Dependable Systems SS 2014

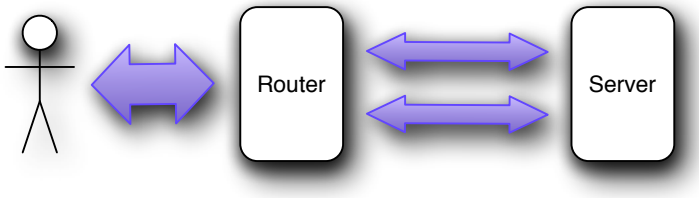
Assignment 1

Fault Tree Modeling

In this assignment, it is your task to perform a ‚pen and paper' fault tree modeling for a given system setup. Please upload your solution report as PDF document (no ZIP, no RAR) at https://www.dcl.hpi.uni-potsdam.de/submit/

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.



Consider the following facts for the setup of the server system:

- The expected fault model is fail-stop, meaning that replaceable components fail without propagating their error state..
- 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, operating in mirroring mode (RAIM 1).
- Memory modules are assumed to fail ‚as a whole' if an uncorrected bit error occurs.
- A memory controller not being able to provide memory is considered as broken.
- The CPU stops to work if one of the memory controllers is broken.
- The CPU fails immediately if the attached fan fails.
- The power supplies act as redundant couple, so one of them can take the complete load.
- The operating system is Linux in the *kernel.org* default configuration.

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

Develop the fault tree for the described system setup, including the server and the router. You are free to use the fault tree modeling tool developed by the Operating Systems & Middleware group, which is available at fuzzed.org.

The modeling tool allows the creation of ‚graph snapshots'. For this assignment, it is sufficient to add a snapshot URL to your submitted report. The corrector will be able to read it.

Add an explanation of your model design decisions to the written report.

Task 1.2

Explain how the minimum cut sets of the fault tree and their probability of occurrence can be determined.

Discuss the difference between cut set length / cardinality and cut set probability as ranking criteria.

What are appropriate steps to improve the system reliability ?

Task 1.3

Determine the probability that the system does not break before the end of warranty time (2 years = 17520h).

Explain your calculation steps.

Task 1.4 (optional)

Please send us your feedback about the fuzztrees.net modeling tool. We are happy about any kind of bug report or feature suggestion at

http://fuzzed.uservoice.com/

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