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 21, 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, August 22, on the course homepage.

Exam review/Granskning: September 11and 12, at 12.00 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 fault-tolerant system consisting of **three** computer modules. When the system is fault-free, two of the modules operate in active redundancy, while the third one serves as a ***cold*** standby module. The cold standby module is activated when any of the other two modules fails. The system remains operational as long as at least one module operates correctly.

   a) Assume that the life time of an active module is exponentially distributed with a failure rate λ. The failure rate of the standby module is negligible as long as it is in the cold standby state. The fault coverage is ideal (100%). Derive an expression for the reliability of the system.

   (6p)

   b) Derive an expression for the MTTF of the system.

   (4p)

   c) Derive an expression for the expected time to the first node failure.

   (2p)

   Hint: Useful Laplace transforms are listed on the last page of the exam paper.

2. Derive an expression for the steady-state availability of a system consisting of three computer modules operating as a triple modular redundant system. Assume that the life times of the modules, as well as their repair times, are exponentially distributed. Let λ denote the failure rate and μ the repair rate for one module. The fault coverage is ideal (100%). If the system fails (which happens if two or more modules fail), the system is not restarted until all nodes are repaired. To simplify the calculation, assume that no failures occur when the system is down. Assume that repairs are conducted by one service technician.

   (12p)

3. A file sever consists of two processors and two disk units. Let λ_p denote the failure rate and μ_p the repair rate for one processor. Let λ_d denote the failure rate and μ_d the repair rate of one disk unit. The server is operational when at least one processor and one disk are working. Repairs are conducted by one service technician.

   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. In the paper “Basic Concepts and Taxonomy of Dependable and Secure Computing”, Avizienis et al. provide a taxonomy of faults.

   a) They identify three major partially overlapping groups of faults. Describe these three major groups of faults.

   (3p)

   b) The three major groups of faults mentioned in problem a) are derived from 8 *elementary fault classes*, or *viewpoints*. Three of these of viewpoints are i) *Phase of creation or occurrence,* ii) *Intent* and iii) *Persistence*. Each of these viewpoints contain two subclasses. Describe the subclasses of each of these three viewpoints.

   (3p)

5. Answer the following questions related to Hewlett-Packard’s NonStop Computers.

   a) Several generations of the NonStop Computers have relied on the concepts of self-checking processors. Before the introduction of the NonStop Advanced Architecture (NSAA) in 2005, NonStop systems relied on tightly lock-stepped microprocessors for error detection in order to implement self-checking processors. This technique was abandoned in the NSAA architecture. State three reasons why tightly lock-stepped microprocessors no longer is a viable approach for implementing self-checking processors.

   (3p)

   b) How are self-checking processors implemented in the NonStop Advanced Architecture?

   (3p)

   c) The NonStop Advanced Architecture supports both dual modular redundancy (DMR) and triple modular redundancy (TMR). Compare these two techniques with respect to their ability to tolerate faults.

   (2p)

6. Consider a distributed system consisting of four nodes which execute the interactive consistency algorithm for ordinary messages proposed by Lamport, Shostak and Pease. Assume that the system uses a broadcast bus for communication. Calculate the number of messages (broadcasts) that are exchanged between the nodes in order to reach consensus on one value. Explain the calculation, for example, by drawing a figure of how the messages are exchanged.

   (6p)

7. Explain the concept of *risk reduction* and the associated terms *basic risk, tolerable risk*, *residual risk* (or *achieved risk*) and *external risk reduction.*

   (4p)

Mathematical Formulas

Laplace transforms

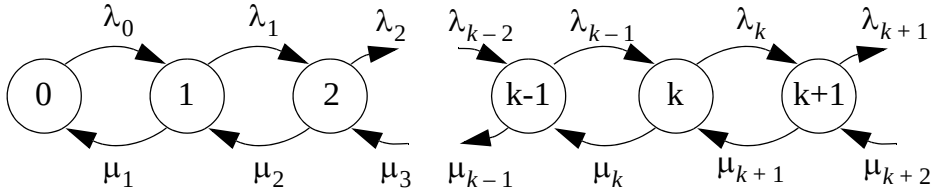
$e^{-a \cdot t}$	$\frac{1}{s+a}$
$t \cdot e^{-a \cdot t}$	$\frac{1}{(s+a)^2}$
$t^n \cdot e^{-a \cdot t}$	$\frac{n!}{(s+a)^{n+1}}$ $\quad n = 0, 1, 2, \ldots$
$\frac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a}$	$\frac{1}{(s+a)(s+b)}$
$\frac{e^{-a \cdot t} - e^{-b \cdot t} - (b-a)te^{-bt}}{(b-a)^2}$	$\frac{1}{(s+a)(s+b)^2}$

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