

FAULT TOLERANT SYSTEMS

<http://www.ecs.umass.edu/ece/koren/FaultTolerantSystems>

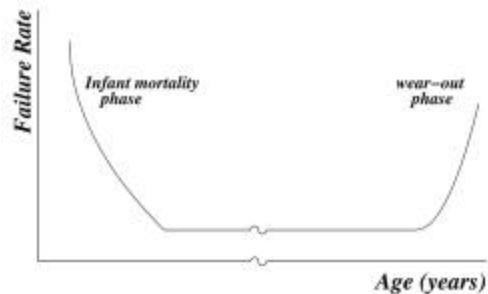
Part 2 - Canonical Structures Chapter 2 - Hardware Fault Tolerance

Part.2 .1

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Failure Rate

- ◆ Rate at which a component suffers faults
- ◆ Depends on age, ambient temperature, voltage or physical shocks that it suffers, and technology
- ◆ Dependence on age is usually captured by the **bathtub curve**:

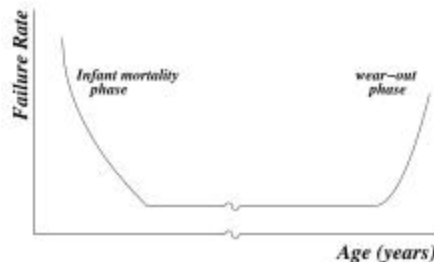


Part.2 .2

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Bathtub Curve

- ◆ Young component - high failure rate
 - * Good chance that some defective units slipped through manufacturing quality control and were released
- ◆ Later - bad units weeded out - remaining units have a fairly constant failure rate
- ◆ As component becomes very old, aging effects cause the failure rate to rise again



Part.2 .3

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Empirical Formula for λ - Failure Rate

- ◆ $\lambda = p_L p_Q (C_1 p_T p_V + C_2 p_E)$
 - * p_L : Learning factor, (how mature the technology is)
 - * p_Q : Manufacturing process Quality factor (0.25 to 20.00)
 - * p_T : Temperature factor, (from 0.1 to 1000), proportional to $\exp(-E_a/kT)$ where E_a is the activation energy in electron-volts associated with the technology, k is the Boltzmann constant and T is the temperature in Kelvin
 - * p_V : Voltage stress factor for CMOS devices (from 1 to 10 depending on the supply voltage and the temperature); does not apply to other technologies (set to 1)
 - * p_E : Environment shock factor: from about 0.4 (air-conditioned environment), to 13.0 (harsh environment - e.g., space, cars)
 - * C_1, C_2 : Complexity factors; functions of number of gates on the chip and number of pins in the package
 - * Further details: MIL-HDBK-217E handbook

Part.2 .4

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Reliability and MTTF of a Single Component (Module)

- ◆ Module operational at time $t=0$
- ◆ Remains operational until it is hit by a failure
- ◆ All failures are permanent
- ◆ T - lifetime of module - time until it fails
- ◆ T is a random variable
- ◆ $f(t)$ - density function of T
- ◆ $F(t)$ - cumulative distribution function of T

Part.2 .5

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Probabilistic Interpretation of $f(t)$ and $F(t)$

- ◆ $F(t)$ - probability that the component will fail at or before time t

$$F(t) = \text{Prob} \{T \leq t\}$$
- ◆ $f(t)$ - not a probability, but the momentary rate of probability of failure at time t

$$f(t)dt = \text{Prob} \{t \leq T \leq t+dt\}$$
- ◆ Like any density function (defined for $t \geq 0$)

$$f(t) \geq 0 \text{ (for all } t \geq 0) \text{ and } \int_0^{\infty} f(t)dt = 1$$
- ◆ The functions F and f are related through

$$f(t) = dF(t) / dt \quad \text{and} \quad F(t) = \int_0^t f(s)ds$$

Part.2 .6

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Reliability and Failure (Hazard) Rate

- ◆ The reliability of a single module - $R(t)$
 - * $R(t) = \text{Prob}\{T > t\} = 1 - F(t)$
- ◆ The conditional probability that the module will fail at time t , given it has not failed before, is
$$\frac{\text{Prob}\{t \leq T \leq t+dt \mid T \geq t\}}{\text{Prob}\{T \geq t\}} = f(t)dt / (1-F(t))$$
- ◆ The **failure rate** (or **hazard rate**) of a component at time t , $\lambda(t)$, is defined as
 - * $\lambda(t) = f(t)/(1-F(t))$
- ◆ Since $dR(t)/dt = -f(t)$, we get $\lambda(t) = -1/R(t) \cdot dR(t)/dt$

Part.2 .7

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Constant Failure Rate

- ◆ If the module has a failure rate which is constant over time -
 - * $\lambda(t) = \lambda$
 - * $dR(t)/dt = -\lambda R(t)$; $R(0)=1$
- ◆ The solution of this differential equation is
$$R(t) = e^{-\lambda t}$$
$$f(t) = \lambda e^{-\lambda t}$$
$$F(t) = 1 - e^{-\lambda t}$$
- ◆ A module has a **constant failure rate** if and only if T , the lifetime of the module, has an **exponential distribution**

Part.2 .8

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Mean Time to Failure (MTTF)

◆ **MTTF** - expected value of the lifetime **T**

◆ Two ways of calculating **MTTF**

◆ **First way:** $MTTF = E[T] = \int_0^{\infty} t \cdot f(t) dt$

◆ **Second way:** $dR(t) / dt = -f(t)$

$$MTTF = -\int_0^{\infty} t \cdot dR(t) / dt \cdot dt = -tR(t) \Big|_0^{\infty} + \int_0^{\infty} R(t) dt = \int_0^{\infty} R(t) dt$$

◆ **If the failure rate is a constant λ**

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

$$MTTF = \int_0^{\infty} t \cdot \lambda e^{-\lambda t} dt = \int_0^{\infty} e^{-\lambda t} dt = \frac{1}{\lambda}$$

Part.2 .9

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Weibull Distribution - Introduction

◆ Most calculations of reliability assume that a module has a constant failure rate λ (or equivalently - an **exponential distribution** for the module lifetime **T**)

◆ There are cases in which this simplifying assumption is inappropriate

◆ **Example** - during the "infant mortality" and "wear-out" phases of the bathtub curve

◆ **Weibull distribution** for the lifetime **T** can be used instead

Part.2 .10

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Weibull distribution - Equation

- ◆ The Weibull distribution has two parameters, λ and b
- ◆ The density function of the component lifetime T :

$$f(t) = \lambda b t^{b-1} e^{-\lambda t^b}$$

- ◆ The failure rate for the Weibull distribution is

$$l(t) = \lambda b t^{b-1}$$

$l(t)$ is decreasing with time for $b < 1$, increasing with time for $b > 1$, constant for $b = 1$, appropriate for infant mortality, wearout and middle phases, respectively

Reliability and MTTF for Weibull Distribution

- ◆ Reliability for Weibull distribution is

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

- ◆ MTTF for Weibull distribution is

$$MTTF = \Gamma(1/b) / (\lambda b^{1/b})$$

($\Gamma(x)$ is the Gamma function)

- ◆ The special case $b = 1$ is the exponential distribution with a constant failure rate λ

Canonical Structures

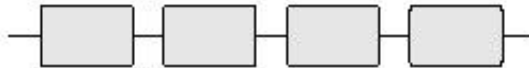
- ◆ A canonical structure is constructed out of **N** individual modules
- ◆ The basic canonical structures are
 - * A series system
 - * A parallel system
 - * A mixed system
- ◆ We will assume **statistical independence** between failures in the individual modules

Part.2 .13

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Reliability of a Series System

- ◆ A series system - set of modules so that the failure of any one module causes the entire system to fail



- ◆ **Reliability** of a series system - $R_s(t)$ - product of reliabilities of its **N** modules

$$R_s(t) = \prod_{i=1}^N R_i(t)$$

- ◆ $R_i(t)$ is the reliability of module **i**

Part.2 .14

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Series System - Modules Have Constant Failure Rates

- ◆ Every module i has a constant failure rate λ_i

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

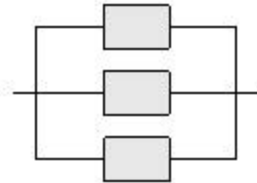
$$R_s(t) = e^{-\lambda_s t} = e^{-\sum \lambda_i t}$$

- ◆ $\lambda_s = \sum \lambda_i$ is the constant failure rate of the series system
- ◆ **Mean Time To Failure** of a series system -

$$MTTF_s = \frac{1}{\lambda_s} = \frac{1}{\sum \lambda_i}$$

Reliability of a Parallel System

- ◆ **A Parallel System** - a set of modules connected so that all the modules must fail before the system fails



- ◆ **Reliability** of a parallel system - $R_p(t)$

$$R_p(t) = 1 - \prod_{i=1}^N [1 - R_i(t)]$$

- ◆ $R_i(t)$ is the reliability of module i

Parallel System - Modules have Constant Failure Rates

- ◆ Module i has a constant failure rate, λ_i

$$R_i(t) = e^{-\lambda_i t} \qquad R_p(t) = 1 - \prod_{i=1}^N [1 - e^{-\lambda_i t}]$$

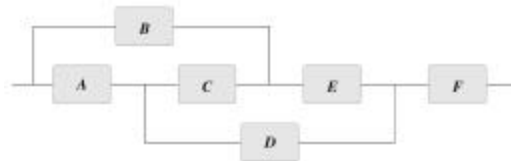
- ◆ **Example** - a parallel system with two modules

$$R_p(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1 + \lambda_2)t}$$

- ◆ **MTTF** of a parallel system with the same λ

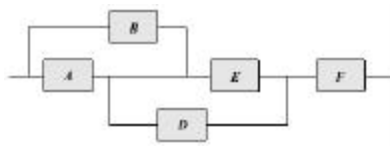
$$MTTF_p = \sum_{i=1}^N \frac{1}{\lambda_i}$$

Non Series/Parallel Systems

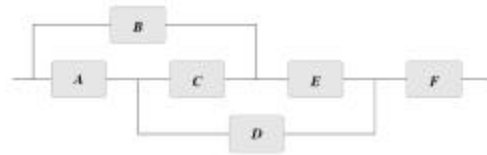


- ◆ Each path represents a configuration allowing the system to operate successfully, e.g., **ADF**
- ◆ The reliability can be calculated by expanding about a single module i :
- ◆ $R_{\text{system}} = R_i \text{ Prob}\{\text{System works} \mid i \text{ is fault-free}\} + (1 - R_i) \text{ Prob}\{\text{System works} \mid i \text{ is faulty}\}$
- ◆ Draw two new diagrams: in (a) module i is operational; in (b) module i is faulty
- ◆ Module i is selected so that the two new diagrams are closer to simple series/parallel structures

Expanding about C



(a)



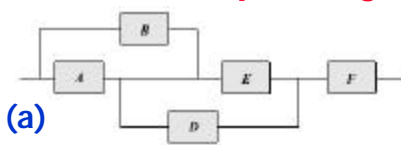
(b)

- ◆ The process of expanding can be repeated until the resulting diagrams are of the series/parallel type
- ◆ Figure (a) needs further expansion about E
- ◆ Figure (a) should not be viewed as a parallel connection of A and B, connected serially to D and E in parallel. Such a diagram will have the path BCDF which is not a valid path

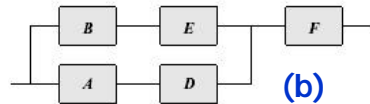
Part.2 .19

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Expanding about C and E



(a)



(b)

- ◆ $R_{\text{system}} = R_C \text{ Prob \{System works \mid C is operational\}} + (1 - R_C) R_F [1 - (1 - R_A R_D)(1 - R_B R_E)]$
- ◆ Expanding about E yields
- ◆ $\text{Prob \{System works \mid C is operational\}} = R_E R_F [1 - (1 - R_A)(1 - R_B)] + (1 - R_E) R_A R_D R_F$
- ◆ Substituting results in
- ◆ $R_{\text{system}} = R_C [R_E R_F (R_A + R_B - R_A R_B) + (1 - R_E) R_A R_D R_F] + (1 - R_C) [R_F (R_A R_D + R_B R_E - R_A R_D R_B R_E)]$
- ◆ Example: $R_A = R_B = R_C = R_D = R_E = R_F = R$
 $R_{\text{system}} = R^3 (R^3 - 3R^2 + R + 2)$

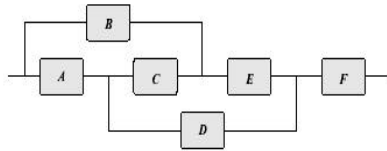
Part.2 .20

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Upper Bound on Reliability

- ◆ If structure is too complicated - derive upper and lower bounds on R_{system}
- ◆ An upper bound - $R_{system} \leq 1 - \prod (1 - R_{path_i})$
 - * R_{path_i} - reliability of modules in series along path i
 - * Assuming all paths are in parallel
- ◆ Example - the paths are ADF, BEF and ACEF
- ◆ $R_{system} \leq 1 - (1 - R_A R_D R_F)(1 - R_B R_E R_F)(1 - R_A R_C R_E R_F)$
- ◆ If $R_A = R_B = R_C = R_D = R_E = R_F = R$ then

$$R_{system} \leq R^3(R^7 - 2R^4 - R^3 + R + 2)$$



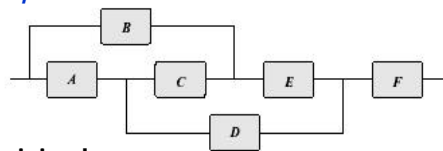
- ◆ Upper bound can be used to derive the exact expression: perform multiplication and replace every occurrence of R_i^j by R_i

Part.2 .21

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Lower Bound on Reliability

- ◆ A lower bound is calculated based on minimal cut sets of the system diagram
- ◆ A minimal cut set: a minimal list of modules such that the removal (due to a fault) of all modules will cause a working system to fail
- ◆ Minimal cut sets: F, AB, AE, DE and BCD
- ◆ The lower bound is
- ◆ $R_{system} \geq \prod (1 - Q_{cut_i})$
 - * Q_{cut_i} - probability that the minimal cut i is faulty (i.e., all its modules are faulty)
- ◆ Example - $R_A = R_B = R_C = R_D = R_E = R_F = R$



$$R_{system} \geq R^5(24 - R^5 + 9R^4 - 33R^3 + 62R^2 - 60R)$$

Part.2 .22

Copyright 2007 Koren & Krishna, Morgan-Kaufman

Example - Comparison of Bounds

- ◆ **Example** - $R_A=R_B=R_C=R_D=R_E=R_F=R$
- ◆ Lower bound here is a very good estimate for a high-reliability system

