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, D4, E4, Z4, GU, Erasmus and Graduate students, Monday, January 12, 2008, 08.30 - 12.30

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, January 14, on the course homepage.

Exam review/Granskning: February 2 and 3, 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 architecture of a fault-tolerant computer node in a distributed control system. The node is intended for use in a satellite and consists of two redundant processor modules, PM1 and PM2, and two redundant sensors, S1 and S2. The system operates in cold stand-by redundancy, where PM1 and S1 are the primary units and PM2 and S2 the backup units.

   a) Divide the system into an appropriate number of error containment regions. Motivate the answer.
   (2p)

   b) How many primary independent subsystems does the system consist of? Describe these subsystems.
   (1p)

   c) Assume that the life times of the processor modules and sensors are exponentially distributed with a failure rate of λ_p for an active (hot) processor module and λ_s for an active sensor. The failure rate of the buses is neglible. The dormancy factor is 10 for the processor modules and 1 for the sensors. (This means that the failure rate of a cold processor module is ten times lower than the failure rate of an active processor module, while the failure rate is the same for cold and active sensors.) Derive an expression for the reliability of the node. Assume ideal coverage (c = 1).
   (5p)

   d) Derive an expression for the reliability of the node under the following assumptions: Sensor S1 has a failure mode which cannot be detected by the processor modules. Such a sensor failure will cause the entire system to fail immediately. The probability of this failure mode, given that S1 fails, is 1- c. The fault coverage for faults occurring in the processor modules is perfect. The dormancy factors are the same as in problem c).
   (4p)

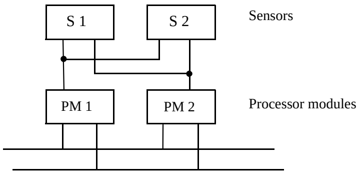


Figure 1

2. Consider a system with two processor modules that operate in active redundancy. Assume that the fault coverage is perfect if a module fails while the other module is operational. If a module fails while the other module is being repaired, then an attempt is made to shutdown the system safely. The probability for a *safe* shutdown is c, and hence the probability for an *unsafe* shutdown is (1-c). After a shut down, the system becomes available again as soon as one module has been repaired. Assume that the modules have exponentially distributed function times and repair times. The repair rate for bringing the system from the *unsafe* shutdown state to an operational state in which one module works is ρ. Otherwise, the repair rate for a module is μ. The failure rate of a module is λ. Assume that repairs are conducted by one person.

   a) Derive an expression for the steady state probability for the event that the system is in the *unsafe* shutdown state.
   (10p)

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

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

   Figure 2 shows a GSPN model of a cold standby system with a dormancy factor k, a "hot" failure rate λ and and a repair rate μ. Derive the reachability graph of the GSPN model.

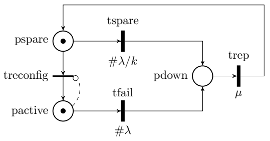


Figure 2

(6p)

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

   Consider the typical tasks performed during a hazard analysis as described in the book by N. Storey. Three of these tasks are: *Preliminary hazard analysis (PHA)*, *System hazard analysis* and *Safety review*. Describe how these tasks are related to each other and their objectives.
   (6p)

4. Describe how the IEC 61508 standard defines *safety integrity levels* (SILs).
   (4p)

5.
   a) Describe the two main objectives of fault injection. (Clue: these objectives are included in the dependability and security tree.)
   (4p)

   b) Describe the two main approaches to *software implemented fault injection* (SWIFI).
   (2p)

6. Describe the system-level error detection mechanisms employed in the MARS system. In what way do these mechanisms depend on each other? (Clue: there are two such mechanisms, one is based on time redundancy and one on checksums.)
   (6p)

7. Assumptions about the failure modes of computer nodes are important in the design of fault tolerant distributed systems. Describe the meaning of the following failure modes:

   a) Value failure

   b) Timing failure

   c) Silent failure

   d) Send omission failure

   e) Signalled failure

   f) Blocking failure
   (6p)

8. Describe and explain the two main principles of system recovery.
   (4p)

9. Describe the main principles for how fault tolerance is achieved in the flight control system of the JAS Gripen Aircraft. Focus your description on how the system deals with sensor faults and processor faults.
   (4p)

Mathematical Formulas

Laplace transforms

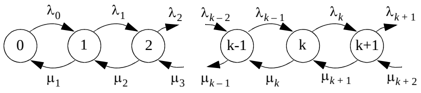
$e^{-a \cdot t}$	$\frac{1}{s+a}$	
$t \cdot e^{-a \cdot t}$	$\frac{1}{(s+a)^2}$	
$t^n \cdot e^{-a \cdot t}$	$\frac{n!}{(s+a)^{n+1}}$	$n = 0, 1, 2, ...$
$\frac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a}$	$\frac{1}{(s+a)(s+b)}$	
$\frac{e^{-a \cdot t} - e^{-b \cdot t} - (b-a)te^{-bt}}{(b-a)^2}$	$\frac{1}{(s+a)(s+b)^2}$	

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*