EXAM–3 Fault Tolerant Systems 12/13/2005

READ CAREFULLY BEFORE BEGINNING

1. This exam comprises 25% for 400 level, 20% for 500 level of your total grade. Points are indicated for each question/section.
2. This is an **open book/notes** exam.
3. This is an 1 hour exam but you have 2 hour to finish.
4. Make sure your copy has **6** questions.
5. Read each question completely before answering. Be sure you understand all assumptions and constraints.
6. **Show all work and state all assumptions**. Partial credit can not be given for work not shown. Use the back of the page, if necessary.

REG MAXIMUM	100
DEDUCTIONS	−
TOTAL SCORE	

PRINTED NAME _____

SIGNATURE _____

1. (15) We have considered diagnosability of a ring, a graph $G = (V, E)$ where V is the set of n vertices (units) and E the set of N edges (test assignments). Now consider an extension of G, denoted by G^p, which is a **directed** (not undirected) graph with the same vertex set V. In G^p, a vertex $v_i \in V$ has an edge to each $v_{(i+j) mod\ n}$, for $j = 1, 2, ..., p$. You can envision G^p as a "ring" where each vertex is connected to p neighbor vertices in one direction. Note, that G^1 is a simple ring.

   (a) Draw the graph G^2 for $V = \{v_0, v_1, ..., v_7\}$.

   (b) Derive an explicit formula for the number of tests (test-count c) performed in a diagnosability scenario which uses G^p as the test assignment graph.

   (c) We want to determine the reliability of the test procedure under the assumption that the tests executed on each unit may return false results, i.e. they may indicate that a test returns "passed" where in reality there is a fault, with rate λ. Derive a Petri net that captures the reliability of the diagnosability problem based on the test assignment represented by G^p.

2. (20) With respect to the Boeing 777 flight control (paper by Bob Yeh):

   (a) In general, not specific to the 777, what is the primary feature of the "fly-by-wire" concept?

   (b) How are *Byzantine faults* dealt with? Can the triple-TMR handle such faults? Justify your answer.

   (c) Show a scenario that indicates the *maximum* number of faults the triple-triple redundant system could handle and still function correctly.

   (d) Now show a scenario that indicates the *minimum* number of faults that could cause the triple-triple redundant system to fail. (Note, this is a very different scenario from the previous question.)

   (e) What happens if the primary flight computer system fails? Does the plane crash, or is there an alternative?

3. (20) The Boeing 777 Air Data Inertial Reference Unit (ADIRU) has processors (P), gyros (G), accelerometers (A) power supplies (V) and left/center/right ARINC channels (AL, AC, AR). Assume at dispatch all fault containment modules (FCM) are functional. Derive a Petri net that models ADIRU reliability. Use the data of the paper, but to simplify the labeling, assume all FCMs have the same fail rate λ.

4. (15) RAID questions:

   (a) Draw a Markov chain for a RAID level 4 system using 8 **data** disks assuming that MTTF and MTTR are given. Make sure you indicate the rates of transitions. (Note: the 8 disks are only the data disks, so don't forget the check disk. Also, think about what it means for a RAID to fail.)

   (b) Why would anybody use RAID level 0? What is its claim to fame and what is its weakness?

   (c) What is the unreliability of a RAID 0 system that has 8 drives with a MTTF of 500,000h for t equal one year.

5. (20) With respect to fail-stop-processors (FSP) answer the following questions:

   (a) A control application operating in hostile environment, e.g., heat or vibrations, needs 4 processors to perform real-time calculations. Due to the special environment the computing system should be designed to handle k faults and it is suggested to use k-FSP. How many p-processors and s-processors do we need if faults are assumed to be independent? Pay attention to how you count processors!

   (b) Someone claims that (while preserving independence of faults) one can design a single k-FSP with only k rather than $k+1$ p-processors. The number of s-processors are not disputed. Is this possible or not? Justify your answer.

   (c) Another person claims that (while preserving independence of faults) one can design a single k-FSP with only $2k$ rather than $2k+1$ s-processors. The number of p-processors are not disputed. Is this possible or not? Justify your answer.

6. (10) Dealing with faults:

   (a) Assume there is a system consisting of N processing units and you are using the PMC model forming a ring. In general, can this system be one-step 2-fault-diagnosable? Justify your answer.

   (b) Considering the fault model of the Thambidurai and Park paper. What fault mode does the PMC model assume? Justify your answer and indicate why the other fault modes do not apply.

Extra Page