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

Exam in EDA122 (Chalmers) and DIT061 (GU) Fault-tolerant computer systems, Monday, January 11, 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, January 13, on the course homepage.

Exam review/Granskning: February 2 and 3, 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. A fault-tolerant computer for a satellite launcher consists of two processor modules (PM) and two I/O-modules (I/O). The modules are interconnected via two parallel buses as shown in Figure 1. All subsystems (PM modules, I/O modules and the buses) use hot standby-redundancy to achieve fault-tolerance.

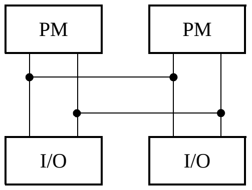


Figure 1

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

(3p)

b) Derive an expression for the reliability of the system. Assume that the life times of the modules and the buses are exponentially distributed. Let λ_p, $\lambda_{i/o}$, and λ_b, respectively, denote the failure rates for one processor module, one I/O module and one bus. Assume that the fault coverage for the primary processor module is *c* ($c < 1$) and that the fault coverage is ideal (100%) for the stand-by processor module, the I/O-modules and the parallel buses.

(6p)

c) Derive an expression for the MTTF of the PM module subsystem.

(3p)

2. Derive an expression for the steady-state availability of a computer system consisting of two processors and two disk units. The system is operational as long as at least one processor and at least one disk are working correctly. Assume that the processors and disk units are repaired independently of each other and that all repair rates and failure rates are constant. Assume that there is one repair person for the processors and one repair person for the disks. In case both processors fail, the processor subsystem is not restarted until both processors have been repaired. The same policy applies to the disk subsystem. To simplify the problem, assume that a repaired, but not restarted unit (processor or disk) does not fail. Use the following notations for the failure rate and repair rates:

λ_p	failure rate for one processor
λ_d	failure rate for one disk unit
μ_p	repair rate for one processor
μ_d	repair rate for one disk units

(12p)

3. Consider a computer system that consists of **four** processor modules operating in active redundancy. Define a GSPN model for calculating the steady-state availability of the system. The system is considered “available” if at least one processor is working. Assume that the life time of the modules is exponentially distributed with the failure rate λ and that the repair time for one processor module is exponentially distributed with a repair rate of μ. Assume ideal coverage and a maximum of **two** repair persons. The repair of a failed processor starts immediately after it has failed provided that a repair person is free. State the marking(s) corresponding to the event that the system is unavailable.
(8p)

4.

a) Draw a block diagram of a typical protection system. (Hint: A protection system is a safety system that monitors the behaviour of another system known as the EUC, or Equipment Under Control.)
(2p)

b) Describe the main advantages and disadvantages of using a programmable electronic system (PES) instead of a non-programmable device in a safety-related application.
(2p)

5.

a) Show by an example how the *risk* of an hazardous event can be calculated. The risk should be expressed in deaths per person-years.
(2p)

b) Explain the process of risk reduction.
(2p)

c) Explain the concept of *external* risk reduction.
(1p)

d) Within standards for aircraft systems the frequency of an hazardous event is often expressed as the expected number of occurrences per hour of flight. Depending on the frequency, an event is classified into three categories: probable, improbable and extremely improbable. What is the range of frequencies that correspond to i) a probable event, ii) an improbable event and iii) an extremely improbable event.
(3p)

6.

a) Describe the principle of the Recovery Blocks technique.
(2p)

b) Describe four techniques that can be used for constructing acceptance tests.
(4p)

7.

a) Describe the meaning of the terms *failure mode* and *failure model* in the context of distributed systems.
(2p)

b) In the course, we introduced a method for specifying failure modes where a failure mode is defined by a basic failure mode and a set of failure mode attributes. The method defines five basic failure modes. Describe these five basic failure modes. (Hint: the five basic failure modes can be applied to both nodes and networks.)
(5p)

8. What are the main advantages of using a network with a star topology compared to using a network with bus topology in the Time-Triggered Architecture?
(3p)

Mathematical Formulas

Laplace transforms

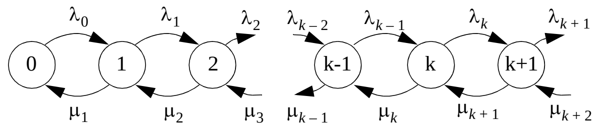
$$
\begin{array}{rll}
e^{-a \cdot t} & \dfrac{1}{s+a} & \\[2ex]
t \cdot e^{-a \cdot t} & \dfrac{1}{(s+a)^2} & \\[2ex]
t^n \cdot e^{-a \cdot t} & \dfrac{n!}{(s+a)^{n+1}} & n = 0, 1, 2, \ldots \\[2ex]
\dfrac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a} & \dfrac{1}{(s+a)(s+b)} & \\[2ex]
\dfrac{e^{-a \cdot t} - e^{-b \cdot t} - (b-a)te^{-bt}}{(b-a)^2} & \dfrac{1}{(s+a)(s+b)^2} &
\end{array}
$$

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