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

Exam in EDA122/EDA121 (Chalmers) and DIT061/DIT060 (GU) Fault-tolerant computer systems for DCMAS, D5, E5, Z5, GU, Erasmus and Graduate students, Tuesday, August 18, 2009, 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 19, on the course homepage.

Exam review/Granskning: September 1 and 2, at 12.30 in room 4128.

NOTE: THERE ARE TWO VERSIONS OF PROBLEM 3 - ONE FOR EDA122/DIT061 AND ONE FOR EDA121/DIT060.

MAKE SURE YOU SOLVE THE APPROPRIATE PROBLEM!!!

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	

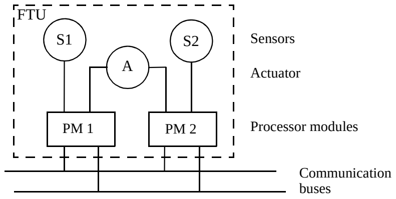
Good Luck!

1. Figure 1 shows the hardware architecture for a fault-tolerant unit (FTU) in a distributed control system. The FTU consists of two processor modules, two sensors and one actuator. The processor modules operate as a hot-standby pair where PM1 is active from system start and PM2 is the standby unit.

   a) Divide the FTU including the communication buses into an appropriate number of error containment regions. Motivate you answer. (3p)

   b) Derive an expression for the reliability of the FTU. Assume that the life times of the components are exponentially distributed with the following failure rates:
   λ_p failure rate for one processor module
   λ_s failure rate for one sensor
   λ_a failure rate for the actuator
   Assume ideal coverage. Neglect the failure rate of interconnections and buses. (4p)

   c) Derive an expression for the reliability of the FTU under the following assumptions: The sensors has a failure mode that cannot be detected. If such a failure occurs in S1, then the FTU fails immediately. The probability that a sensor failure is detected is *c*. The coverage for faults occurring in the processor modules is ideal (100%). (5p)



Figur 1

2. Consider a fault-tolerant unit (FTU) that consists of **two** computer nodes operating in a hot-standby configuration. Assume that the life time of the nodes are exponentially distributed with the fault rate λ. The fault coverage is c (c<1) for faults occurring in the primary node and ideal (100%) for faults that occur in the spare node. The nodes are repaired one at a time (one repair person) with a constant repair rate, which is 2μ when the fault is covered, and μ when the fault is non-covered. The FTU is restarted after a crash as soon as one node is available. Make the following simplifying assumptions: i) The fault coverage is ideal for the standby node also when it is active, i.e. when the primary node has failed because of a covered fault. ii) the spare does not fail while the primary node is being repaired after a non-covered fault.

   a) Derive an expression for the steady-state probability that the FTU is down because of a non-covered fault. (4p)

   b) Derive an expression for the steady-state probability that both nodes function correctly. (4p)

   c) Derive an expression for the steady-state availability of the FTU. (4p)

3. THIS PROBLEM SHALL BE SOLVED ONLY BY STUDENTS TAKING EDA122/DIT061 (GIVEN 2008/2009).

   Draw a GSPN model that can be used for calculating the reliability of a cold standby system consisting of one active unit and one spare unit where the dormancy factor is k, the failure rate for an active module is λ and and the repair rate for one module is μ. Assume perfect fault coverage. (6p)

3. THIS QUESTION SHOULD BE ANSWERED ONLY BY STUDENTS TAKING EDA121/DIT060 (GIVEN 2006/2007 AND EARLIER).

   Draw and explain the *dependability and security tree* as it is defined in “Basic Concepts and Taxonomy of Dependable and Secure Computing” by Avizienis et al. *Clue:* the main branches of the dependability and security tree are *attributes*, *threats* and *means*. (6p)

4. Answer the following questions related to the Time-Triggered Architecture (TTA).

   a) What are the main hardware and software components of a TTA-node? (2p)

   b) TTA supports two different physical interconnection topologies. What are these topologies called and what are their main characteristics with respect to fault tolerance? (4p)

   c) Where in a TTA system is a *guardian* located and what does it do? *Clue*: the location of guardian depends on the interconnection topology. (2p)

5.

   a) Describe the two main objectives of fault injection. (Clue: these objectives are included in the dependability and security tree.) (4p)

   b) Describe two advantages and two drawbacks of *software implemented fault injection* (SWIFI). (4p)

6.

   a) Describe informally the meaning of the Byzantine generals problem and the concept of a Byzantine failure. (4p)

   b) Consider a distributed system consisting of four nodes which execute the interactive consistency algorithm for ordinary messages proposed by Lamport, Shostak and Pease. Calculate the number of messages 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. Describe briefly the purpose and the main conclusion of the experiment described in the paper “A Large Experiment in N-version Programming” by Knight, Leveson and St. Jean. (4p)

Mathematical Formulas

Laplace transforms

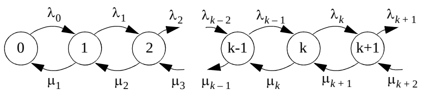
$e^{-a \cdot t}$	$\frac{1}{s+a}$	
$t \cdot e^{-a \cdot t}$	$\frac{1}{(s+a)^2}$	
$t^n \cdot e^{-a \cdot t}$	$\frac{n!}{(s+a)^{n+1}}$	$n = 0, 1, 2, ...$
$\frac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a}$	$\frac{1}{(s+a)(s+b)}$	
$\frac{e^{-a \cdot t} - e^{-b \cdot t} - (b-a)te^{-bt}}{(b-a)^2}$	$\frac{1}{(s+a)(s+b)^2}$	

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