Dependable Systems
SS 2011

Assignment 1 (v1.2)

(Submission deadline: May 22th, 23:59 CET)

Fault Tree Modeling

In this assignment, it is your task to perform a complex fault tree modeling for a given system setup. You can (but don‘t have to) use the SHARPE fault tree tool for the modeling activities. The tool is written in Java, but was only tested and prepared to run with Windows. It is available with the password from the lecture at

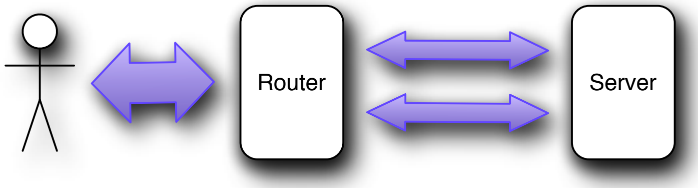
http://www.dcl.hpi.uni-potsdam.de/teaching/depend/sharpe/sharpe.zip

Please submit your written solution report as PDF document (no ZIP, no RAR, no native SHARPE files) at:

https://www.dcl.hpi.uni-potsdam.de/dependassign/

The System Setup

The system setup contains of a high-end server machine with support for *field-replaceable units* (FRU), and a network router connecting the system to the external user. Router and server system are connected via two redundant network connections. Incoming requests and outgoing responses for / from the server must be transmitted through the router. It operates in an active-active mode, were the redundant links are both used under normal conditions.



The reliability of the server components and the network router is given below. Please consider the following facts for the setup of the server system:

- Some server hardware components have ‚hot swapping‘ capabilities, meaning that all but one redundant unit can be replaced without interruption of server operation.
- The expected fault model is fail-stop, meaning that replaceable components fail without propagating their error state to other parts of the system. Memory modules are assumed to fail ‚as a whole‘ if an uncorrected bit error occurs.
- Non-listed components are assumed to never fail.

- For non-described component dependencies, meaningful defaults should be assumed and documented.
- Xeon 7500 series processors have two memory controllers integrated. In the investigated setting, each memory controller has exactly two memory modules connected to it.
- Memory controllers are assumed to not fail if one of the memory modules fails.

The (completely artificial) failure rates are given in failures per 10^9 hours of operation[1].

Component	Quantity	Failure Rate
Power supply with hot swapping support	2	9708,737
Operator information panel	1	12231,725
DVD drive	1	8443,0935
Nehalem EX (Intel Xeon X7560) processor	2	1500,23
Processor fan	2	10131,712
Memory module	8	4000,333
Mainboard with CPU, memory and PCI-E hot swapping support	1	6070,46
Gigabit PCI-E network card	2	3121,32
PCI-E RAID controller in RAID 15 mode	1	3121,32
Hard disc drive	6	2008,12
Network Router	1	1870,12

Task 1.1 (mandatory)

Develop the fault tree and the reliability block diagram for the described system setup, including the server and the router. Determine the probability that the system does not break before the end of warranty time (2 years). Add both graphs, the probability value and your model design decisions to the written report.

Task 1.2 (mandatory)

Describe the minimum cut set of the fault tree. What are appropriate steps to improve the system reliability ?

Task 1.3 (optional)

Add the operating system as part of your reliability analysis. Compare the cases were the operating system does / does not support hot swapping of CPU‘s.

Task 1.4 (optional)

Based on the result of task 1.3, compare the cases were the operating system does / does not support hot swapping of memory modules.

[1] ftp://ftp.acer-euro.com/server/AAR500/certificates/