Projeto com Circuitos Reconfiguráveis
Projeto de Sistemas em Chip

Fault Tolerant System Design

Prof. Daniel M. Muñoz Arboleda

FGA - UnB

Overview

- Introduction
  - Definition of fault tolerance
  - Applications of fault tolerant system design
- Fundamentals of dependability
  - dependability attributes: reliability, availability, safety
  - dependability impairments: faults, errors, failures
- **Some dependability evaluation techniques**
  - common measures: failure rate, MTTF, MTTR
- Redundancy techniques
  - space redundancy
    - hardware redundancy
    - information redundancy
    - software redundancy
  - time redundancy

Fault tolerance

- Targets development of a system which functions correctly in presence of faults
- Achieved by some kind of **redundancy**
  - redundancy allows either to detect or to mask a fault
- Fault detection/masking are followed by fault location, containment and recovery
  - the goal is to **reconfigure** the system to remove faulty components

Fault detection, localization, containment and recovery

Fault detection is the process of recognising that a fault has occurred

Fault location is the process of determining where a fault has occurred

Fault containment (contenção) is the process of isolating a fault and preventing its effect to propagate throughout a system

Fault recovery is the process of regaining operational status

Summary

- fault detection
  - identify that a fault has occurred
- fault location
  - find where the fault is
- fault containment
  - prevent propagation of the fault
- fault recovery
  - modify structure to remove faulty component
  - graceful degradation: continue operation with a degraded performance

Evaluation techniques

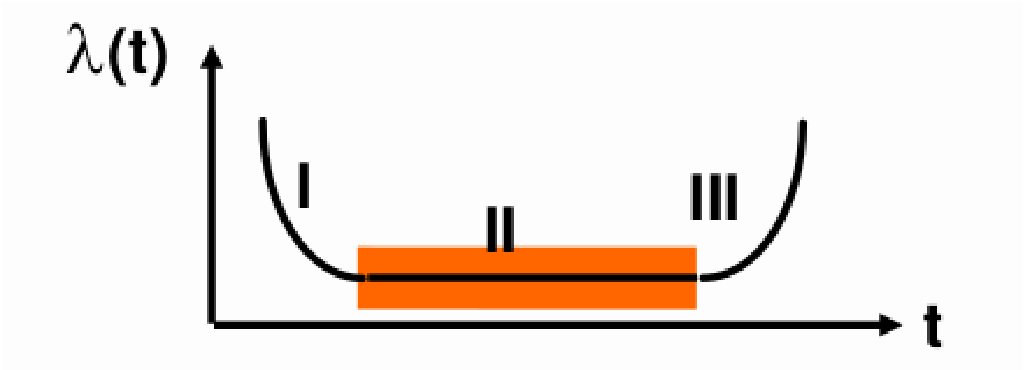
- Qualitative evaluation
  – aims to identify, classify and rank the failure modes, or event combinations that would lead to system failures
- Quantitative evaluation
  – aims to evaluate in terms of probabilities the attributes of dependability:
    - failure rate
    - mean time to failure
    - mean time to repair
    - mean time between failures
    - fault coverage

Failure rate

- failure rate
  - expected number of failures per time-unit
  - example
    - 1000 controllers working at t_0
    - after 10 hours: 950 working
    - failure rate for each controller:
      0.005 failures / hour
      (50 failures / 1000 controllers) / 10 hours

Failure rate

- typical evolution of λ(t) for hardware:



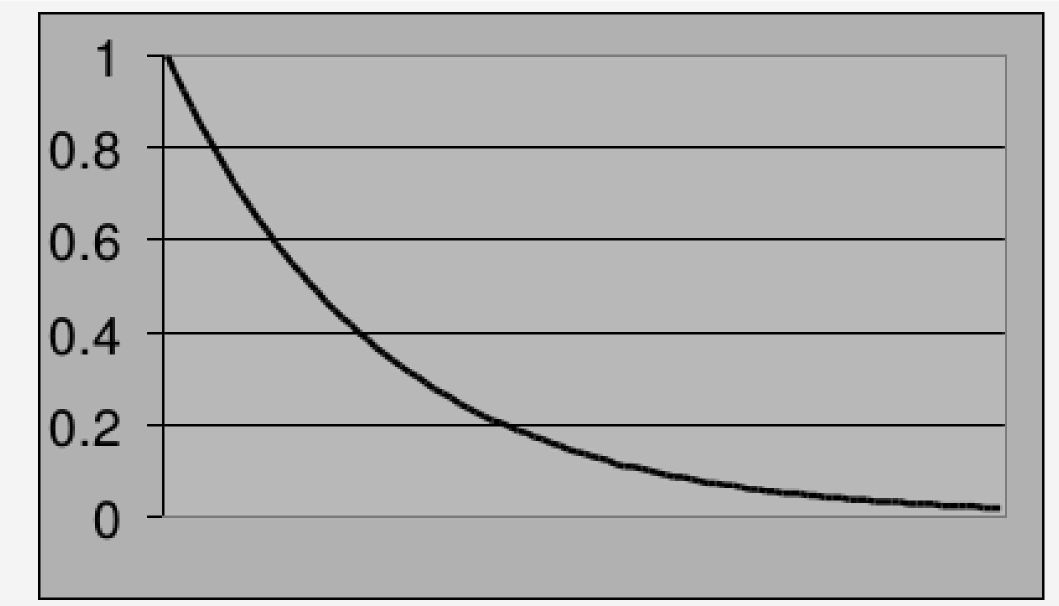
- bathtub: I infant mortality, II useful life, III wear-out
- for useful life period λ = constant, the reliability is given by

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

Exponential failure law

If λ is constant, $R(t)$ varies exponentially as a function of time

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



Failure rate calculation

- determined for components
  - systems: combination of components
  - λ of the system = sum of λ of the components
- determine λ experimentally
  - slow
    - e.g. 1 failure per 100 000 hours (=11.4 years)
  - expensive
    - many components required for significance
- use standards for λ

MTTF

- MTTF: mean time to failure
  - expected time until the first failure occurs

- If we have a system of N identical components and we measure the time t_i before each component fails, then MTTF is given by

$$MTTF = \frac{1}{N} \sum_{1=1}^{N} t_i$$

MTTF

- MTTF is meaningful only for systems which operate without repair until they experience a failure

- Most of mission-critical systems a undergo a complete check-up before the next mission
  - all failed redundant components are replaced
  - system is returned to fully operational state

- When evaluating reliability of such system, mission time rather then MTTF is used

MTTR

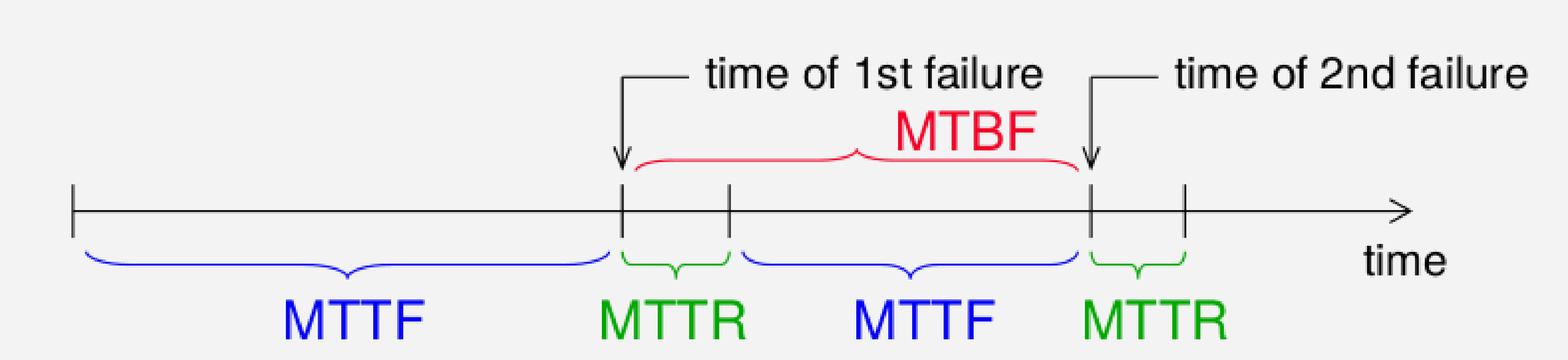
- MTTR: mean time to repair
  - expected time until repaired
- If we have a system of N identical components and i^{th} component requires time t_i to repair, then MTTR is given by

$$MTTR = \frac{1}{N} \sum_{1=1}^{N} t_i = \frac{1}{\mu}$$

- difficult to calculate
- determined experimentally
- normally specified in terms of repair rate μ, which is the average number of repairs that occur per time period

MTBF

- MTBF: mean time between failures
    - functional + repair
    - MTBF = MTTF + MTTR
  - small time difference: MTBF ≈ MTTF
  - conceptual difference

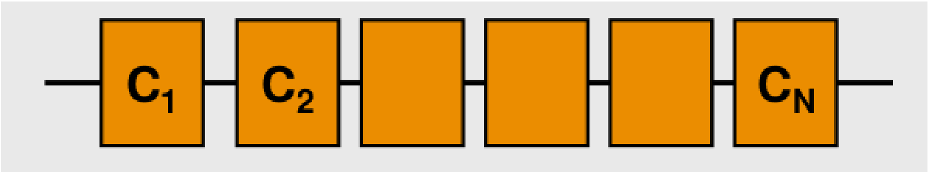


Dependability modelling

- up to now: λ and R(t) for components
- systems are sets of components
- system evaluation approaches:
  - reliability block diagrams (RBD)
  - Markov processes

Serial system

- system functions if and only if all components function



- If C_i are independent:

$$Rseries(t) = \prod R_i(t)$$

$$\lambda\, series(t) = \sum_{i=1}^{N} \lambda_i$$

Parallel system

- system works as long as one component works
- unreliabity: Q(t) = 1 – R(t)
- If C_i are independent:

$$Qparallel(t)=1-\prod_{i=1}^{N} Q_i(t)$$

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