Department of Systems Engineering
George Mason University

SYST 302: Systems Methodology and Design II #8

Kuo-Chu Chang
Fairfax, Virginia

Design for Reliability

- Concepts and Definition
- Measure of Reliability
- Reliability in System design
- Reliability Evaluation

What is Reliability

- **Reliability:** **the *probability* that the system will perform its required function in the desired manner during the time intervals when used under specified operating conditions**
  - **A desirable quality to measure performance**
  - **Standard of reliability is in general proportional to cost**
  - **An economic balance need to be made**
- **Risk Factor:** **high risk requires high reliability**
  - **Large invested capital: chemical plants, electrical power supply systems**
  - **Risk to human life: aircraft systems, nuclear power plants**
- **Reliable System Design:** **optimal design subject to budget constraint**

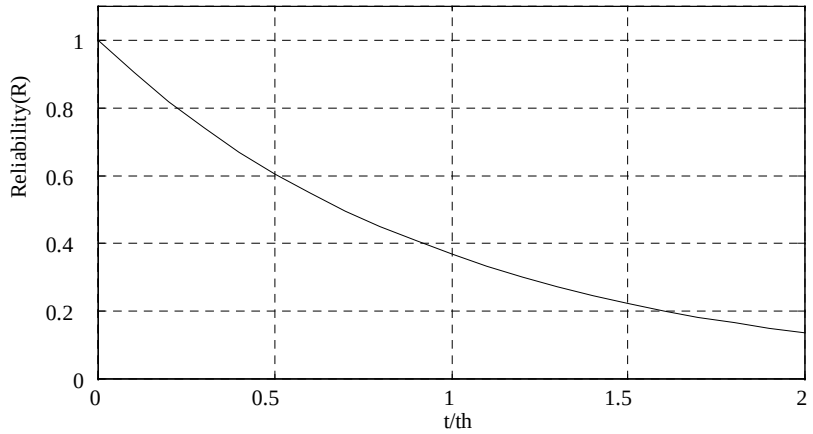
Measures of Reliability

- **Reliability Function: the *probability* that the system will be functional at least for some specified time *t***

$$R(t) = 1 - F(t) = 1 - \int_{-\infty}^{t} f(\tau)d\tau = \int_{t}^{\infty} f(\tau)d\tau$$

For exponential distribution $f(t) = \lambda e^{-\lambda t} = \frac{1}{\theta} e^{-\frac{t}{\theta}} \Rightarrow R(t) = e^{-\frac{t}{\theta}}$

λ: failure rate, θ: mean life (mean time between failures: MTBF)

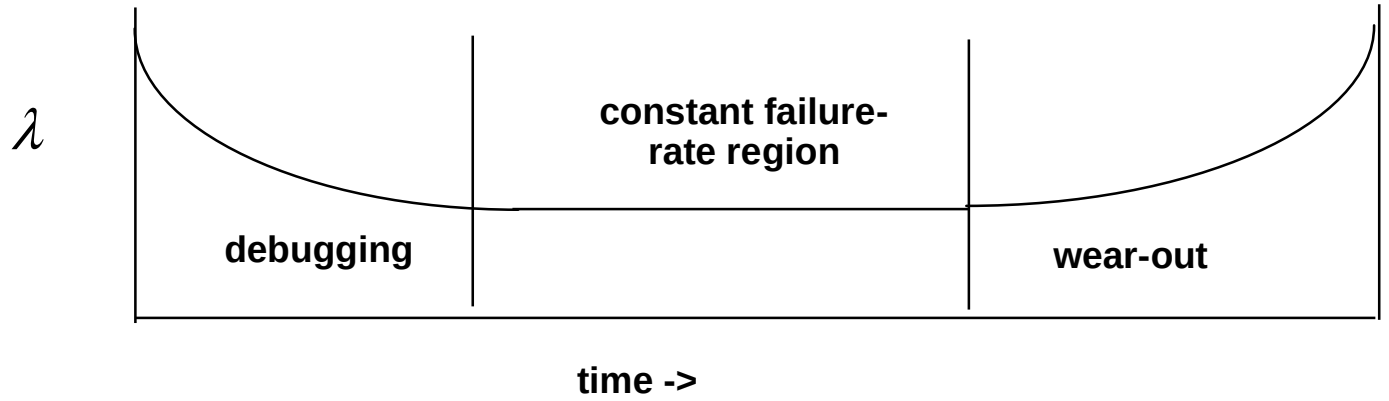


Failure Rate

failure rate: $\lambda = \dfrac{\text{number of failures}}{\text{total operating time}}$

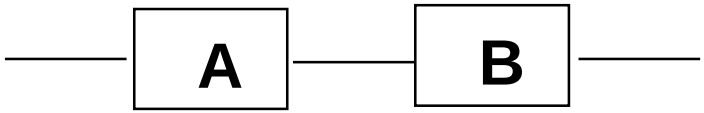
(average number of failures per unit time period)

$\text{MTBF} = \dfrac{1}{\lambda}$



Reliability Analysis

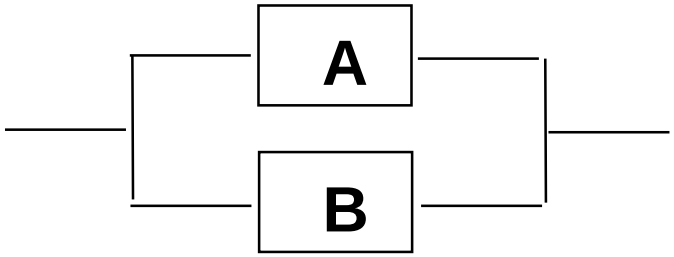
- **Standard Analysis: examines components or subsystems in series or in parallel**



Reliability of system $\equiv R_S = P(\text{system up})$

$= P(\text{system up} \mid A \text{ is up})P(A \text{ is up}) + P(\text{system up} \mid A \text{ is down})P(A \text{ is down})$

$= P(B \text{ is up})P(A \text{ is up}) = R_B R_A$



$R_S = P(\text{system up} \mid A \text{ is up})P(A \text{ is up}) + P(\text{system up} \mid A \text{ is down})P(A \text{ is down})$

$= 1 \cdot P(A \text{ is up}) + P(B \text{ is up})P(A \text{ is down})$

$= R_A + R_B(1 - R_A) = R_A + R_B - R_A R_B = 1 - (1 - R_A)(1 - R_B)$

Examples

Series networks:

$$R_S = R_1 R_2 \cdots R_n = (e^{-\lambda_1 t})(e^{-\lambda_2 t}) \cdots (e^{-\lambda_n t}) = e^{-(\lambda_1+\lambda_2+\cdots+\lambda_n)t}$$

$$\Rightarrow MTBF_S = \frac{1}{\lambda_1 + \lambda_2 + \cdots + \lambda_n} = \frac{1}{\frac{1}{MTBF_1} + \frac{1}{MTBF_2} + \cdots + \frac{1}{MTBF_n}}$$

Parallel networks:

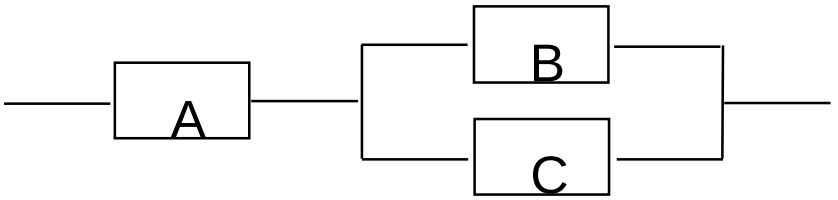
$$R_S = 1 - (1 - R_1)(1 - R_2) \cdots (1 - R_n)$$

if components are identical, i.e., $R_i = R \ \ \forall i,$ then

$$R_S = 1 - (1 - R)^n$$

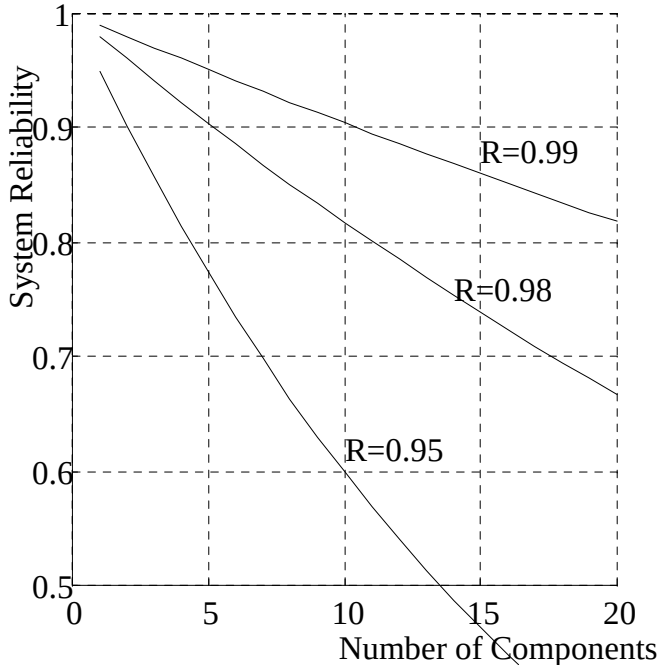
Combined networks:

$$R_S = R_A(R_B + R_C - R_B R_C)$$

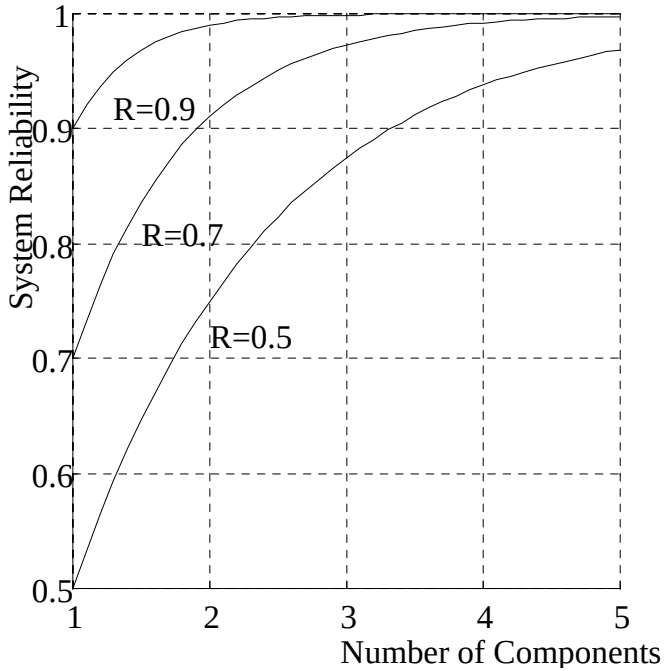


System Reliability

Series system



Parallel system



Fully and Partial Redundancy

- **Total Redundancy: the system will operate if one or more of the subsystems operate**

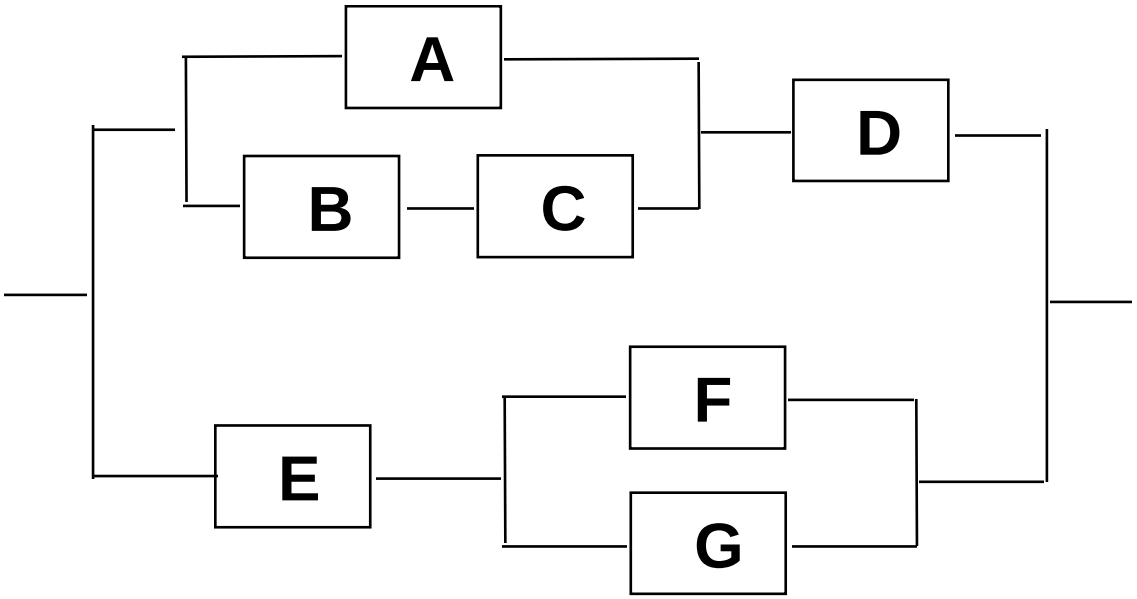
$$R_S = 1 - U_S = 1 - U_1 U_2 \cdots U_n = 1 - \prod_{i=1}^{n} (1 - R_i)$$

- **Partial Redundancy: the system will operate only if more than a minimum number of subsystems operate**

Assuming all subsystems have same reliabilities R_0 and at least k out of n subsystems need to operate in order for system to work,

then $$R_S = \sum_{i=k}^{n} C_i^n R_0^i (1 - R_0)^{n-i} = \sum_{i=k}^{n} \frac{n!}{i!(n-i)!} R_0^i (1 - R_0)^{n-i}$$

Redundancy in Design



Q: given reliability of each component

(1) which redundant component to add in order to increase system reliability the most
(2) which component has most/least impact on system reliability

Reliability Design

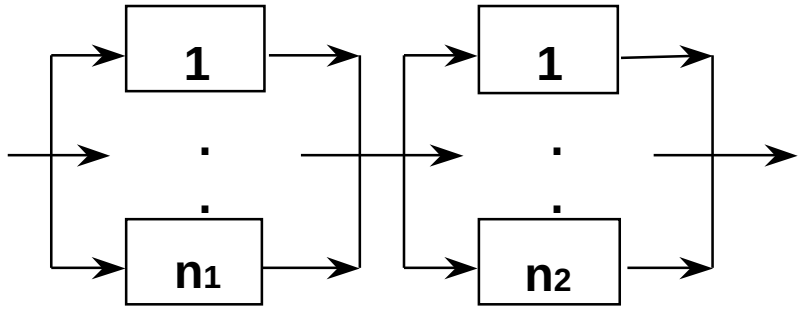
- **Systems Design:** with a reliability model, optimize the allocation of a given resource to various redundant items to improve system reliability
  - Maximize system reliability subject to budget constraint
  - Achieve a desirable reliability with minimum budget
- **Example:** A system comprises two stages. Components can be reproduced in parallel in both stages. The probabilities that, at any time, a component is functioning in stage 1 and 2 are p1 and p2 respectively. The component costs are c1 and c2. The total budget is B.
- So the problem becomes:

$$\text{Maximize } R = (1-(1-p_1)^{n_1})(1-(1-p_2)^{n_2})$$
$$\text{subject to } n_1c_1 + n_2c_2 \le B$$

Example

Maximize $R = (1-(1-p_1)^{n_1})(1-(1-p_2)^{n_2})$

subject to $n_1 c_1 + n_2 c_2 \le B$



Assuming $p_1 = 0.9,\ p_2 = 0.7,\ c_1 = \$2k, c_2 = \$3k,\ B = \$9k$

Sol:

1. Let $n_1 = 1,$ then $2n_1 + 3n_2 \le 9 \Rightarrow 3n_2 \le 7 \Rightarrow n_2 = 2$

$\Rightarrow R = (1-0.1)(1-0.3^2) = 0.819,$ cost $= \$8k$ *

2. Let $n_1 = 2,$ then $2n_1 + 3n_2 \le 9 \Rightarrow 3n_2 \le 5 \Rightarrow n_2 = 1$

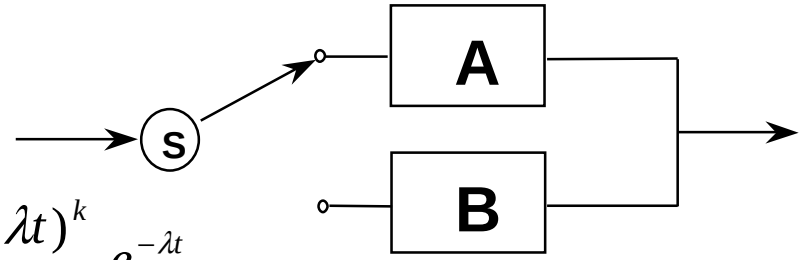
$\Rightarrow R = (1-0.1^2)(1-0.3) = 0.693,$ cost $= \$7k$

3. Let $n_1 = 3,$ then $2n_1 + 3n_2 \le 9 \Rightarrow 3n_2 \le 3 \Rightarrow n_2 = 1$

$\Rightarrow R = (1-0.1^3)(1-0.3) = 0.699,$ cost $= \$9k$

Note: for more complicated problems, use dynamic programming approach

Stand-by Redundancy



With Poisson assumption

Prob { k components fail in t } = $\frac{(\lambda t)^k}{k!} e^{-\lambda t}$

In a two - component stand - by redundancy system

R_s = Prob { $\leq$ 1 component fail in t } = $e^{-\lambda t} + (\lambda t) e^{-\lambda t}$

For a n - component stand - by redundancy system

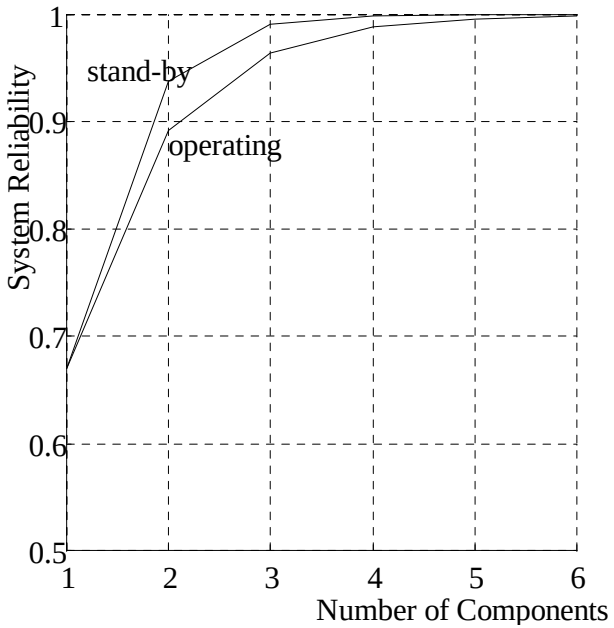
R_s = Prob { $\leq$ n - 1 component fail in t } = $e^{-\lambda t} + (\lambda t) e^{-\lambda t} + \cdots + \frac{(\lambda t)^{n-1}}{(n-1)!} e^{-\lambda t}$

Compare to a operating redundancy syetm

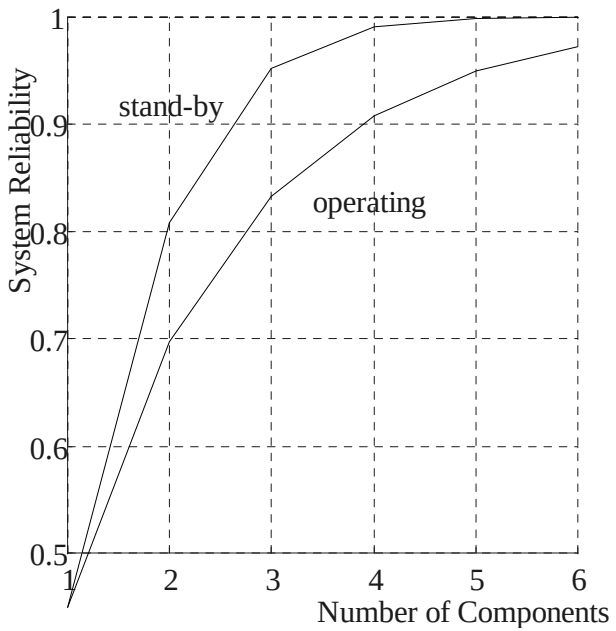
$R_o = 1 - (1 - e^{-\lambda t})^n$

ICBST: $R_s > R_o$ (ex: $\lambda = 0.002, t = 200, R_s = 0.9348 > R_o = 0.8913$ for a 2 - component system)

Examples



$\lambda t = 0.4$



$\lambda t = 0.8$

Reliability Test and Evaluation

- **Goal:** to determine whether the system under test meets the specified MTBF requirements
  - Many test methods and statistical procedures available
  - Most based on hypothesis testing
- **Reliability Sequential Qualification Testing**
  - To provide an evaluation of system development progress
  - To assure the specified requirements are met prior to proceeding to the next phase
  - Three possible decision: accept, reject, continue testing
  - Allow for an earlier decision if the system is highly reliable or unreliable
  - Subject to producer's risk (Type I error) and user's risk (Type II error)

Reliability Sequential Qualification Testing