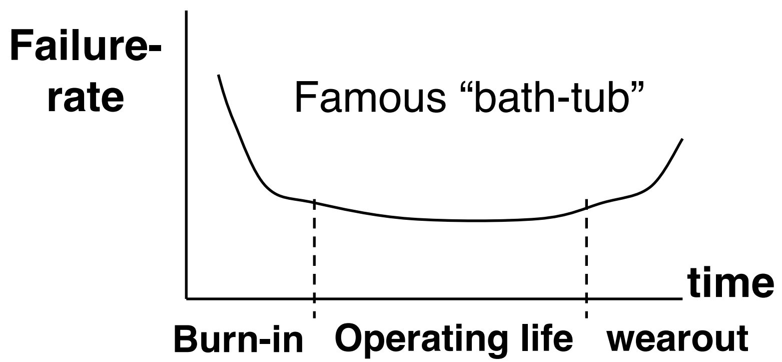
- We next consider two very important basic cases that serve as the basis for time-dependent analysis.

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.



FAQ

Disjoint vs independent

- **If A and B are disjoint, i.e. if** $A \bigcap B = \varphi$ **(i.e. empty set),**

$$P\{A \bigcup B\} = P\{A\} + P\{B\}$$

- **If A and B are independent,** P{A|B}= P{A}. **Then**

$$P\{A \bigcap B\} = P\{A\} P\{B\}$$

- **Estimation by Inspection Sampling: assuming Team 1 discovers the same fraction of faults, of all and those fund by Team**
- **Then x1/x = x3/x2**
- **Problem: tose found by Team 2 are easier to find. Thus actually** $\frac{x_3}{x_2} > \frac{x_1}{x} \; hence \; x > \frac{x_1 x_2}{x_3}$

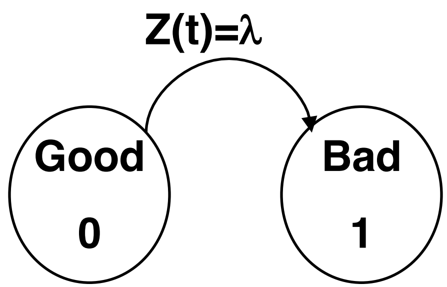
Policies

https://www.cs.colostate.edu/~cs530dl/

- Use of electronic devices (phones, pads or laptops) is not permitted in during the class.
- No collaboration of any type is permitted among the students in homework assignments and quizzes.

Basic Cases: Single Unit with Permanent Failure

- **Failure rate is the probability of failure/unit time**
- **Assumption: constant failure-rate λ**



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

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

$$\text{on probability of being in state 0}$$

$$p_0(0) = 1 \qquad \text{initial condition}$$

Single Unit with Permanent Failure (2)

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

$$p_0(0) = 1$$

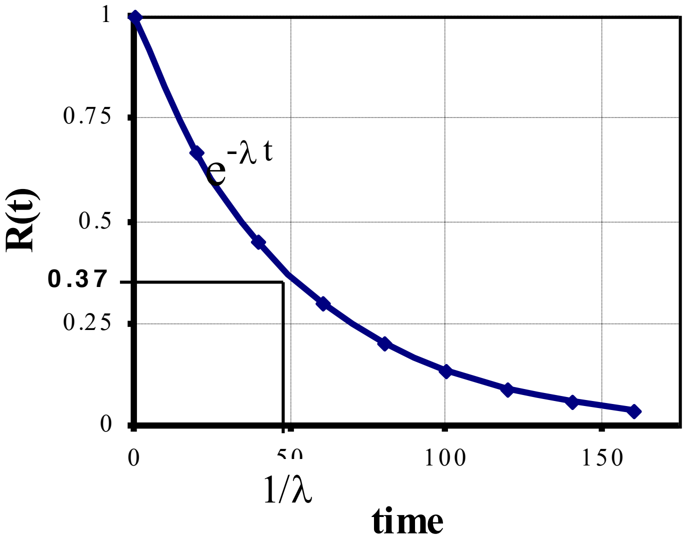
$$Solution : p_0(t) = e^{-\lambda\ t}$$

$$Since\ \ R(t) = p_0(t)$$

$$\boxed{R(t) = e^{-\lambda\ t}}$$

"The Exponential reliability law"

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



Single Unit: Permanent Failure (3)

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

$A(t)$ *is same as* $R(t)$ *in this case.*

$$MTTF = \int_0^\infty R(t)dt = \int_0^\infty e^{-\lambda t} dt$$

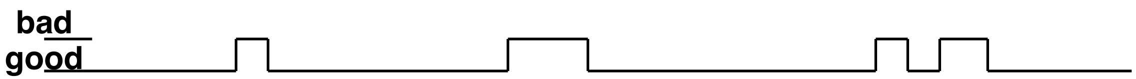
$$= [-\frac{e^{-\lambda t}}{\lambda}]_0^\infty$$

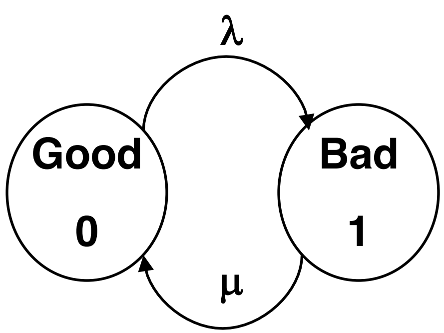
$$= \frac{1}{\lambda}$$

- **Ex 1:** a unit has MTTF =30,000 hrs. Find failure rate.
  $\lambda=1/30{,}000=3.3\text{x}10^{-5}/\text{hr}$
- **Ex 2:** Compute mission time T_M if R_{th} =0.95.
  $e^{-\lambda T_M} = 0.95$ $T_M = -\ln(0.95)/\lambda$
  $\approx 0.051/\lambda$
- **Ex 3:** Assume $\lambda=3.33\text{x}10^{-5}$, 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.

Note state diagram &

Differential equations for Markov modeling

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

Similarly we can get an expression for $\mathrm{p}_1(\mathrm{t})$, however it is not needed since $\mathrm{p}_1(\mathrm{t}) = 1 - \mathrm{p}_0(\mathrm{t})$.

Y. K. Malaiya, S. Y. H. Su: Reliability Measure of Hardware Redundancy Fault-Tolerant Digital Systems with Intermittent Faults. IEEE Trans. Computers 30(8): 600-604 (1981)

Single Unit: Temporary Failures(2)

- $p_0(t) = p_0(0)e^{-(\lambda+\mu)t} + \dfrac{\mu}{\lambda+\mu}(1-e^{-(\lambda+\mu)t})$
- Availability $\mathrm{A(t)} = p_0(t)$

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

- Note that steady – state probabilities exist :

$$\mathrm{t} \to \infty, p_0(t) = \frac{\mu}{\lambda+\mu} \qquad p_1(t) = \frac{\lambda}{\lambda+\mu}$$

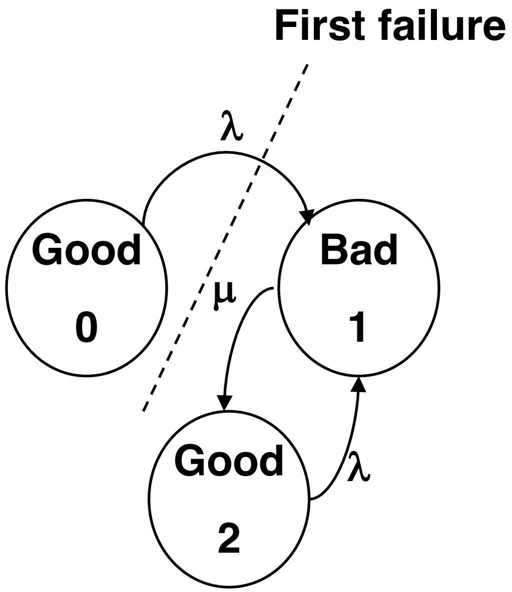
- Steady - state availability is $\dfrac{\mu}{\lambda+\mu}$

Single Unit: Temporary Failures(3)

- Reliability (durational)

$$R(t) = P\{\text{no failures in } (0, \text{t})\}$$
$$= P\{in\ Good\, 0\ at\ t\}$$
$$= e^{-\lambda t}$$

same as permanent failure



- Thus MTTF $= \dfrac{1}{\lambda}$
- 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 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:

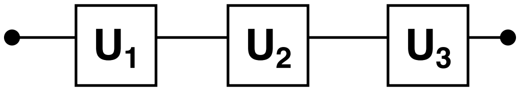
- Series configuration
- Parallel configuration
- Other cases involve combinations and other configurations.

- Note that conceptual modeling is applicable to R(t), A(t), R_t(t). A system is either good or bad.

Series configuration

Series configuration: all units are essential. System fails if one of them fails .

- **Assumption:** statistically independent failures in units.

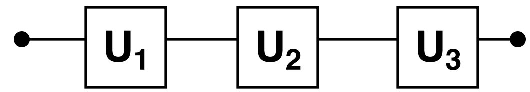


$$R_S = P\{U_1\ good \bigcap U_2\ good \bigcap U_3\ good\}$$
$$= P\{U_1\ g\}P\{U_2\ g\}P\{U_3\ g\}$$
$$= R_1 R_2 R_3$$

$$\text{In general } R_S = \prod_{i=1}^{n} R_i$$

Series configuration

The reliability block diagrams like this are only conceptual, not physical.



$$\text{If } \mathrm{R}_{\mathrm{i}}(t) = e^{-\lambda_i t}$$

$$\text{then } \mathrm{R}_{\mathrm{s}}(t) = \Pi e^{-\lambda_i t} = e^{-[\lambda_1 + \lambda_2 + \cdots + \lambda_n]t}$$

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

$$\lambda_{\mathrm{S}} = \lambda_1 + \lambda_2 + \cdots + \lambda_n$$

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"

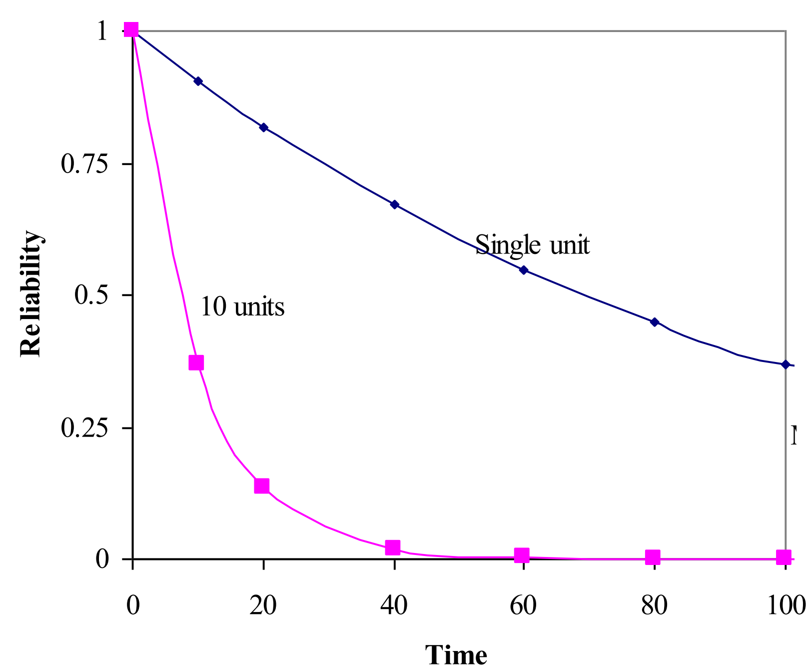
Do you agree?

Let us see for a 4-unit series system

- Assume $R_1=R_2=R_3=0.95$, $R_4=0.75$
  - $R_S= 0.95x0.95x0.95x0.75 = 0.643$
- 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.

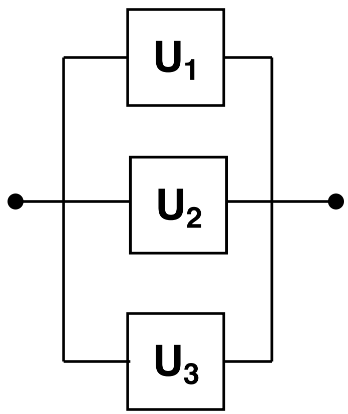
- More units, less reliability.



Combinatorial: Series

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.



$$
\begin{aligned}
R_s &= 1 - P\{all\ units\ \ bad\} \\
&= 1 - P\{U_1\ bad \bigcap U_2\ bad \bigcap U_3\ bad\} \\
&= 1 - P\{U_1\ b.\}P\{U_2\ b.\}P\{U_3\ b.\} \\
&= 1 - (1 - R_1)(1 - R_2)(1 - R_3)
\end{aligned}
$$

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

$$i.e.\quad \overline{R}_s = \prod_{i=1}^{n} \overline{R}_i$$

Where $\overline{\text{R}}$ represents 1-R, i.e. "*unreliability*"

Parallel Configuration: Example

Problem: Need system reliability $R_s = 1 - \in$

How many parallel units are needed

if $R_1 = R_2 = \cdots = R_m, R_m < R_s$?

Sometimes it is more convenient to talk in terms of "*unreliability*"

$$\text{Solution}: 1 - R_s = (1 - R_m)^x$$

$$\in = (1 - R_m)^x$$

$$x = \frac{\ln \in}{\ln(1 - R_m)}$$

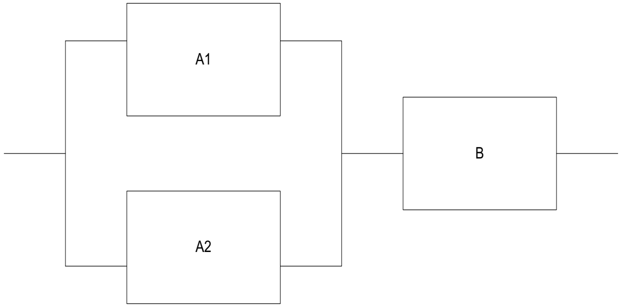
Assume $R_s = 0.9999$ ($\in = 0.0001$),

$R_m = 0.9$

gives $x = 4$.

Remember, we're consider an *ideal* system

An Example Problem



The failure rate for sub-units A1 and A2 is λ_A, for sub-unit B the failure rate is λ_B, 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}] ∩ P{B is good}**

  = [1- P{A1 is bad}P{A2 is bad}] ∩ P{B is good}

  $= [1-(1-e^{-\lambda_A t})^2\,]e^{-\lambda_B t} = [2e^{-\lambda_A t} - e^{-2\lambda_A t}\,]e^{-\lambda_B t}$

  $= [2 - e^{-\lambda_A t}\,]\, e^{-(\lambda_A+\lambda_B)t}$

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

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