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

Exam in EDA122 (Chalmers) and DIT061 (GU) Fault-tolerant computer systems, Tuesday, August 16, 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 Monday, August 20, on the course homepage.

Exam review/Granskning: September 13 and 20, 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 system that consists of two computer modules that operate in a hot standby configuration. A simplified failure mode effects analysis (FMEA) of the system is shown in Table 1. As shown in the table, the effect of a computer module (CM) failure depends on whether the module is active or acts as a backup unit. (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 modes are stable, i.e., once a module has failed its failure mode will not change. Explain the meaning of each state in the state diagram shortly. (4p)

   b) Derive an expression for the steady-state safety of the system. (2p)

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

Table 1. Simplified FMEA for hot standby system

Unit	**Failure mode**	**Failure effect**	**Failure rate**
Active CM	Content failure (Module produces erroneous results.)	System delivers erroneous result - catastrophic (unsafe) system failure. No fail-over to backup module.	λ_1
Active CM	Silent failure (Module produces no results.)	Two alternatives: a) Fail-over to backup CM if backup CM is available. System continues to deliver correct service. b) Safe system failure if backup CM is not available.	λ_2
Backup CM	Content failure (Module produces erroneous results.)	System delivers correct service. No backup CM available.	λ_1
Backup CM	Silent failure. (Module produces no results.)	System delivers correct service. No backup CM available.	λ_2

2. Derive an expression for the steady-state availability of a computer system consisting of **two** processors and **three** 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 the hot standby system described in Problem 1.

   a) Define a GSPN model for calculating the steady-state availability of the system. Use the failure rates given in Table 1 and the following assumptions about repairs. The repair rate is ρ for an active computer module that causes a catastrophic (unsafe) system failure. The repair rate is μ for a backup module and an active module that causes a safe failure. Repairs are conducted by one person.

   (6p)

   b) Draw the reachability graph of the GSPN.

   (6p)

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) Show by an example how the *risk* of an hazardous event can be calculated. The risk should be expressed in deaths per person-years.

   (2p)

   b) In IEC 61508, risks are divided into four risk classes denoted I, II, III and IV. Describe the meaning of each of these risk classes.

   (4p)

6.

   a) Describe briefly the chain of events that led to the Ariane 5 Disaster on 4 June 1996. Which subsystems failed and what were the reasons for these failures?

   (4p)

   b) Describe four important lessons we can learn from the Ariane 5 Disaster.

   (4p)

7.

   a) Describe the concept of a Byzantine fault.

   (1p)

   b) Show by an example how a Byzantine fault can be tolerated by a distributed system that consists of four nodes.

   (3p)

Mathematical Formulas

Laplace transforms

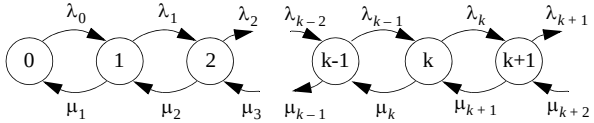
$e^{-a \cdot t}$	$\frac{1}{s+a}$
$t \cdot e^{-a \cdot t}$	$\frac{1}{(s+a)^2}$
$t^n \cdot e^{-a \cdot t}$	$\frac{n!}{(s+a)^{n+1}}$ $\quad n = 0, 1, 2, \ldots$
$\frac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a}$	$\frac{1}{(s+a)(s+b)}$
$\frac{e^{-a \cdot t} - e^{-b \cdot t} - (b-a)te^{-bt}}{(b-a)^2}$	$\frac{1}{(s+a)(s+b)^2}$

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