CHALMERS TEKNISKA HÖGSKOLA
Institutionen för data- och informationsteknik
Avdelningen för datorteknik

Exam in EDA122 (Chalmers) and DIT061 (GU) Fault-tolerant computer systems and DAT270 (Chalmers) Dependable computer systems, Tuesday, October 23, 2012, 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 Friday, October 21, on the course homepage.

Exam review/Granskning: November 19 and 21, at 12.00 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. Figure 1 shows the hardware architecture for a fault-tolerant unit (FTU) in a distributed control system. The FTU consists of two processor modules and two sensors. Each sensor is connected to one processor module. All units operate in active redundancy. The processor modules are designed to be fail silent, but may in rare cases exhibit value failures. The occurrence of a value failure is considered to be a failure of the entire FTU.

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

   (1p)

   b) Draw a fault-tree of the FTU. Assume that all failures are silent failures.

   (2p)

   c) Derive an expression for the reliability of the FTU. Assume that the life times of all units are exponentially distributed with the following failure rates and coverage factors:

   λ_p failure rate of one processor module
   λ_s failure rate of one sensor
   c_p coverage factor for a processor module failure
   c_s coverage factor for a sensor failure

   Non-covered sensor failures and non-covered failures of the processor modules have the same effect; they cause a processor module to exhibit a value failure. A covered failure causes the processor modules to fail silently.

   (5p)

   d) Derive an expression for the steady-state safety of the FTU. The FTU is in a safe shutdown state when both processor modules have failed silently and in a unsafe state when a value failure has occurred. Assume that the safe shutdown state and the unsafe state are absorbing states.

   (4p)

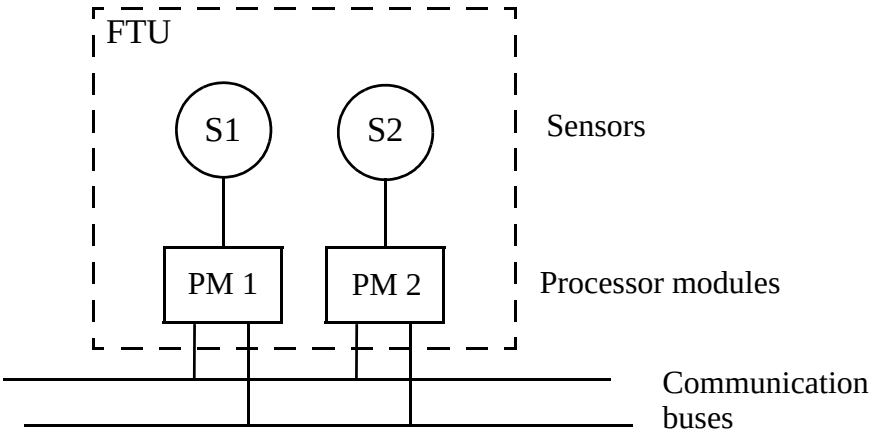


Figure 1

2. Consider a file server consisting of one control unit and two mirrored disks, see Figure 2. The mirrored disks allow the file server to be operational even if one disk fails. Assume perfect fault coverage and that all function times and repair times have an exponential distribution.

   a) Derive an expression for the steady-state availability of the control unit. The control unit has two failure modes, Type A and Type B. The failure rate is $2\lambda_c$ for Type A failures and λ_c for Type B failures. The repair rate is $2\mu_c$ for Type A failures and μ_c for Type B failures. Assume that a Type A failure cannot occur while the control unit is being repaired for a Type B failure, and vice versa.

   (6p)

   b) Derive an expression for the steady-state availability of the disk subsystem. The failure rate is λ_d and the repair rate is μ_d for one disk. The disk subsystem is repaired by one service technician. If both disks fail, the disk subsystem is restarted immediately when one disk has been repaired.

   (5p)

   c) Derive an expression for the steady-state availability of the file server. Assume that failures and repairs of the control unit occur independently of failures and repairs of the disk subsystem.

   (1p)

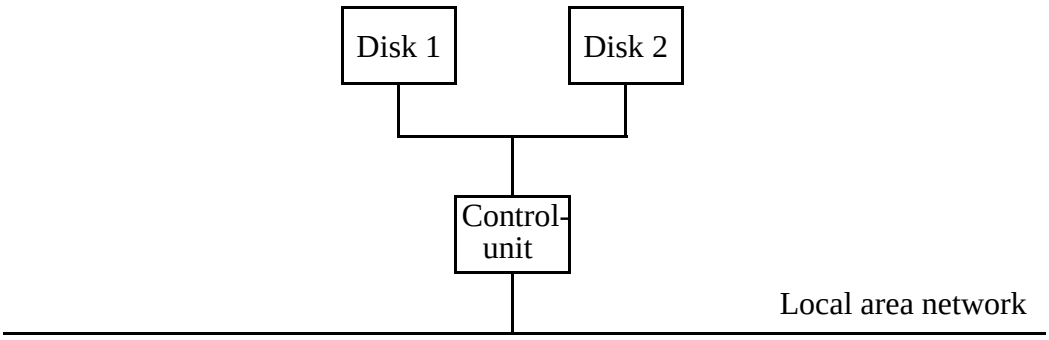


Figure 2: File server with two mirrored disks and one control unit

3. A fault-tolerant computer system consists of two active modules. The modules have two failure modes, Type I and Type II. The failure rate is λ_1 for Type I failures and λ_2 for Type II failures. The repair rate is μ_1 for Type I failures and μ_2 for Type II failures. Repairs are conducted by one service technician.

   a) Define a GSPN model for calculating the steady-state availability of the system.

   (6p)

   b) Draw the *extended reachability graph* of the GSPN.

   (6p)

4. Answer the following questions related to time-triggered distributed real-time systems.

   a) Explain how the use of time-triggered message scheduling ensures response time predictability in peak-load situations.

   (2p)

   b) Explain the term *composability*.

   (2p)

   c) Explain how time-triggered message scheduling facilitates composability.

   (2p)

5. Answer the following questions related to hazard and risk analysis.

   a) Describe the role of *safety reviews* in hazard analysis.

   (2p)

   b) The ISO 26262 standard uses a qualitative approach for determining the ASIL class for an item. The ASIL class is determined based on three properties (or factors). Describe the three properties.

   (3p)

6. In the paper “A Large-Scale Study of Failures in High-Performance Computing Systems”, Schroeder and Gibson make several interesting observations concerning failure rates and repair rates.

   a) What observation was made concerning the relationship between failure rate and system size?

   (2p)

   b) What observation was made concerning the variability of repair times?

   (2p)

   c) In what way did the age of the investigated systems influence repair times?

   (2p)

7.

a) Describe the principle of a multi-stage triple modular redundant (TMR) system.

(3p)

b) Show by an example how a multi-stage TMR system can tolerate Byzantine failures.

(4p)

Mathematical Formulas

Laplace transforms

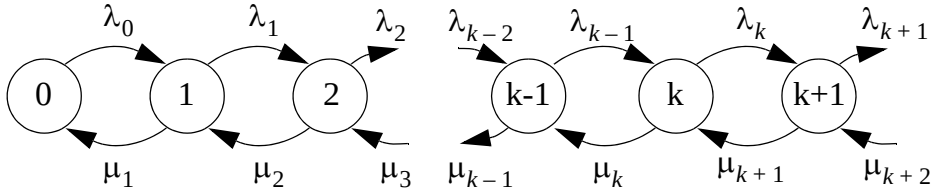
$e^{-a \cdot t}$	$\frac{1}{s+a}$
$t \cdot e^{-a \cdot t}$	$\frac{1}{(s+a)^2}$
$t^n \cdot e^{-a \cdot t}$	$\frac{n!}{(s+a)^{n+1}}$ $\quad n = 0, 1, 2, \ldots$
$\frac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a}$	$\frac{1}{(s+a)(s+b)}$
$\frac{e^{-a \cdot t} - e^{-b \cdot t} - (b-a)te^{-bt}}{(b-a)^2}$	$\frac{1}{(s+a)(s+b)^2}$

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