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

Exam in EDA122 (Chalmers) and DIT061 (GU) Fault-tolerant computer systems, Tuesday, October 21, 2008, 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.

Results/Resultat: Posted Monday, November 3, at 9.00.

Solutions/Lösningar: Posted Thursday, October 23, on the course homepage.

Exam review/Granskning: November 3 and 4, at 12.45 in Room 4107.

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 a fault tolerant unit (FTU) in a distributed real-time system. The FTU consists of two fail-silent computer nodes denoted A and B, which operate in active redundancy. Each node contains one processor, P, and two communication interfaces, C1 and C2. Two mutually redundant time-triggered buses are connected to the node via the communication interfaces.

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

   (2p)

   b) Derive an expression for the reliability of the FTU. Assume that all unit fails independently of each other, and that the function times of all units are exponentially distributed. Assume perfect coverage (100%). A node is considered operational when the processor and at least one communication interface is working. Use the following symbols:

   λ_p failure rate for one processor
   λ_c failure rate for one communication interface

   (6p)

   c) Assume that a communication interface failure leads to a fail silence violation with a probability of *1 - fsc*. (The probability *fsc* is the fail-silence coverage of communication interface failures.) Derive an expression for the expected time from the start of a fully functioning FTU to the first occurrence of a fail-silence violation. Assume that this time is not affected by processor failures.

   (2p)

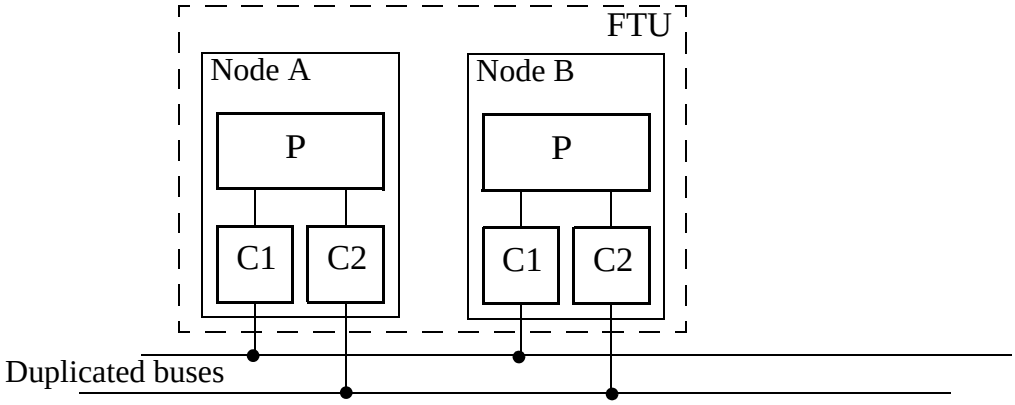


Figure 1

2. Derive an expression for the steady-state availability of the FTU shown in Figure 1. As in Problem 1), a node in the FTU is considered to be working when the processor and at least one communication interface are working. A service technician is notified immediately when any processor or communication interface fails. The repair time is completely dominated by the time it takes for the technician to travel to the system. The travel time is exponentially distributed with a rate of μ. The function times of the processors and communication interfaces have the same distributions as in Problem 1. Make the following simplifying assumptions:
   - A faulty node is repaired immediately when the technician arrives. (The actual repair time is negligible compared to the travel time.)
   - Repair is done by replacing the entire node.
   - The nodes have their own repair facility.
   - Coverage is perfect.
   - Working units within a non-working node do not fail.

   (12p)

3. Figure 2 shows a GSPN model of a duplex system with non-perfect coverage. Derive the reachability graph of the GSPN model.

   (6p)

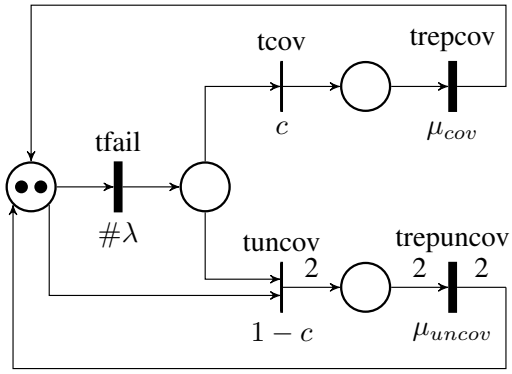


Figure 2

4. 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 their objectives and how they are related to each other (i.e., the order in which they are performed).

   (6p)

5. We have during the course discussed several techniques that can be used for prototype-based fault injection (fault injection in real systems). Describe three of these techniques and compare their characteristics with respect to *repeatability* and *reachability (accessability of fault injection points)*.

(6p)

6. The Time-Triggered Architecture supports two physical interconnection topologies for implementing clusters. Describe these topologies and their advantages and drawbacks.

(6p)

7. The Time-Triggered Architecture uses state messages to distribute *state information*. Describe the time properties and the semantics of state information.

(3p)

8.

a) Describe three types of consistency checks that are used in hardware implemented CPU exceptions.

(3p)

b) Describe the principle of a watchdog timer.

(2p)

9.

a) Describe the nature of a Byzantine failure.

(2p)

b) Explain how a Byzantine failure can be tolerated by voting in a distributed system consisting of four nodes.

(4p)

Mathematical Formulas

Laplace transforms

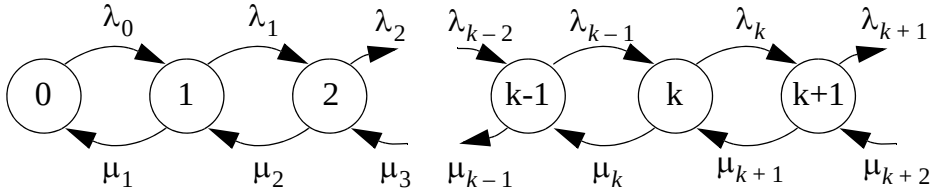
$e^{-a \cdot t}$	$\frac{1}{s+a}$
$t \cdot e^{-a \cdot t}$	$\frac{1}{(s+a)^2}$
$t^n \cdot e^{-a \cdot t}$	$\frac{n!}{(s+a)^{n+1}}$ $\quad n = 0, 1, 2, \ldots$
$\frac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a}$	$\frac{1}{(s+a)(s+b)}$
$\frac{e^{-a \cdot t} - e^{-b \cdot t} - (b-a)te^{-bt}}{(b-a)^2}$	$\frac{1}{(s+a)(s+b)^2}$

Reliability for *m* of *n* systems

$$R_{\text{m-of-n}} = \sum_{i=m}^{n} \binom{n}{i} \cdot R^i (1-R)^{n-i}$$

$$\binom{n}{k} = \frac{(n)_k}{k!} = \frac{n(n-1) \cdot \ldots \cdot (n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

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