Fault-Tolerant Computer Systems

Welcome to Lecture 2

Reliability modeling

Outline Lecture 2

- Basic probability theory
- Reliability
- MTTF = Mean Time To Failure
- Reliability block diagrams
- Series systems
- Parallel systems
- TMR
- m-of-n systems

Motivation

We use probability theory to gain insight into the properties of redundancy configurations and architectures of fault-tolerant systems.

Probability theory allow us to quantitatively assess the dependability of a fault-tolerant system in terms of

- ***Reliability***
- ***Availability***, and
- ***Safety***

Concepts in Probability

Let X denote the lifetime for a component.

$F(t) = P(X \le t)$ Distribution function

$R(t) = 1 - F(t) = P(X > t)$ Reliability function

$f(t) = \frac{\mathrm{d}}{\mathrm{d}t}F(t)$ Probability density function

The exponential distribution

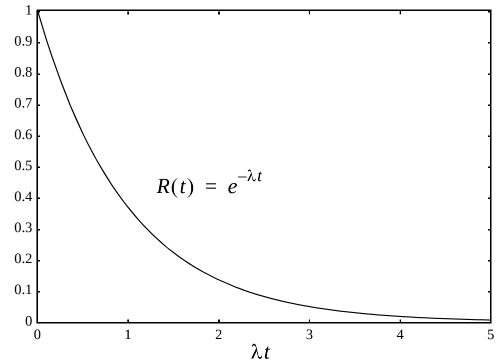
$F(t) = 1 - e^{-\lambda t}$ Distribution function

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

$f(t) = \lambda e^{-\lambda t}$ Probability density function

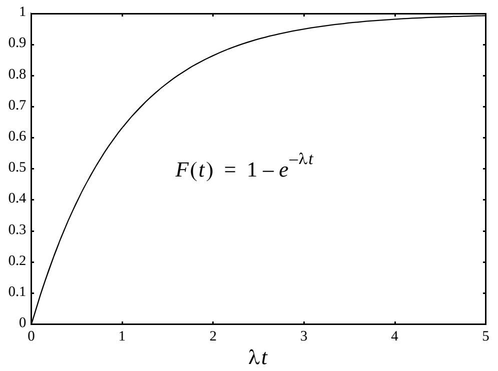
λ is the failure rate for the component and ***t*** is the time

Reliability function



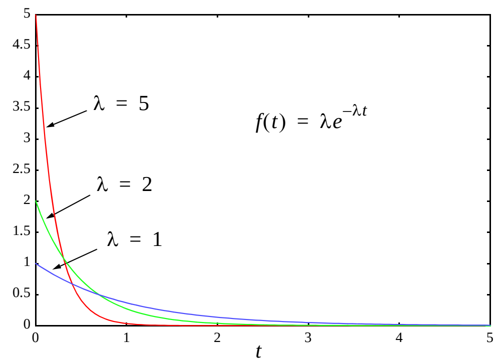
The exponential distribution

Distribution function



The exponential distribution

Probability density function



The exponential distribution

Failure rate function

$$h(t) = \frac{f(t)}{R(t)}$$

The exponential distribution has a constant failure rate:

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

The Bathtub Curve

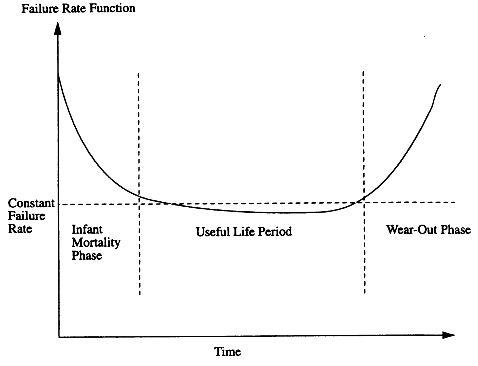


Figure 1.25: Illustration of the bathtub curve relationship. (From Barry W. Johnson, *Design and Analysis of Fault-Tolerant Digital Systems*, Addison-Wesley Publishing Company, Reading, Mass., 1989, p. 173.)

Mean Time To Failure (MTTF)

MTTF = expected time to failure

$$MTTF = \int_0^\infty R(t)dt$$

Proof of $MTTF = \int_0^\infty R(t)dt$

Let *X* denote the lifetime for the component

$$MTTF = E[X] = \int_0^\infty t \cdot f(t)dt = -\int_0^\infty t \cdot R'(t)dt$$

$$= -t \cdot R(t)\Big|_0^\infty + \int_0^\infty R(t)dt = \int_0^\infty R(t)dt$$

MTTF for the exponential distribution

$$MTTF = E[X] = \int_0^\infty e^{-\lambda t} dt = -\frac{e^{-\lambda t}}{\lambda}\Bigg|_0^\infty = \frac{1}{\lambda}$$

Example

What is the probability that a component with an exponentially distributed lifetime will survive the expected lifetime?

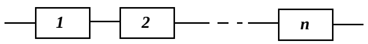
$$R\left(t = \frac{1}{\lambda}\right) = e^{-\left(\lambda \cdot \frac{1}{\lambda}\right)} = e^{-1} = 0,37$$

Only 37% of the components survive the expected lifetime.

Reliability Block Diagrams

- Series systems
- Parallel systems
- m-of-n systems

Series system with *n* components



Reliability block diagram

The reliability of the series system is

$$R_{serie} = R_1 \cdot R_2 \cdot \ldots \cdot R_n = \prod_{i=1}^{n} R_i$$

iff the component failures are <u>independent.</u>

Reliability of a series system

For the components $i = 1, 2, \ldots, n$ we define the events

$$A_i = \text{'component } i \text{ works'}$$

We denote the probability that the component *i* works

$$P(A_i) = R_i$$

If the events A_i are independent, the reliability of the series system is

$$R_{serie} = P(\text{'The system works'}) = P(A_1 \cap A_2 \cap \ldots \cap A_n)$$
$$= P(A_1) \cdot P(A_2) \cdot \ldots \cdot P(A_n)$$
$$= \prod_{i=1}^{n} R_i$$

Series system of components with exponentially distributed lifetimes

$$R_i = e^{-\lambda_i \cdot t}$$

$$R_{serie} = \prod_{i=1}^{n} e^{-\lambda_i \cdot t} = e^{-\sum_{i=1}^{n} \lambda_i \cdot t}$$

The failure rate of the series system is equal to the sum of the component failure rates.

This is called the *“parts count”* principle.

MTTF for a series system

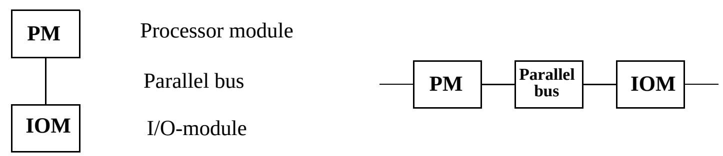
The failure rate for the series system is

$$\lambda_{sys} = \sum_{i=1}^{n} \lambda_i$$

The MTTF is then

$$MTTF = \frac{1}{\lambda_{sys}} = \frac{1}{\sum_{i=1}^{n} \lambda_i}$$

Example 1 - Series system



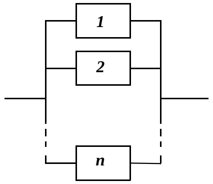
System architecture

Reliability block diagram

The reliability of the system is:

$$R_{sys} = e^{-(\lambda_{PM} + \lambda_{Parallelbus} + \lambda_{IOM}) \cdot t}$$

Parallel system with *n* components



Reliability block diagram

The reliability of a parallel system is

$$R_{par} = 1 - F_{par} = 1 - \prod_{i=1}^{n} F_i = 1 - \prod_{i=1}^{n} (1 - R_i)$$

Reliability of a parallel system

For the components $i = 1, 2, \ldots, n$ we define the events

$\overline{A_i}$ = 'component i has failed'

The probability that component i is broken can then be expressed as

$$P(\overline{A_i}) = F_i$$

If the events $\overline{A_i}$ are independent, the reliability for the parallel system is

$$R_{par} = 1 - P(\text{'The system has failed'}) = 1 - P(\overline{A_1} \cap \overline{A_2} \cap \ldots \cap \overline{A_n})$$
$$= 1 - P(\overline{A_1}) \cdot P(\overline{A_2}) \cdot \ldots \cdot P(\overline{A_n})$$
$$= 1 - \prod_{i=1}^{n} F_i = 1 - \prod_{i=1}^{n} (1 - R_i)$$

Examples

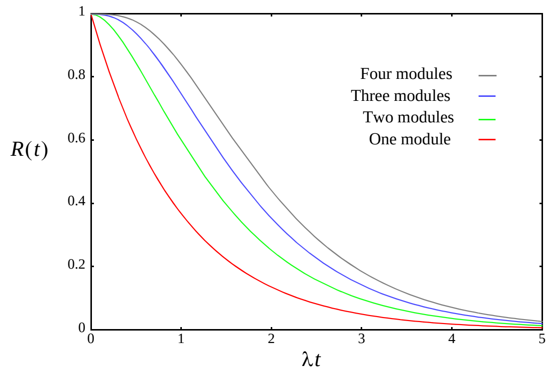
The reliability for parallel systems consisting of 2, 3 or 4 identical components with exponentially distributed lifetimes are:

2 modules: $R_{2p} = 1 - (1 - R_1)^2 = 1 - (1 - e^{-\lambda t})^2 = 2e^{-\lambda t} - e^{-2\lambda t}$

3 modules: $R_{3p} = 1 - (1 - R_1)^3 = 1 - (1 - e^{-\lambda t})^3 = 3e^{-\lambda t} - 3e^{-2\lambda t} + e^{-3\lambda t}$

4 modules: $R_{4p} = 1 - (1 - R_1)^4 = 1 - (1 - e^{-\lambda t})^4 = 4e^{-\lambda t} - 6e^{-2\lambda t} + 4e^{-3\lambda t} - e^{-4\lambda t}$

The reliability for parallel systems



MTTF for a parallel system with *n* components

Let *X* denote the lifetime of the system

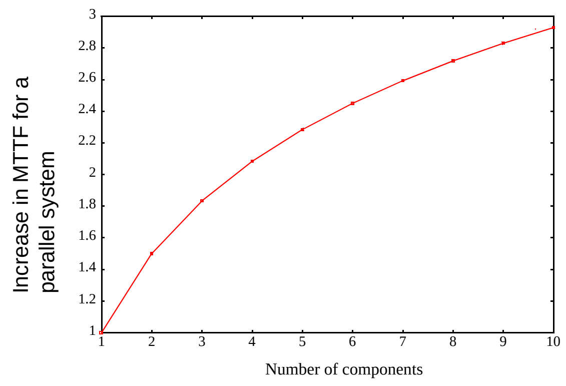
$$MTTF = E[X] = \int_0^\infty R(t)dt = \int_0^\infty 1-(1-e^{-\lambda t})^n dt$$

Make the substitution $u = 1 - e^{-\lambda t}$, $dt = \frac{1}{\lambda(1-u)} \cdot du$. We then obtain

$$MTTF = \frac{1}{\lambda} \cdot \int_0^1 \frac{1-u^n}{1-u} du = \frac{1}{\lambda} \cdot \int_0^1 \sum_{i=1}^{n} u^{i-1} du = \frac{1}{\lambda} \cdot \sum_{i=1}^{n} \frac{u^i}{i} \Big|_0^1$$

$$= \frac{1}{\lambda} \cdot \sum_{i=1}^{n} \frac{1}{i} \approx \frac{1}{\lambda} \cdot (\ln(n) + 0,57722)$$

MTTF for parallel systems

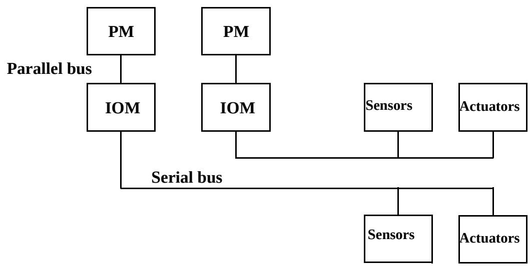


Example - MTTF for parallel systems

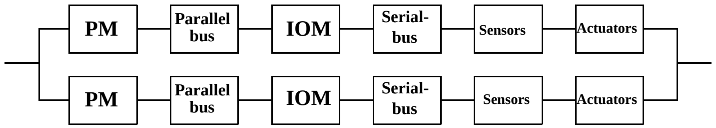
What is the MTTF for a parallel system consisting of 4 components if the MTTF for one component is $\frac{1}{\lambda}$?

$$MTTF = \frac{1}{\lambda} \cdot \sum_{n=1}^{4} \frac{1}{i} = \frac{1}{\lambda} \cdot \left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4}\right) = \frac{25}{12} \cdot \frac{1}{\lambda}$$

Example 2, A parallel system



Example 2, parallel system (cont'd.)



Reliability block diagram

The system reliability is:

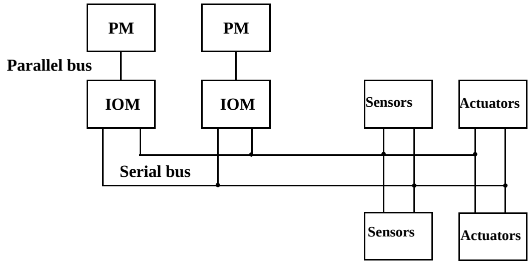
$$\lambda_{subsys} = \lambda_{PM} + \lambda_{parallelbus} + \lambda_{IOM} + \lambda_{serialbus} + \lambda_{sensors} + \lambda_{actuators}$$

$$R_{subsys} = e^{-\lambda_{subsys} \cdot t}$$

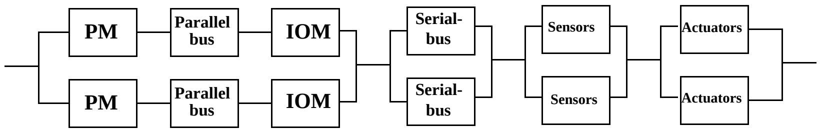
$$R_{sys} = 1 - (1 - R_{subsys})^2 = 1 - (1 - 2 \cdot R_{subsys} + R_{subsys}^2) = 2 \cdot R_{subsys} - R_{subsys}^2$$

$$= 2e^{-\lambda_{subsys} \cdot t} - e^{-2\lambda_{subsys} \cdot t}$$

Example 3



Example 3 (cont'd.)



Reliability block diagram

The reliability function

$$\lambda_1 = \lambda_{PM} + \lambda_{parallelbus} + \lambda_{IOM}$$

$$R_{sys} = (1 - (1 - e^{-\lambda_1 \cdot t})^2) \cdot (1 - (1 - e^{-\lambda_{serialbus} \cdot t})^2) \cdot (1 - (1 - e^{-\lambda_{sensors} \cdot t})^2) \cdot$$

$$(1 - (1 - e^{-\lambda_{actuators} \cdot t})^2)$$

Example m-of-n systems

Derive the reliability for a TMR system (= 2-of-3 system).
Let *R* denote the reliability for one module.

$$R_{TMR} = P(\text{'all modules are functioning'}) + P(\text{'exactly two modules are functioning'})$$

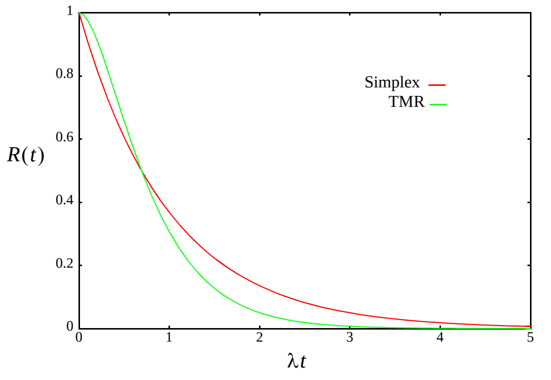
$$= R^3 + 3R^2 \cdot (1 - R) = 3R^2 - 2R^3$$

If the lifetimes of the modules are exponentially distributed, we obtain:

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

$$R_{TMR} = 3e^{-2\lambda t} - 2e^{-3\lambda t}$$

Reliability for TMR and Simplex systems



MTTF for a TMR-system

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

$$= -\frac{3}{2\lambda} \cdot e^{-2\lambda t}\Big|_0^\infty + \frac{2}{3\lambda} \cdot e^{-3\lambda t}\Big|_0^\infty =$$

$$= \frac{3}{2\lambda} - \frac{2}{3\lambda} = \frac{5}{6} \cdot \frac{1}{\lambda}$$

The MTTF for the TMR-system is only 5/6 of the MTTF for the simplex system!

m-av-n systems (cont'd.)

In general, we can write the reliability for an ***m-of-n*** system as

$$R_{\text{m-of-n}} = \sum_{i=m}^{n} \binom{n}{i} \cdot R^i (1-R)^{n-i}$$

m-of-n systems (cont'd)

Examples:

2-of-3 system

$$R_{\text{2-of-3}} = \sum_{i=2}^{3} \binom{3}{i} \cdot R^i (1-R)^{3-i} = \binom{3}{2} \cdot R^2 (1-R) + \binom{3}{3} \cdot R^3 = 3R^2 - 2R^3$$

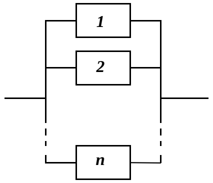
2-of-4 system:

$$R_{\text{2-of-4}} = \sum_{i=2}^{4} \binom{4}{i} \cdot R^i (1-R)^{4-i} = \binom{4}{2} \cdot R^2 (1-R)^2 + \binom{4}{3} \cdot R^3 (1-R) + \binom{4}{4} \cdot R^4$$

$$6R^2(1-R)^2 + 4R^3(1-R) + R^4 = 6R^2 - 8R^3 + 3R^4$$

Reliability block diagram for *m-of-n* systems

m-of-n



Reliability block diagram

Overview of Lecture 3

- More about hardware redundancy
- Case Study: HP's Non-Stop Advanced Architecture
- Preparations:

  Storey: Section 6.1, 6.3, 6.4, 6.5, 6.8

  Bernick et al., "Non-Stop Advanced Architecture"