CHALMERS TEKNISKA HÖGSKOLA
Institutionen för data- och informationsteknik
Avdelningen för nätverk och system

Exam in EDA122 (Chalmers) and DIT061 (GU) Fault-tolerant computer systems, Monday, January 9, 2012, 14.00 - 18.00

Teacher/Lärare: Johan Karlsson, tel 7721670

Allowed items/Tillåtna hjälpmedel: Beta Mathematics Handbook, Physics Handbook, English dictionaries

Language/Språk: Answers shall be given in English.

Solutions/Lösningar: Posted Wednesday, January 11, on the course homepage.

Exam review/Granskning: January 30 and February 6, at 12.15 in room 4128.

Grades:

Chalmers				
Points	0-23	24-35	36-47	48-60
Grades	Failed	3	4	5

GU				
Points	0-23	24-41	42-60	
Grade	Failed	G	VG	

Good Luck!

1. The system architecture for a fault-tolerant node in a distributed computer system is shown in Figure 1. The node consists of two processor modules (PMs) and two I/O modules (IOMs). The processor modules are connected to the I/O modules via two parallel bus. The I/O modules communicate with other nodes in the system via two serial buses.

   All modules operate in active redundancy. For silent failures, the system remains operational as long as at least one processor module, one I/O module and one parallel bus are working.

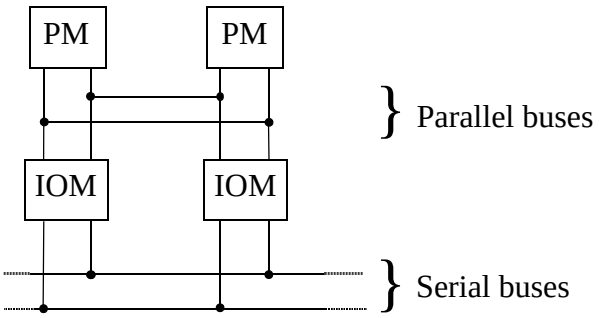


Figure 1.

a) Divide the system into the minimum number of fault containment regions required to achieve maximum reliability. Motivate the answer.

(2p)

b) Derive an expression for the reliability of the node. Assume that all failures are silent failures and that the function times of all modules are exponentially distributed. Use the following notation:

λ_1 failure rate for one processor module
λ_2 failure rate for one I/O-module

Disregard failures of the parallel buses and the serial buses.

(3p)

c) Assume that the processor modules has a coverage factor, *c*, for fulfilling the fail-silence assumption. Derive expressions for the reliability and the MTTF of the processor module subsystem. (A violation of the fail-silence assumption is considered as a subsystem failure.)

(3p)

d) Assume that a violation of the fail silent assumption leads to catastrophic (unsafe) failure of the node. Derive an expression for the *steady state* safety of the node under the assumption that coverage factor is *c* for the processor modules and ideal (*c* =100%) for the I/O modules. Disregard failures of the parallel buses and the serial buses. Use the same notation for the failure rates as in problem b).

(4p)

2. A fault-tolerant file server consists of two processors and three disk units. All units operate in active redundancy. The server is operational as long as at least one processor and one disk are working.

   Derive an expression for the availability of the file server. Assume that the function times of the processors and the disks are exponentially distributed. Let λ_p denote the failure rate for one processor and λ_d the failure rate for one disk. Assume that the fault coverage is ideal (100%) for the disks and c (< 100%) for the processors.

   The repair rate is μ_d for the disks and $2\mu_p$ for the processors in cases where a processor failure is covered. For non-covered failures, the repair rate is μ_p for the processors. In cases where a non-covered processor failure has occurred, assume that no additional processor failure can occur while the crashed processor is being repaired. In cases where multiple disk failures or multiple covered processor failures lead to a system failure, the system is restarted as soon as one processor and one disk are available.

   ***Hint*:** the use of a dedicated repair person for each subsystem implies that failures and repairs of the two subsystems occur independently of each other.

   (12p)

3. A fault tolerant computer system consists of three computer modules. Two modules are active and one is a standby module when all modules are working. The failure rate is λ for an active module and ρ for a standby module. The standby module assumes the role an active module whenever one of the active modules fails. A failed module is repaired with a repair rate of μ. A module that has been repaired becomes a standby module if the other two modules are working. The system is serviced by one repair person.

   a) Define a GSPN model for calculating the steady-state availability of the system.

      (6p)

   b) Draw the ***extended*** reachability graph of the GSPN.

      (6p)

4.

   a) Describe the basic principle of a CPU-exception.

      (2p)

   b) Describe two types of CPU-exceptions.
      ***Hint*:** The word type here refers to the type of errors that a CPU-exception detects.

      (2p)

   c) Describe the principle of an end-to-end checksum.

      (2p)

   d) Describe the principles of power supply monitoring.
      Hint: Describe how a power supply monitoring device interacts with a CPU and how the CPU reacts to a power supply failure.

      (2p)

5. In the paper “Basic Concepts and Taxonomy of Dependable and Secure Computing”, Avizienis et al. describe a method for characterizing service failure modes according to four viewpoints. Three of the viewpoints are *failure detectability*, *failure consistency* and *failure domain.*

   Describe these three viewpoints and explain why they are important.

   (6p)

6. Answer the following questions related to time-triggered real-time systems.

   a) What are the main ***advantages*** of a time-triggered system compared to an event-triggered system?

   (2p)

   b) What are the main ***disadvantages*** of a time-triggered system compared to an event-triggered system?

   (2p)

   c) Why is it simpler to achieve ***composability*** in a time-triggered system than in an event-triggered system?

   (2p)

7.

   a) Describe the principle of N-version programming.

   (1p)

   b) Describe the principle of the Recovery Blocks technique.

   (1p)

   c) N-version programming and Recovery Blocks use two different approaches to introduce design diversity. Describe the two approaches.

   (2p)

Mathematical Formulas

Laplace transforms

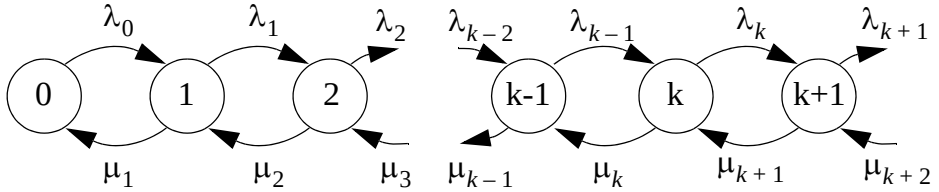
$e^{-a \cdot t}$	$\frac{1}{s+a}$
$t \cdot e^{-a \cdot t}$	$\frac{1}{(s+a)^2}$
$t^n \cdot e^{-a \cdot t}$	$\frac{n!}{(s+a)^{n+1}}$ $\quad n = 0, 1, 2, \ldots$
$\frac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a}$	$\frac{1}{(s+a)(s+b)}$
$\frac{e^{-a \cdot t} - e^{-b \cdot t} - (b-a)te^{-bt}}{(b-a)^2}$	$\frac{1}{(s+a)(s+b)^2}$

Reliability for *m* of *n* systems

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

$$\binom{n}{k} = \frac{(n)_k}{k!} = \frac{n(n-1) \cdot \ldots \cdot (n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

Steady-state probabilities for a general birth-death process



$$\Pi_1 = \frac{\lambda_0}{\mu_1} \cdot \Pi_0$$

$$\Pi_{k+1} = \frac{\lambda_k}{\mu_{k+1}} \cdot \Pi_k$$

$$\sum_{i=0}^{k} \Pi_i = 1$$

where Π_i = steady-state probability of state i