University of Twente

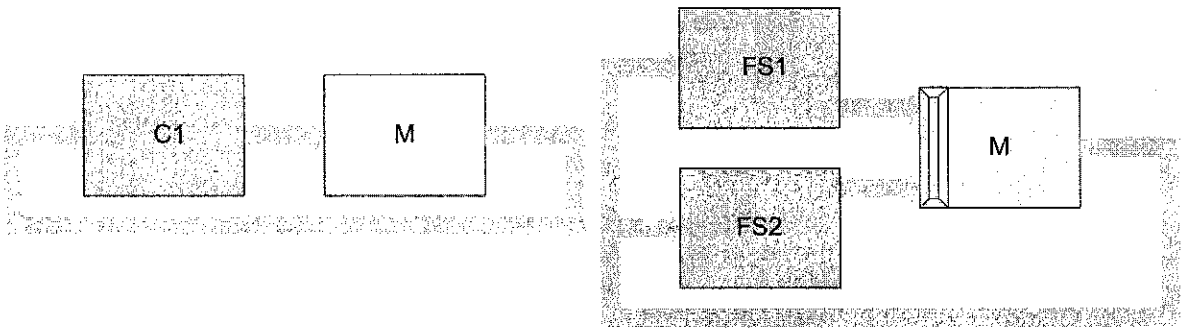
Examination "Fault Tolerant Digital Systems"

Code: (19)213009

Assignments (5 pieces):
Dutch students are allowed to provide the answers in Dutch. International students are allowed to use Dutch or English.

Assignment 1: Reliability Criteria

A computer system C1 controls a machine M as shown in Figure a). The machine is part of a production process where interruptions are very costly. It turns out, the failure rate λ_1 of the computer system C1 is too large ($\lambda_1 = 10^{-3}$ / hour).
The failure rate λ_M of the machine is 10^{-4} / hour. For the total system, the computer control C1 and the machine M, a failure rate λ_T of 2.10^{-4} / hour is acceptable.



a) b)

In order to improve the reliability of the system, the original computer system C1, is replaced by a fail-stop system FS1 (Figure b)) having a failure rate $\lambda_{FS1} = (1,2).\lambda_1$. In addition, a second fail-stop system FS2 is added, having a failure rate $\lambda_{FS2} = (2).\ \lambda_1$. Both systems send their control data to the machine M, which has been adapted in such a way that it will function correctly as long as both inputs receive the same data, or if data is received at one of the inputs. However, as result of the adaptation, the failure rate of the machine M has increased with 7.8%.
Fail-stop systems are rarely *completely* fail-stop. In our case we assume that in 3% of the cases where a fault appears, the fail-stop system will still provide incorrect data, resulting in machine (M) failure. Hence the coverage of both FS1 and FS2 is 97%.
The repair time of the fail-stop system FS1 is one and a half (1,5) hours.

Questions:

1. What is the failure rate of the total of computer control (C1) and machine (M) in the non-redundant system as shown above in Figure a?

2. Provide the Markov diagram of the redundant system and give in the diagram all transition probabilities

3. Calculate the maximum allowed average repair time of the fail-stop part FS2

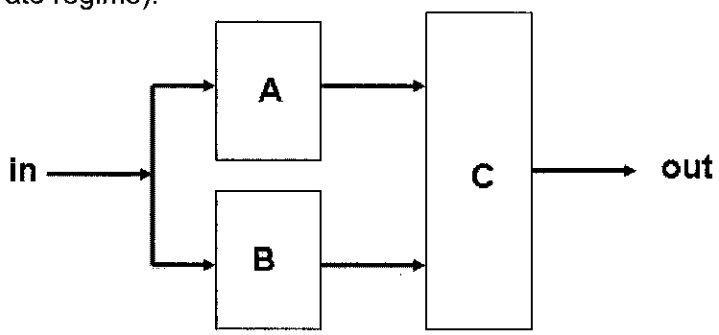
University of Twente

Assignment 2: Reliability Criteria

Examine the figure below, showing a redundant, non-repairable system. The functional blocks A and B are the same (equivalent) and carry out the same operations on the input data.

The block C compares the data of A and B, and decides which block is fault-free. If the block C is fault-free it carries out its task with 100% certainty. In the case block C is faulty, its decision is incorrect with 100% certainty.

The failure rates $\lambda_A=2\lambda$, $\lambda_B=2\lambda$, and $\lambda_C=3\lambda$ of A, B en C respectively, are constant (constant failure-rate regime).



Questions:

1. Provide the exact definition of the failure rate $\lambda_A(t)$ of block A
2. Determine the reliability function R(t) of the total system as shown in the figure
3. Provide the exact definition of the mean time to failure (MTTF) of a system
4. Determine the MTTF of the total system as shown in the figure
5. Suppose the above system is extended with a functional block D ($\lambda_D=3\lambda$), identical in function to A and B, and put in parallel to A and B; furthermore we assume that C in this case is a fault-free ($\lambda_C=0$) majority voter. A majority voter is a block which makes its decision on the basis of a majority.
   Determine the resulting R(t) of this triplicate system.

Assignment 3: Fault Tolerant Techniques

The (N, K) concept uses multiple independent modules and makes use of fault correcting codes. The most popular ones are (3, 1) and (4, 2).

Questions:

1. Show a drawing of the architecture of the (4, 2) concept in the case of a 16-bits processor, including codecs and the width of data paths and memories.
2. Explain why the above system can mask a random fault in a module
3. Assume a system employing the (3, 1) concept. How does the system notice the occurrence of a fault in a module and which additional hardware resources are required for this?
4. If the previous module is being replaced without stopping the system, which procedure has to be followed to insert a new module in the system?

Assignment 4: Consensus Algorithms

Malicious faults in fault-tolerant systems can be tackled using consensus algorithms, like the Byzantine Generals algorithm.

Questions:

1. What characterizes a malicious fault, what can it do to a fault tolerant system? Provide several physical causes of this type of faults.
2. Which properties are satisfied in Byzantine General algorithms, and give the definitions of these properties.
3. Describe the Byzantine Generals algorithm (without authenticated messages) for four modules of which one can be a faulty module at maximum. Show by means of an unfolded data flow graph that the properties in question 2 are met in this example.
4. Provide the relation between the minimal number of modules, the number of faulty modules in those, and the number of required communication rounds in order to guarantee a fault-free behaviour of the system.

Assignment 5: Self-Stabilizing Algorithms

A number of processors in a network is driven synchronously. Every processor has a clock which determines the local time. At the initiation of the system, or after a fault, the clock times of the system can be different. The clocks do not have to represent the absolute time, but their local times should be the same. This requires the synchronization of the clock time in this synchronous system, for instance by applying a self-stabilizing algorithm.

Questions:

1. Which two properties are required in a self-stabilizing system, and subsequently provide their definitions.
2. Provide an algorithm that synchronizes the clocks of the processors, assuming that all processors and their communication are fault-free. Show that the synchronization is achieved after a number of rounds.
3. What is the minimal requirement with regard to the graph which models the connectivity between the processors?