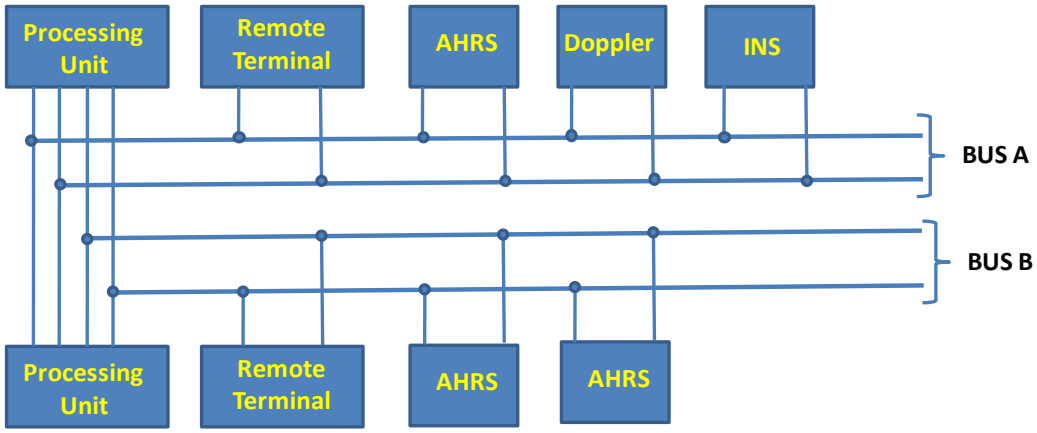
Design of Fault-tolerant Digital Systems (EECE 513): Assignment 1

Due Date: In class on **Thursday, Feb 13th, 2014 (in class).**

This assignment consists of ten questions, each of which carries 10 points. Please show all your work and list all assumptions you make in your answers.

Question 1: Series/Parallel System Redundancy

The system shown in the figure below is a processing system for a helicopter. The system has dual- redundant processors and dual-redundant interface units. Two buses are used in the system, and each bus is also dual-redundant. The interesting thing part of the system is the navigation equipment. The aircraft can be completely navigated using the Inertial Navigation System (INS). If the INS fails, the aircraft can be navigated using the combination of the Doppler and the attitude heading and reference system (AHRS). The system contains three AHRS units, of which only one is needed. This is an example of functional redundancy where the data from the AHRS and the Doppler can be used to replace the INS, if the INS fails. Because of the other sensors and instrumentation, both buses are required for the system to function properly regardless of which navigation mode is being employed. Answer the following questions about the system.



a. Draw the reliability block diagram of the system as a series-parallel diagram.

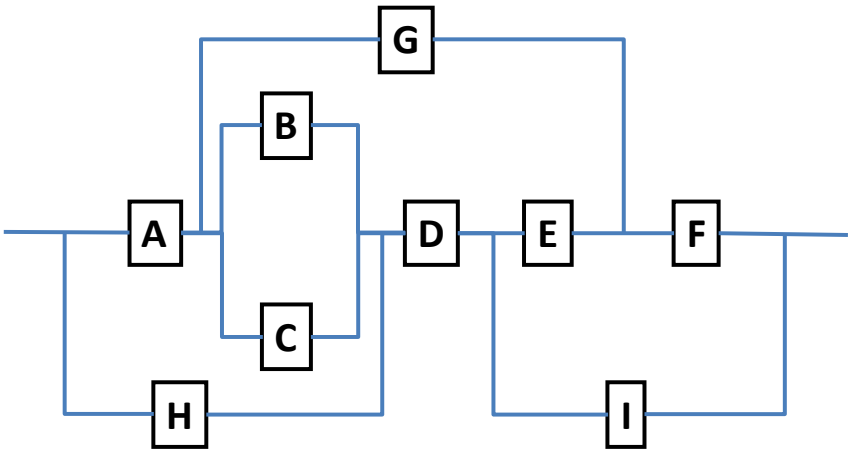
b. Derive the expression for the reliability of the system R(t) in terms of the reliabilities of its individual components. You may assume that the reliabilities of the same types of components are identical.

c. Calculate the reliability of the system for 1 hour, assuming that component failures are exponentially distributed and the Mean Time to Fail (MTTF) of individual components are as follows. Assume perfect detection coverage.

Component	**MTTF in hours**
Processing unit	2000
Remote Terminal	3500
AHRS	1000
INS	1000
Doppler	700
Bus	500

Question 2: Non-series/Non-Parallel System Redundancy

Using an approach described in class, calculate the reliability of the system below. Calculate an upper bound on the reliability using the independent path assumption.



Question 3: Software fault-tolerance and coverage

A. A system design uses N-Version programming for reliability. There are 3 versions of the software and the decision algorithm generates output if at least 2 out of the 3 versions agree and generates a failure condition if they don't match.

- The probability that Version 1 generates incorrect output on a random input is 0.0002.
- The probability that Version 2 generates incorrect output on a random input is 0.0023.
- The probability that Version 3 generates incorrect output on a random input is 0.0001

Assume that failures of versions are independent. There is also a bug in the decision algorithm that is triggered only when all three versions agree and causes it to generate a failure condition with probability 0.0000002. Assuming that incorrect outputs do not match, what is the probability that the system works?

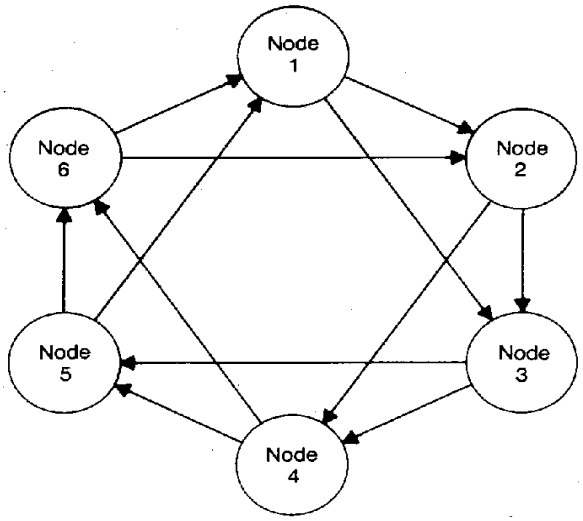
B. How would the answer to part A differ if the system uses the three modules in a recovery block like configuration. In other words, version (i + 1) is activated if and only if version i fails and the decision algorithm detects the failure or if the decision algorithm generates a false failure condition. (assume that the decision mechanism has the same bug as in part A, but that it is otherwise perfect).

Question 4: Skip Ring Network

The architecture of a network of computers in a system is shown below. The architecture is called a skip-ring network and is designed to allow processors to communicate even after node failures have occurred. For example if node 1 fails, node 6 can bypass the failed node by routing data over the alternative link connecting nodes 6 and 2. Assuming the links are perfect and the nodes each have a reliability of R_m , derive an expression for

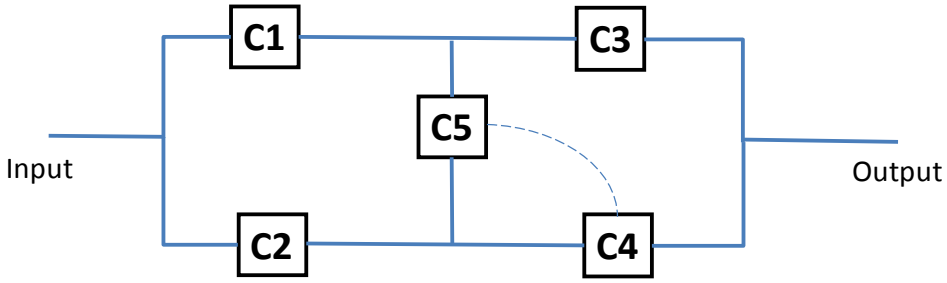
the reliability of the network. If R_m obeys the exponential failure and the failure rate of each node is 0.002 failures per hour, determine the reliability of the system at the end of a ten-hour period. How does this compare with the reliability of a simple ring system?

Note: We consider, the network system to be fully operational (i.e., there is no system failure) as long as each working node can communicate (reach) any other working node in the system (either directly or by routing data over other nodes).



Question 5: Correlated Failures

Consider the system below. Assume that each component fails independently and calculate the system's reliability in terms of its components' reliability. Now assume that whenever component C5 fails, it triggers an immediate failure of component C4. What is the total reliability of the system in this case and how does it compare to the previous value? Assume that each component has a reliability of R for both parts.



Question 6: TMR Voting

Consider a simple TMR system with voting. Let the reliability of the voter be R_v and that of the module be R_m. Clearly, the lower the reliability of the voter, the lower the reliability of the system. However, there is a value of R_v beyond which the TMR system will have even lower reliability than that of the corresponding simplex system. Let's call this value $R_{v\text{-}min}$ .You need to answer the following questions:

a. Derive an expression for $R_{v\text{-}min}$, as a function R_m ,in order for the reliability of the TMR system to be greater than the reliability of the Simplex.
b. Draw a graph showing how $R_{v\text{-}min}$ varies as a function of R_m.
c. Assume that the reliability of the voter is 0.95. What is the allowable range of R_m so that the reliability of the TMR system is higher than that of Simplex?

Question 7: Reliability modeling using field data

Failure data collected from a time-sharing system over 38 hours is shown in the table. The first column shows the time interval and the second column shows the number of errors obtained during that time. For instance, the first row of the table means that 6 errors were observed within the first hour of operation of the system.

Time (in hours)	Number of observed errors within the time interval
0 – 1	6
1 – 2	3
2 – 3	5
3 – 4	2
4 – 5	7
5 – 6	5
6 – 7	1
7 – 8	1
8 – 9	3
9 – 10	4
10 – 11	2
11 – 12	1
12 – 13	2
13 – 14	2
14 – 15	1
15 – 16	1
16 – 17	3
17 – 18	1
18 – 21	4
21 – 24	1
24 – 29	3
29 – 38	2

Is the exponential distribution is a good fit for modeling the inter-arrival times of the errors? If so, does the exponential distribution apply throughout the lifetime of the system or only to a specific interval? If it is the former, find the failure rate of the distribution. If it is the latter, find the interval during which the exponential distribution applies and the failure rate during this interval. Justify your answers quantitatively.

Question 8: Failure Rates and Redundancy

This problem addresses the design of memory units with redundancy. To improve reliability, each k-bit memory word is expanded by s spare cells, so each row contains $k + s$ memory cells. There are n rows in the memory system. Assume that the memory chips contain n rows and each row contains only one cell. The entire memory system, then, contains $k + s$ chips. Each chip has a failure rate of λ and obeys the exponential law.

A. Derive an expression for the reliability of the complete memory system using column sparing. The expression must account for fault coverage.
B. Suppose that $k = 16$, $\lambda = 9.15 \times 10^{-6}$ failures per hour, and a fault coverage $C = 0.97$. Determine the number of spares that will maximize the reliability of the memory at the end of a 10-year space mission (HINT: Plot R(t) as a function of s and determine the optimal value from the curve).

Question 9: Definitions of reliability, availability, safety etc.
For the following systems (A and B), identify which attribute (reliability, availability etc.) is considered least important. Justify your answers.

A. An aircraft system has three computers voting on the results of every operation performed by the auto-pilot. If the auto-pilot fails, a warning alarm goes off in the cockpit to alert the pilot, who can then take over the manual controls of the aircraft and guide it to safety. However, the pilot does not interfere as long as the autopilot does not raise the alarm.
B. An online trading website allows its customers to place bids on various items, and to track their bidding online. While it is acceptable for a user to not be able to place bids if the traffic is too high, it is not acceptable for a user who has placed bids to not track their bid's status and modify the bid. Also, as far as possible, the website should not display an incorrect value of the item's current bid, as this can cause users to over/under-bid for it.

In each of the following descriptions (C and D), identify the fault, error and failure.

C. A program contains a rare race condition that is only triggered when the OS schedules threads in a certain order. Once triggered however, the race condition corrupts a value in the program, which in turn is used to make a branching decision. If the branching decision is incorrect, the program will go into an infinite loop and hang, thus failing to produce any output.
D. A radar system uses an array of processors to track its target in real-time. A soft error in a processor can lead to the processor computing an incorrect value for the target's location. However, the system can compensate for this effect by redundantly allocating the tasks to processors and comparing the results. But this compensation entails a performance overhead, which in some cases, can cause the system to miss the tasks' deadlines and lose the target.

Question 10: Identification of fault model
A. Identify the fault model that is addressed in each of the following techniques (you need to clearly state the assumptions you make regarding the technique and justify them):

1. Checkpointing and recovery in parallel systems,
2. Process migration to deal with hard faults in multi-processors.

B. Name a fault-tolerance technique that you have encountered in the course of your own experience, different from the above two. What was the fault model in that technique?