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 17, 2010, 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 18, on the course homepage.

Exam review/Granskning: September 14 and 15, 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 fault-tolerant unit (FTU) in a distributed system that consists of **three** computer nodes operating in active redundancy. The FTU remains operational as long as at least one node operates correctly.

   a) Assume that the operation time of each node is exponentially distributed with a failure rate of λ and a fault coverage of 100%. Derive an expression for the reliability of the FTU.

   (4p)

   b) Derive an expression for the MTTF of the FTU for the assumptions given in problem a).

   (3p)

   c) Assume that the coverage is ideal for the first node failure and c (c<1) for the second node failure. Derive an expression for the reliability of the FTU.

   (5p)

2. Consider a fault-tolerant unit (FTU) that consists of **two** computer nodes operating in active redundancy.

   a) Assume that the operation time of each node with respect to permanent hardware faults are exponentially distributed with a failure rate of λ. The nodes are repaired one at a time (one repair person) with a constant repair rate of μ. The FTU is restarted after a crash as soon as one node is available. Derive an expression for the steady-state availability of the FTU with respect to permanent faults. Assume ideal coverage.

   (4p)

   b) Assume that the nodes in addition to the permanent faults are exposed to transient faults with a constant failure rate of 10λ. The nodes are automatically repaired without human intervention when a transient fault occurs provided that only one of the nodes have failed (the remaining node assists the faulty node in the recovery). Assume that the repair rate for the automatic repair is 100μ. Manual repair is necessary if the FTU crashes (both nodes have failed) and whenever a permanent fault occurs. The nodes are then repaired one at a time (one repair person) with a constant repair rate of μ. The FTU is restarted after a crash as soon as one node is available. The failure rate for permanent faults is λ. Derive an expression for the steady-state availability of the FTU taking into account both permanent and transient faults. Assume ideal coverage.

   (8p)

3. Consider a distributed computer system that consists of **three** processor nodes operating in hot-standby redundancy. Define and draw a GSPN model for calculating the steady-state availability of the system. Assume that the operation time of the nodes is exponentially distributed with a failure rate λ. The repair time for one processor node is exponentially distributed with a repair rate of μ. The system is considered operational as long as at least one node is working. Assume ideal coverage and two repair persons. (No more than two nodes can be under repair at the same time.) State the marking(s) which corresponds to the event that the system is unavailable.

(8p)

4. Define and explain the follow concepts related to risk and hazard analysis

   a) Describe the principle of Failure Mode Effects Analysis (FMEA)

   (2p)

   b) Describe the main strengths and weaknesses of FMEA

   (2p)

   c) Describe the concept and purpose of a safety case

   (2p)

   d) Give four examples of information items that should be included in a safety case

   (2p)

5.

   a) Describe the nature of a Byzantine failure.

   (2p)

   b) Consider a distributed system consisting of four nodes that executes the ICA algorithm (a.k.a. the OM algorithm, OM =oral messages) proposed by Lamport, Pease and Shostak. (This system can tolerate one Byzantine failure.) Assume that nodes exchange information via point-to-point messages. Calculate the total number of messages required for reaching agreement on one value. Explain and motivate your calculations. (Hint: The sender of the value acts as the general in the ICA algorithm.)

   (6p)

6. The Time-Triggered Architecture supports two physical interconnection topologies for implementing clusters. Describe these topologies and their advantages and drawbacks.

(6p)

7.

   a) Why are failure mode assumptions important in the design of fault-tolerant distributed systems?

   (2p)

   b) Give an example of a failure mode assumption that requires *3f+1* nodes to tolerate *f* node failures. Explain why this failure mode assumption requires *3f+1* nodes.

   (2p)

   c) Give an example of a failure mode assumption that require *f+1* nodes to tolerate *f* node failures. Explain why this failure mode assumption requires *f+1* nodes.

   (2p)

Mathematical Formulas

Laplace transforms

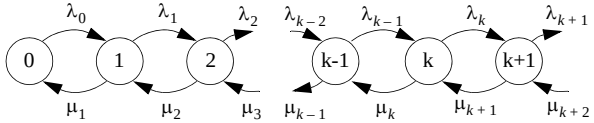
$e^{-a \cdot t}$	$\frac{1}{s+a}$	
$t \cdot e^{-a \cdot t}$	$\frac{1}{(s+a)^2}$	
$t^n \cdot e^{-a \cdot t}$	$\frac{n!}{(s+a)^{n+1}}$	$n = 0, 1, 2, ...$
$\frac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a}$	$\frac{1}{(s+a)(s+b)}$	
$\frac{e^{-a \cdot t} - e^{-b \cdot t} - (b-a)te^{-bt}}{(b-a)^2}$	$\frac{1}{(s+a)(s+b)^2}$	

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