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 19, 2011, 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 14 and 15, 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!**

© Johan Karlsson, 2011



---

1. The system architecture for a fault-tolerant node in a distributed computer system is shown i Figure 1. The node consists of three processor modules (PMs) and two I/O modules (IOMs). Each I/O module is connected to each of the processor modules via a parallel bus. The I/O modules communicate with other nodes in the system via two serial buses. The I/O modules are bus masters for the parallel buses, i.e., they control the transfer of messages between the processor modules and the serial buses.

   All modules operate in active redundancy. If all failures are silent failures, the system remains operational as long as at least one processor module and one I/O module (including the I/O module's parallel bus) are working.

   .

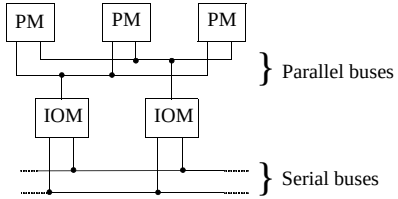



Figure 1.

a) Divide the system into the minimum number of fault containment regions required to achieve maximum reliability. Motivate the answer.
(2p)

b) Derive an expression for the reliability of the node. Assume that all failures are silent failures and that the function times of modules and buses are exponentially distributed. Use the following notation:
$\lambda_1$ failure rate for one processor module
$\lambda_2$ failure rate for one I/O-module
$\lambda_3$ failure rate for one parallel bus
Disregard failures of the serial buses.
(4p)

c) Derive an expression for the MTTF of the I/O module subsystem. (The I/O module subsystem consists of the I/O modules and the parallel buses.) Use the same assumptions and notation as in problem b).
(2p)

d) (See next page.)

d) Assume that the processor modules have two failure modes: silent failure and value failure. To mask value failures, the I/O modules perform a majority vote on the outgoing messages produced by the processor modules. This allows the node to mask the first processor failure, regardless of whether that failure is a value failure or a silent failure.

After the first processor failure, when voting no longer is possible, the I/O modules compare the outgoing messages received from the two remaining processor modules in order to detect value failures. If a value failure is detected, the I/O modules will stop sending messages on the serial buses to ensure that the node exhibits fail-silent failure semantics. Thus, the node is shutdown silently if the second processor failure is a value failure. The node continues to operate if the second processor failure is a silent failure.

The node exhibits a value failure in the case when only one processor module remains operational and that processor module exhibits a value failure. The node is shutdown silently if the third processor module failure is a silent failure.

The conditional probability (given that a processor module has failed) is *c* for a silent failure, and *(1-c)* for a value failure.

Derive an expression for the *steady state probability* that the processor module subsystem causes the node to exhibit a ***silent failure***. Explain your reasoning. Assume that two processor modules cannot fail at the same time. Disregard failures of the I/O module subsystem.

(4p)

2. A fault-tolerant file server consists of two processors and four disk units. All units operate in active redundancy. The server is operational as long as at least one processor and one disk are working.

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 $\lambda_p$ denote the failure rate for one processor and $\lambda_d$ the failure rate for one disk. 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 $\mu_p$ for a processor and $\mu_d$ for a disk. If both processors fail, the processor subsystem is not restarted until both processors have been repaired. If all four disks fail, the disk subsystem is restarted as soon as one disk has been repaired. Hence, the disks and the processors have different repair policies.

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

(12p)



3. A fault tolerant computer system consists of one active module and one cold spare module when the system is started. The failure rate of an active module is $\lambda$ and the dormancy factor k. A failed module is repaired with a repair rate of $\mu$. The system is serviced by one repair person. A failure of an active module is detected immediately by the repair person, but there is no way for the repair person to detect a failure of a cold spare module. Hence, a failure of a cold spare module is not detected until that module is activated following a failure of the other (active) module.

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. In the paper “Basic Concepts and Taxonomy of Dependable and Secure Computing”, Avizienis et al. describe a method for characterizing service failure modes according to four viewpoints. Two of the viewpoints are *failure detectability* and *failure consequences*. Describe the other two viewpoints. Each viewpoint encompasses two or more “failures types”. Describe each “failure type” in the two viewpoints.

(6p)

5. The communication network interface (CNI) between a host computer and the cluster communication system is the most important interface in the Time-Triggered Architecture (TTA).

a) Describe how messages are sent from a host to other hosts within a cluster. Consider data flow, control flow, message scheduling and network arbitration.

(4p)

b) Where is the push interface located and how does it work?

(1p)

c) Where is the pull interface located and how does it work?

(1p)

6.

a) Describe the concept of a Byzantine failure.

(2p)

b) Show by an example how a Byzantine failure can be tolerated in a multi-stage TMR system.

(4p)

7.

a) Explain the concept of *risk* as it is defined in the context of safety-critical computer systems

(2p)

b) Explain the concept of risk reduction and the term ALARP.

(4p)



## Mathematical Formulas

**Laplace transforms**

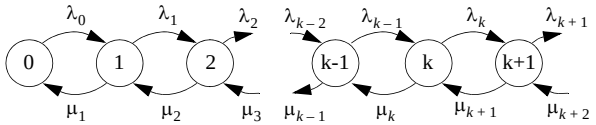
| | |
|---|---|
| $e^{-a \cdot t}$ | $\frac{1}{s+a}$ |
| $t \cdot e^{-a \cdot t}$ | $\frac{1}{(s+a)^2}$ |
| $t^n \cdot e^{-a \cdot t}$ | $\frac{n!}{(s+a)^{n+1}}$ $\quad n = 0, 1, 2, \ldots$ |
| $\frac{e^{-a \cdot t} - e^{-b \cdot t}}{b-a}$ | $\frac{1}{(s+a)(s+b)}$ |
| $\frac{e^{-a \cdot t} - e^{-b \cdot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

**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** $\Pi_i$ = steady-state probability of state $i$