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

Exam in EDA122 (Chalmers) and DIT061 (GU) Fault-tolerant computer systems, Wednesday, October 20, 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 Thursday, October 21, on the course homepage.

Exam review/Granskning: November 15 and 16, 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 network interface for time-triggered communication consisting of a communication controller and a bus guardian. Table 1 show a failure mode effects analysis for the network interface.

   a) Draw a state diagram for a Markov chain model that can be used for calculating the safety and the reliability of the network interface. Assume that the failure mode of a unit does not change after the unit has failed. (E.g., the failure mode of a bus guardian cannot change from a stuck-open failure to a stuck-closed failure.) Motivate and explain the diagram.

   (4p)

   b) Derive and explain an expression for the steady-state safety of the network interface. The interface is in an unsafe state when it has failed in a catastrophic way.

   (2p)

   c) Derive an expression for the reliability of the network interface. Assume that the interface is working if the communication controller works correctly and the bus guardian has failed in the stuck-open mode, and (of course) when no failures have occurred. To simplify the expression, assume that $\lambda_1 = \lambda_3$ and $\lambda_2 = \lambda_4$

   (6p)

Table 1

Unit	**Failure mode**	**Failure effect**	**Failure rate**
Communication Controller	Silent failure	Safe interface failure	λ_1
Communication Controller	Timing failure	Leads to a catastrophic interface failure if the bus guardian has failed in stuck-open mode (see below), otherwise to a safe interface failure The communication controller violates the communication schedule by sending messages at incorrect points in time.	λ_2
Bus Guardian	Stuck-open failure	The bus guardian fails to prevent the communication controller from sending message at incorrect points in time. Leads to a catastrophic interface failure if the communication controller exhibits a timing failure.	λ_3
Bus Guardian	Stuck-closed failure	The bus guardian blocks the communication controller from accessing the bus. Leads to a safe interface failure.	λ_4

2. A fault-tolerant file server consists of two processors and two disk units, which are connected via a dual redundant storage area network, see figure 1. All units operate in active redundancy. The server is operational as long as at least one processor, one disk and one network link are working correctly.

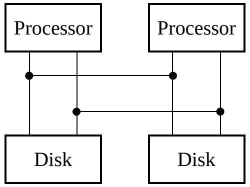


Figure 1

a) Divide the system into an appropriate number of fault containment regions. Motivate the answer.

(2p)

b) Derive an expression for the availability of the file server. Assume that the function times of the processors and the disks are exponentially distributed. Let λ_p denote the failure rate for one processor and λ_d the failure rate for one disk. The failure rate of the network links is low compared to the failure rates of the processors and disks and can therefore be neglected. Assume that the fault coverage is ideal (100%) for all units.

With respect to repairs, assume that there is one repair person for the processors and one repair person for the disks. The repair rate is μ_p for a processor and μ_d for a disk. If both processors fail, the processor subsystem is restarted as soon as one processor has been repaired. If both disks fail, the disk subsystem is not restarted until both disks have been repaired. Hence, the disks and the processors have different repair policies.

Hint: the use of dedicated repair persons for each subsystem implies that failures and repairs of the two subsystems occur independently of each other.

(10p)

3. Consider a computer system that consists of **two** computers operating as a hot standby system. Define a GSPN model for calculating the steady-state availability of the system. The standby computer has a simpler design than the primary computer, and thus it has a lower failure rate than the primary computer. The system is considered “available” if at least one computer is working. Assume that the life time of the computers is exponentially distributed. Let λ_1 denote the failure rate of the primary computer and λ_2 the failure rate of the standby computer. Assume that the repair times is exponentially distributed with a repair rate of μ for both the primary computer and the standby computer. Assume ideal coverage and **one** repair person. If both computers fails, the system is restarted immediately when one computer has been repaired. An on-going repair of one of the computers is **not** pre-emptied when the other computer fails.

State the marking(s) which corresponds to the event that the system is unavailable. Draw the reachability graph of GSPN

(10p)

4. In the paper “Basic Concepts and Taxonomy of Dependable and Secure Computing”, Avizienis et al. describe a method to characterize service failure modes according to four viewpoints. One of the viewpoints is the failure domain. Describe the different ways in which a failure mode can be characterized in the failure domain.

(6p)

5.

a) Describe the main features of the Hazard and Operability Study (HAZOP) technique.

(4p)

b) Describe the concept of ALARP (as low as reasonably practicable) and how it is used in risk analysis.

(4p)

6. Answer the following questions related to the Time-triggered Architecture (TTA).

   a) How does TTA provide temporal firewalls between different nodes?
   (2p)

   b) Describe the design principle and overall structure of the communication network interface (CNI). Describe the principles for data flow and control flow.
   (4p)

   c) What is an elementary unidirectional data-flow interface?
   (2p)

7. Describe how design diversity is used in the fly-by-wire system for the Airbus A340/A330 aircraft.
   (4p)

Mathematical Formulas

Laplace transforms

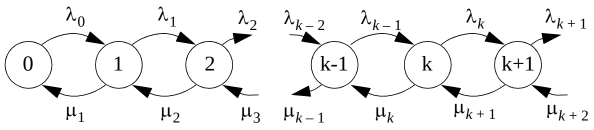
$e^{-a \cdot t}$	$\frac{1}{s+a}$	
$t \cdot e^{-a \cdot t}$	$\frac{1}{(s+a)^2}$	
$t^n \cdot e^{-a \cdot t}$	$\frac{n!}{(s+a)^{n+1}}$	$n = 0, 1, 2, ...$
$\frac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a}$	$\frac{1}{(s+a)(s+b)}$	
$\frac{e^{-a \cdot t} - e^{-b \cdot t} - (b-a)te^{-bt}}{(b-a)^2}$	$\frac{1}{(s+a)(s+b)^2}$	

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*