ECE 510 Fault Tolerant Systems Exam #1 (SOLUTION)

All answers must be on the exam and in the space provided. Any answers submitted on separate sheets of paper will not be graded.

1. Consider the partial fault tree on page 172 of your text. Assume the memory test fails to detect with probability 0.02 and the end-around test fails to detect with probability 0.01. All other basic events occur with probability 0.05. What is the probability that a spurious computer command is not detected?

P(spurious operator) = (0.01)(0.05) = 0.0005
P(spurious CPU) = (0.05)(0.05) = 0.0025
P(spurious memory) = (0.02)(0.05) = 0.0010

P(spurious computer) = 0.0005 + 0.0025 + 0.0010 = 0.0040

2. What is a "safety-critical" computer system?

A computer system in which failure can result in injury, death or major environmental damage.

3. The software fault density varies widely from a low of 0.002 to a high of 0.02. The software is expressed in a state diagram with 350 nodes. In addition, there are 22 I/O variable assignments. Estimate the number of software faults.

From table 5.14, 350 nodes and 22 I/O variable assignments produces 372 equivalent lines of code.

the nominal software fault density is $\sqrt{(0.002)(0.02)} \approx 0.0063$

Therefore, the estimated number of software faults is (0.0063)(272) = 2.34

4. Does an FMET check for commission failures or omission failures? (Justify your answer)

An FMET purposely injects faults into a system to evaluate their effect. Suppose this fault leads to a failure. Then you are evaluating how the software responds to a system failure. By definition this is checking for an omission failure.

5. What is the best way to guarantee the accuracy of an FTA?

Conduct an FMET using the failure modes identified in the FTA.

NOTE: Just saying "conduct an FMET" is not a sufficient answer. You must be specific in which failures you inject into the system undergoing test. The FTA will identify which failures in which components caused the mishap. Those are the failures you must use in the FMET. If those failures do indeed cause the mishap, then you have verified the FTA is accurate.

6. How are a mishap, hazard, fault and a failure related?

fault $\Rightarrow$ failure $\Rightarrow$ hazard $\Rightarrow$ mishap

7. A mishap destroys a system valued at $800,000. According to MIL-STD-882D, this mishap would be classified in which severity category?

category II (critical)

8. What is a transducer?

A device that transforms one physical entity into another.

9. What are the three types of software? application, developmental and system

10. Historical data indicates a hardware module has 5 component failures every 90 days. What is the probability of a component failure in 50 days?

$P(t) = 1 - e^{-\lambda t}$ where $\lambda = 5$ failures/90 days and $t = 50$ days. Substituting yields

$$P(50) = 1 - \exp\left[-\frac{5}{90} \cdot 50\right] = 0.938$$