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 10, 2011, 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 Thursday, January 20, on the course homepage.

Exam review/Granskning: February 1 and 2, at 12.30 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. Consider a TMR system that consists of three computer modules and a single voter. A failure mode effects analysis (FMEA) of the TMR system is shown in Table 1. (For the sake of simplicity we consider only permanent hardware faults and a limited set of failure modes in this problem.)

   a) Draw a state diagram for a Markov chain model that can be used for calculating the safety and the reliability of the system. Assume that the failure mode of the system does not change once it has failed. Explain the state diagram shortly. (4p)

   b) Derive an expression for the steady-state safety of the system. (Clue: the system is in an unsafe failure state when the voter delivers erroneous results.) (2p)

   c) Derive an expression for the reliability of the TMR system. (6p)

Table 1. FMEA for the TMR system

Unit	**Failure mode**	**Failure effect**	**Failure rate**
Computer Module	Content failure (The module produces erroneous results.)	First module failure: The failure is masked by the voter. Second module failure: The voter produces no result (silent failure), which corresponds to a safe system failure. Third module failure: Same effect as for the second module failure. Note: The probability for two modules failing at the same time is assumed to be negligible.	λ_1
Voter	Silent failure (The system produces no results.)	Safe system failure	λ_2
Voter	Content failure (The system produces erroneous results.)	Unsafe (catastrophic) system failure.	λ_3

2. Derive an expression for the steady-state availability of a computer system consisting of **two** processors and **four** disk units. The system is considered operational as long as at least **one** processor and at least **one** disk are working correctly. Assume that the processors and disk units are repaired independently of each other and that all repair rates and failure rates are constant. Assume that there is **one** repair person for the processors and **one** repair person for the disks. A failed processor or disk is restarted immediately after it has been repaired. Use the following notations for the failure rates and the repair rates:

   λ_p failure rate for one processor
   λ_d failure rate for one disk unit
   μ_p repair rate for one processor
   μ_d repair rate for one disk units

   (12p)

3. Consider a computer system that consists of **three** computers. When all computers are working, **two** of them are active while **one** is a warm standby unit. The system is considered available if at least one computer is working. Assume that the function time of the computers is exponentially distributed. Let λ_1 denote the failure rate of an active computer and λ_2 the failure rate of a computer in standby mode, where $\lambda_1 > \lambda_2$. Assume that the repair time for one computer is exponentially distributed with a repair rate of μ. Assume ideal fault coverage and **one** repair person. If the system has failed (all computers are broken), it is restarted immediately when one computer has been repaired.

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

   (5p)

   b) State the marking(s) which corresponds to the event that the system is unavailable.

   (1p)

   c) Draw the reachability graph of the GSPN.

   (4p)

4. 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. Two of the viewpoints are *failure domain* and *failure consequences*. Describe the other two viewpoints.

   (6p)

5.

   a) Draw a diagram of the hardware architecture of Hewlett-Packard’s NonStop System. The diagram shall illustrate the hardware redundancy employed for Self-checked processors, LSU units, System Area Networks, Storage Adaptors, Disks and Network Adaptors. Write a short explanation of the diagram.

   (4p)

   b) Describe shortly how the self-checked processors are constructed in the NonStop system. Explain specifically the concepts of *slices* and *logical processors*.

   (2p)

6. In the course book, Neil Storey describes typical hazard analysis tasks which are conducted during the development of safety-critical computer systems. **Three** of these tasks are Preliminary hazard identification, Safety review and Independent safety audit. Describe the purpose and content of these tasks, and for what kind of systems they are performed.

   (6p)

7.

   a) Describe the purpose and principle of N-version programming.

   (2p)

   b) Describe the purpose and principle of the recovery block method.

   (2p)

   c) Describe four key differences between N-version programming and the recovery block method.

   (4p)

Mathematical Formulas

Laplace transforms

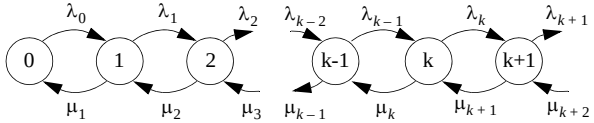
$e^{-a \cdot t}$	$\frac{1}{s+a}$
$t \cdot e^{-a \cdot t}$	$\frac{1}{(s+a)^2}$
$t^n \cdot e^{-a \cdot t}$	$\frac{n!}{(s+a)^{n+1}}$ $\quad n = 0, 1, 2, \ldots$
$\frac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a}$	$\frac{1}{(s+a)(s+b)}$
$\frac{e^{-a \cdot t} - e^{-b \cdot t} - (b-a)te^{-bt}}{(b-a)^2}$	$\frac{1}{(s+a)(s+b)^2}$

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