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 21, 2009, 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 4 and 5, 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. Figure 1 shows the hardware architecture of a computer node for a real-time system. The node contains two mutually redundant processors that operate in active redundancy. Under fault-free circumstances, the processors produce identical messages that are transferred via the comparator to the two network interfaces, which broadcast the messages on two redundant buses. For each logical message, the comparator receives two message copies, one from each processor.

   The messages are protected by end-to-end checksums which are checked by the comparator. The comparator uses a two step approach to detect and mask errors in the messages. It first checks the checksums for each message copy individually, and then if both checksums are correct, it compares the messages bit-by-bit. If one or both end-to-end checksums are incorrect, no comparison is made.

   If none of the two message copies have a correct checksum, or if there is a mismatch in the comparison, no message is transferred to the network interfaces, and hence the node sends no message. If the checksum of one message copy is correct and the checksum of the other message copy is incorrect, the comparator transfers the message with the correct checksum to the bus interfaces, which then broadcast this message.

   a) Derive an expression for the reliability of the node. The node is considered to be operational if the comparator *and* both network interfaces *and* at least one processor is working correctly. Assume that the life times of the components are exponentially distributed with the following failure rates:
      λ_p failure rate for one processor
      λ_c failure rate for the comparator
      λ_n failure rate for one network interface
      Neglect failures of interconnections and bus guardians. Assume that the error coverage for the end-to-end checksums is ideal (c = 1) and that the probability for simultaneous processor failures is negligible.
      (3p)

   b) Derive an expression for the reliability of the node under the same assumptions as those given for problem a), with the exception that the error detection coverage for the end-to-end checksums is *c*, where $c < 1$. (Hint: a non-covered error occurs when the content of a message copy is incorrect, but the end-to-end checksum is valid.)
      (5p)

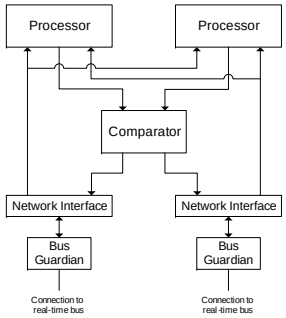


Figure 1

2. Derive an expression for the steady-state availability of a computer system that consists of two processors and three disk units. The system is operational as long as at least one processor and at least two disks are working correctly. Assume perfect fault coverage and that processors and disk units are serviced separately by two independent repair persons. Each repair person can only service one unit at a time. 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

   (8p)

3. Consider a computer system that consists of **two** processor modules operating as a hot-standby pair. Define a GSPN model for calculating the steady-state availability of the system. Assume that the life time of the modules is exponentially distributed with the failure rate λ. Repair is not started until both modules have failed. The repair time for one processor module is exponentially distributed with a repair rate of μ. The system is not restarted until both modules have been repaired. Assume ideal coverage and one repair person. State the marking(s) which corresponds to the event that the system is unavailable.

   (8p)

4. Define and explain the follow concepts related to risk and hazard analysis

   a) Define the term *hazard.*

   (1p)

   b) Define the term *risk*.

   (1p)

   c) Explain the terms *tolerable risk* and *achieved risk* and how they are related to each other.

   (2p)

   d) Explain the concept of *external risk reduction.*

   (1p)

   e) Explain the concept of ALARP and how it is used in risk analysis.

   (3p)

5. Describe and explain the following items related to the time-triggered architecture (TTA)

   a) Describe the main design principles for the communication network interface (CNI) in TTA

   (4p)

   b) Explain the concept of *composability* and how TTA supports composability.

   (4p)

   c) Describe the concept of a Fault-Tolerant Unit (FTU)

   (2p)

6. Figure 2 shows the hardware architecture of the electronic flight control system (EFCS) used in the JAS Gripen Aircraft.

   a) Describe the main principles for how fault tolerance is achieved in this system, and especially the role of the mid-level voters (MLV:s) and the cross-channel data link (CCDL).

   (2p)

   b) Show with an example the impact of an asymmetric sensor failure in this architecture. (An asymmetric sensor failure is when a sensor exhibits an asymmetric value failure, also known as an inconsistent content failure.)

   (2p)

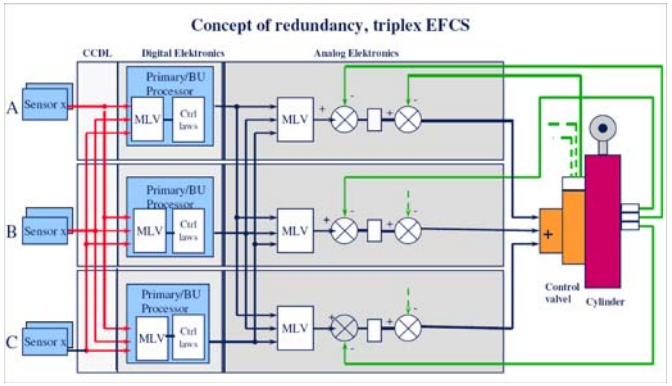


Figure 2

7.

   a) Describe the principle of N-version programming

   (2p)

   b) Describe briefly the purpose and the main conclusion of the experiment described in the paper “A Large Experiment in N-version Programming” by Knight, Leveson and St. Jean.

   (4p)

8.

   a) Show with an example that it is impossible for three nodes in a distributed system to reach consensus on a non-replicated value in the presence of one Byzantine failure.

   (3p)

   b) Show with an example how four nodes in a distributed system can reach consensus on a non-replicated value in the presence of one Byzantine failure

   (5p)

Mathematical Formulas

Laplace transforms

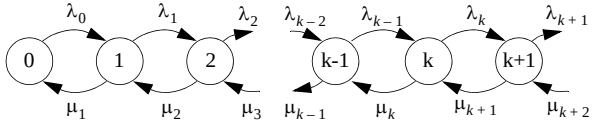
$e^{-a \cdot t}$	$\frac{1}{s+a}$	
$t \cdot e^{-a \cdot t}$	$\frac{1}{(s+a)^2}$	
$t^n \cdot e^{-a \cdot t}$	$\frac{n!}{(s+a)^{n+1}}$	$n = 0, 1, 2, ...$
$\frac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a}$	$\frac{1}{(s+a)(s+b)}$	
$\frac{e^{-a \cdot t} - e^{-b \cdot t} - (b-a)te^{-bt}}{(b-a)^2}$	$\frac{1}{(s+a)(s+b)^2}$	

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