


Karlsruhe Institute of Technology

# Reliable Computing I

## Lecture 5: Reliability Evaluation

Instructor: Mehdi Tahoori


INSTITUTE OF COMPUTER ENGINEERING (ITEC) – CHAIR FOR DEPENDABLE NANO COMPUTING (CDNC)



KIT – University of the State of Baden-Wuerttemberg and  
National Research Center of the Helmholtz Association

[www.kit.edu](http://www.kit.edu)

## 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

(c) 2012, Mehdi Tahoori

Reliable Computing I: Lecture 5

2

## 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 ...

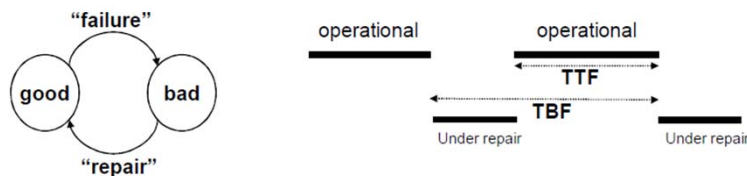


- Mean Time to Failure (MTTF):
  - expected time the unit will work without a failure.
- Mean time between failures (MTBF):
  - expected time between two successive failures.
    - Applicable when faults are temporary.
    - The time between two successive failures includes repair time and then the time 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

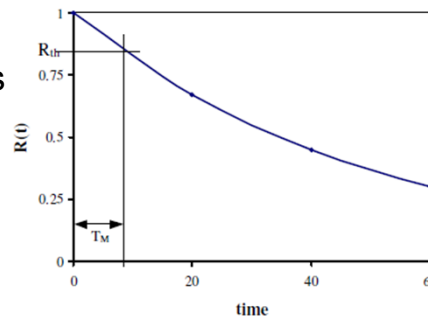


- $MTBF = MTTF + MTTR$
- MTBF, MTTF are same when  $MTTR \approx 0$
- Steady state availability =  $MTTF / (MTTF + MTTR)$

## Mission Time (High-Reliability Systems)



- Reliability throughout the mission must remain above a threshold reliability  $R_{th}$ .
- 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.



(c) 2012, Mehdi Tahoori

Reliable Computing I: Lecture 5

7

## 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.

(c) 2012, Mehdi Tahoori

Reliable Computing I: Lecture 5

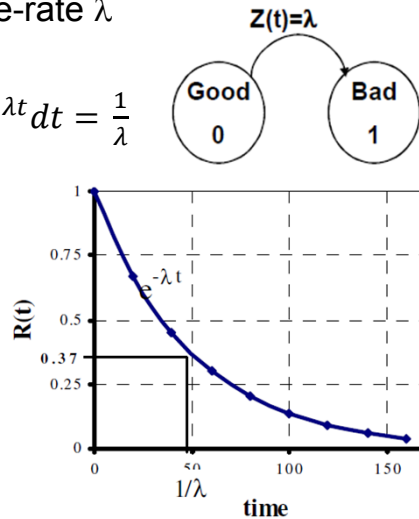
8

## 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.  
 $\lambda = 1/30,000 = 3.33 \times 10^{-5}/\text{hr}$
- Ex 2:** Compute mission time  $T_M$  if  $R_{th} = 0.95$ .  
 $e^{-\lambda T_M} = 0.95 \quad T_M = -\ln(0.95)/\lambda \approx 0.051/\lambda$
- 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)



(c) 2012, Mehdi Tahoeri

Reliable Computing I: Lecture 5

9

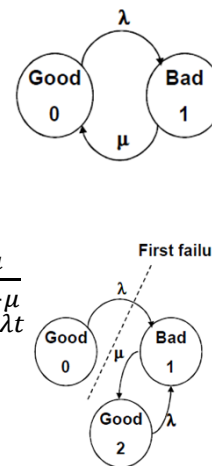
## Single Unit: Temporary Failures



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



(c) 2012, Mehdi Tahoeri

Reliable Computing I: Lecture 5

10

## 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



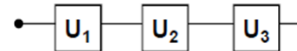
- Objective is: Given a
  - systems structure in terms of its units
  - reliability attributes of the units
  - some simplifying assumptions
- We need to evaluate the overall reliability measure.
- There are two extreme cases we will examine first:
  - Series configuration
  - Parallel configuration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

$$\begin{aligned} R_s &= P\{U_1 \text{ good} \cap U_2 \text{ good} \cap U_3 \text{ good}\} \\ &= P\{U_1 \text{ g}\}P\{U_2 \text{ g}\}P\{U_3 \text{ g}\} \\ &= R_1 R_2 R_3 \end{aligned}$$



- Reliability of the system

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

## Series configuration



- For exponential failure rate of each component

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

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

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

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

- System failure rate is the sum of individual failure rates:

$$\lambda_s = \lambda_1 + \lambda_2 + \dots + \lambda_n$$

- Mean time to failure:

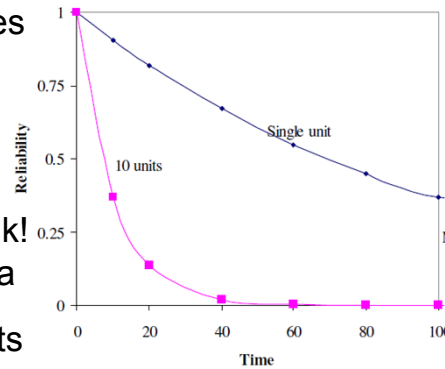
$$MTTF_{series} = \frac{1}{\sum_{i=1}^n \lambda_i}$$

## “A chain is as strong as it's weakest link”?

- Let us see for a 4-unit series system

- Assume  $R_1=R_2=R_3=0.95$ ,  
 $R_4=0.75$
- $R_5=0.643$

- 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.



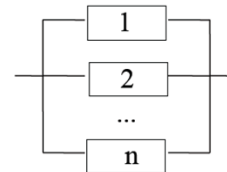
- More units, less reliability

if  $X_i \equiv$  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 =
  - $(1 - R_1)(1 - R_2) \dots (1 - R_n)$
- Prob [at least one module survives] =
  - $1 - \text{Prob [none module survives]}$
- Reliability of the parallel system



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



## Parallel Systems



$$\begin{aligned}
 E(X) &= \int_0^{\infty} [1 - (1 - e^{-\lambda t})^n] dt \\
 &= \dots \\
 &= \frac{1}{\lambda} \sum_{i=1}^n \frac{1}{i} \\
 &\approx \frac{\ln(n)}{\lambda}
 \end{aligned}$$

## Parallel Configuration: Example



- Problem: Need system reliability  $R_s = 1 - \epsilon$ 
  - How many parallel units are needed
    - If  $R_1 = R_2 = \dots = R_m$ ,  $R_m < R_s$

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

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

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

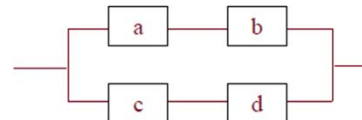
Assume  $R_s = 0.9999$  ( $\epsilon = 0.0001$ ),  
 $R_m = 0.9$   
 gives  $x = 4$ .

## Series-Parallel Systems

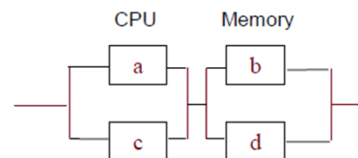


- Consider combinations of series and parallel systems
- Example, two CPUs connected to two memories in different ways

$$R_{sys} = 1 - (1 - R_a R_b) (1 - R_c R_d)$$



$$R_{sys} = (1 - (1 - R_a)(1 - R_c)) (1 - (1 - R_b)(1 - R_d))$$



(c) 2012, Mehdi Tahoori

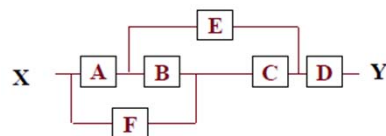
Reliable Computing I: Lecture 5

19

## Non-Series-Parallel-Systems



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



Each path from X to Y represents a configuration that leaves the system operational

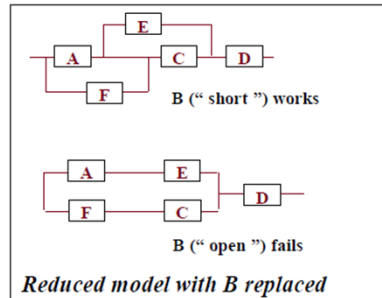
- Reliability of the system can be derived by expanding around a single module  $m$
- $R_{sys} = R_m P(\text{system works} \mid m \text{ works}) + (1 - R_m) P(\text{system works} \mid m \text{ fails})$ 
  - where the notation  $P(s \mid m)$  denotes the conditional probability “s given m has occurred”

(c) 2012, Mehdi Tahoori

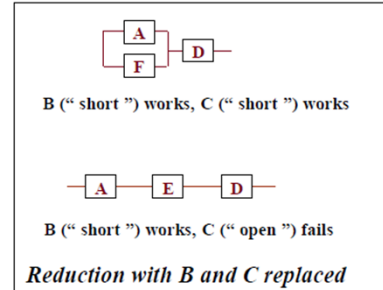
Reliable Computing I: Lecture 5

20

## Non-Series-Parallel-Systems



$$R_{sys} = R_B P(\text{system works} | B \text{ works}) + (1 - R_B) \{R_D [1 - (1 - R_A R_E)(1 - R_F R_C)]\}$$



$$P(\text{system works} | B \text{ works}) = R_C \{R_D [1 - (1 - R_A)(1 - R_E)]\} + (1 - R_C)(R_A R_D R_E)$$

Letting  $R_A \dots R_F = R_m$  yields  $R_{sys} = R_m^6 - 3R_m^5 + R_m^4 + 2R_m^3$

## Non-Series-Parallel-Systems



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

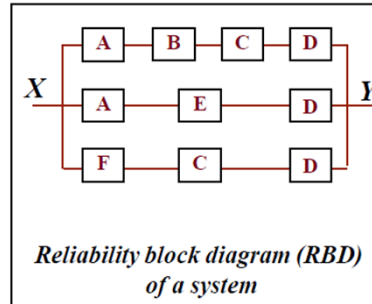
- An upper bound on system reliability is:

$$R_{sys} \leq 1 - \prod (1 - R_{path\ i}) \quad R_{path\ i} \text{ is the serial reliability of path } i$$

- 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



$$R_{sys} \leq 1 - (1 - R_A R_B R_C R_D)(1 - R_A R_E R_D)(1 - R_F R_C R_D)$$

$$R_{sys} \leq 2R_m^3 + R_m^4 - R_m^6 - 2R_m^7 + R_m^{10}$$

## 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.

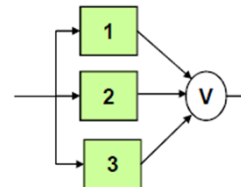
### ■ System reliability then is $R_{k/n} = \sum_{i=k}^n \binom{n}{i} p^i (1-p)^{n-i}$

- 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

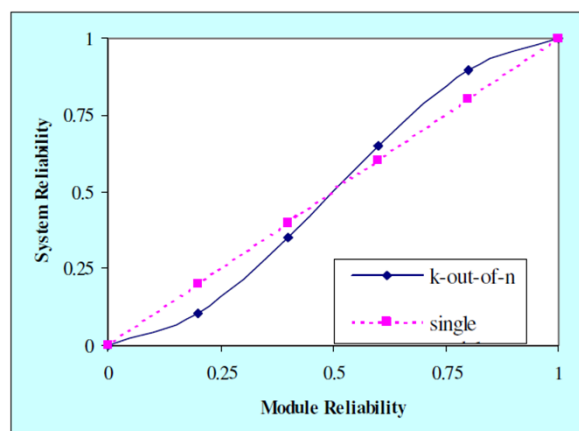
$$\begin{aligned}
 R_{TMR} &= \sum_{i=2}^3 \binom{3}{i} R^i (1-R)^{3-i} \\
 &= 3R^2(1-R) + R^3 \\
 &= 3R^2 - 2R^3
 \end{aligned}$$



- 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

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

$$MTTF_{\text{simplex}} = \int_0^{\infty} e^{-\lambda t} dt = 1/\lambda$$

$$MTTF = \int_0^{\infty} R_{TMR}(t) dt$$

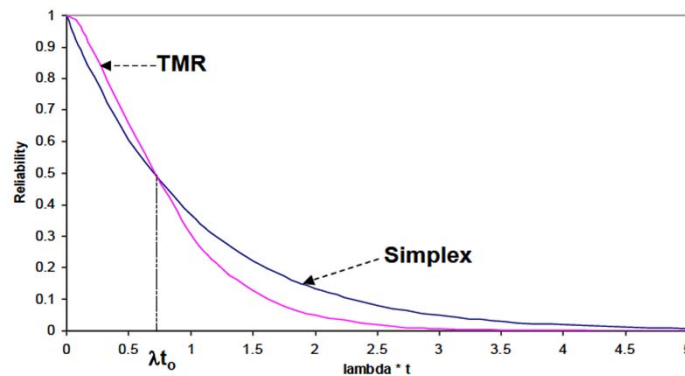
$$R_{TMR}(t) = e^{-3\lambda t} + \binom{3}{2} e^{-2\lambda t} (1 - e^{-\lambda t})$$

$$= \int_0^{\infty} (3e^{-2\lambda t} - 2e^{-3\lambda t}) dt$$

$$MTTF_{TMR} = \frac{3}{2\lambda} - \frac{2}{3\lambda} = \frac{5}{6\lambda}$$

$$MTTF_{\text{simplex}} > MTTF_{TMR}$$

## TMR vs. Simplex: MTTF



$$R_{TMR}(t) \geq R(t) \quad 0 \leq t \leq t_0$$

$$R_{TMR}(t) \leq R(t) \quad t_0 \leq t < \infty$$

$$\text{where } t_0 = \frac{\ln 2}{\lambda} \approx \frac{0.7}{\lambda}$$

## 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

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

	MTTF	$t_m$
single	1yr	0.05
TMR	0.83	0.145

### ■ Thus TMR mission time is much better.

## TMR vs. Simplex: Availability



### ■ Temporary faults: steady state

$$A_{TMR} = 3A^2 - 2A^3, A = \frac{\mu}{\lambda + \mu}$$

$$\text{Ex: } \frac{\lambda}{\mu} = 0.01 \Rightarrow A = 0.9901$$

$$\Rightarrow \bar{A} = 0.01$$

$$A_{TMR} = 0.9997 \Rightarrow \bar{A}_{TMR} = 0.0003$$

### ■ Thus TMR can greatly reduce down-time in presence of temporary faults

## TMR vs. Simplex: Summary

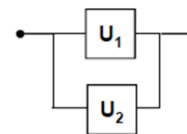


- Instead of MTTF, look at mission time
- Reliability of K-out-of-N systems very high in the beginning
  - spare components tolerate failures
- Reliability sharply falls down at the end
  - system exhausted redundancy, more hardware can possibly fail
- Such systems useful in aircraft control
  - very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

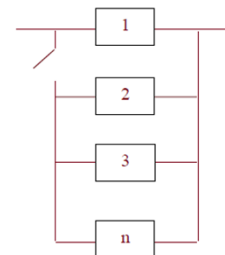


$$\begin{aligned}
 R_s &= P\{U_1 \text{ good}\} + \\
 &\quad P\{U_2 \text{ has taken over} \mid U_1 \text{ failed}\} P\{U_1 \text{ failed}\} \\
 &= R_1 + R_2 C (1 - R_1)
 \end{aligned}$$

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

- General case, n-1 spares

$$R_s = R_m \sum_{i=0}^{n-1} C^i (1 - R_m)^i$$





## 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

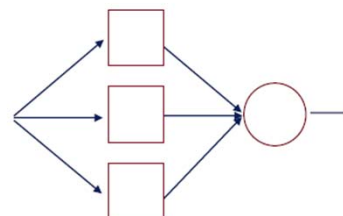
	$R_m = 0.9$	$R_m = 0.7$	$R_m = 0.5$
$C=0.99, n=2$	0.989	0.908	0.748
$C=0.99, n=4$	0.999	0.988	0.931
$C=0.99, n=\infty$	0.999	0.996	0.990
$C=0.8, n=2$	0.972	0.868	0.700
$C=0.8, n=4$	0.978	0.918	0.812
$C=0.8, n=\infty$	0.978	0.921	0.833

## Effect of Voter



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

$$R_{TMRV} = R_v (R_m^3 + \binom{3}{2} R_m^2 (1 - R_m))$$



## 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:
    - $3+2 \rightarrow 3+1 \rightarrow 3+0 \rightarrow 2+0 \rightarrow \text{failure}$
- 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  $\ll 1$
- $R_s = R^{an} [1 - nR(1-R)^{n-1} - (1-R)^n]$