

Dependable Systems

SS 2012

Assignment 2

(Submission deadline: June 17th 2012, 23:59 CET)

Reliability and Maintenance Modeling

In this assignment, you will model a complex reliability scenario with the commercial software „BlockSim 8“ by ReliaSoft. The software is available for 32-bit and 64-bit Windows. Both the mirrored install packages and the academic license number are available at:

<https://www.dcl.hpi.uni-potsdam.de/teaching/depend/blocksim/>

The credentials for the page login were handed out at the lecture. If you did not get them, please ask your colleagues. Manuals for the software are available as in-built Windows help file.

Please submit your solution as one ZIP file, containing the modeling repository file from BlockSim (with all solutions) and the written report, at:

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

Task 2.1 (mandatory)

Model the system described in Task 1.1 from the last assignment as fault tree in BlockSim, considering the following additional conditions:

- If the mainboard fails, the system fails.
- If both network cards fail at the same time, the system fails.
- If both power supplies fail at the same time, the system fails.
- If a fan breaks, the attached CPU breaks too.
- If one of the RAIM pairs goes down as a whole, the memory controller signals a CPU failure.
- The system can only survive if both CPUs are working.
- Operator panel and DVD drive are not part of the fault tree model, they never contribute to a system failure.

Determine the TOP event probability and the minimal cut sets for the model and state them in the written report. Submit the BlockSim model as part of your repository file.

Task 2.2 (mandatory)

A system consists of a single load balancer, 20 application servers in an active/active failover cluster configuration, and 6 database servers in an active/active failover cluster configuration. Due to performance considerations, the system is defined to be failed if either the load balancer fails, 8 application servers fail or 2 database servers fail.

The Dull application servers are commercial-off-the-shelf systems with a comparatively high unreliability, which can be modeled by a 2p Weibull distribution of $\beta=4$ and $\eta=500\text{h}$. Due to their smart enclosure design, they can be fixed quickly within 4h.

The HiP database servers are reliable machines with a failure probability density function following the 2p Weibull distribution with $\beta=2$ and $\eta=800\text{h}$. Due to the necessary re-synchronization of a repaired database server, the repair activity takes 8h on average.

The Casco load balancer does sometimes lock up (2p Weibull; $\beta=5$; $\eta=2500\text{h}$) and needs to be rebooted (5 min).

Model the system in BlockSim as reliability block diagram. Consider the possibility of configuring a block as 'multi-block'. Figure out how to configure their repair times as 'corrective task', f.e. by using the BlockSim resource manager.

Determine the average system availability by simulation. The number of simultaneous repairs shall not be limited. State in your report the results for a system life time of 3 years, 3 months and 3 weeks. Interpret the results. Submit the reliability block diagram as part of your submitted BlockSim repository.

Figure out how to define a repair crew. This crew should be able to conduct exactly one repair task at a time. Assign this repair crew to all three component types. How does the average system availability change for a life time of 3 years? Discuss the results in your written report.

Task 2.3 (mandatory)

A computer pool in a literature studies department consists of 1 central router ($\beta=2$; $\eta=50000\text{h}$), 5 pool machines ($\beta=1,5$; $\eta=20000\text{h}$), 1 file server ($\beta=2$; $\eta=30000$) and 1 backup tape server ($\beta=5$; $\eta=18000\text{h}$). All machines fail according to the 2P Weibull distribution.

What is the average life time of the system when all systems run without interruption? Document the result in your report.

In the next step, consider a department director has the green thumb, so he mandates to switch off unused machines automatically with BIOS alarm clocks. The pool is opened between 8:00h and 22:00h for students. During this time, the tape server is switched off and the file server is operational. After the closing at 22:00h, all pool machines are automatically switched off, the tape server is switched on and a backup of the file server is dumped on the tape server. This backup procedure takes 3h on average. After that, the file server and the tape server shut down until the next morning. The router has to be operational always, in order to allow remote management tasks.

Model the system in BlockSim as phase diagram. This works by copying the initial RBD for defining the alternative phases. The copying also ensures that BlockSim can relate the components to each other for an age simulation in different phases. How does the average life time change with the new green scenario? Document the result in your report.

In the third step, the management thinks about buying a new backup tape server (Weibull 2p; $\beta=3$; $\eta=50000$) that needs only one hour of backup time. Use your model to determine how the new server would change the average system life time. Document the result in your report, and submit the final version of the phase diagram / RBDs as part of your submitted BlockSim repository.


Task 2.4 (optional)

You are designing a system that has a well-known expensive component acting as single point of failure. Its failure probability is known from historical data and can be modeled with a 2p Weibull distribution of $\beta=2,5$ and $\eta=500h$.

The management negotiates with the customer that any planned or unplanned system downtime costs a SLA penalty of 800€ per hour („downtime rate“). For unplanned downtime, the customer gets another fine of 1000€ per failure („costs per failure“).

Since the critical component is too expensive in order to make it redundant, the replacement procedure („corrective task“) for the component is carefully planned: The service mechanic has to locate the problem (1h), read the documentation for replacing and testing a new component (1h), get and setup the new component from the storage (1h) and replace the old component and test the repaired system (1h) before the system is working again.

In order to minimize unplanned downtime, the service mechanic tries to replace the component before it fails. During such planned maintenance („scheduled task“), the first three steps can be done while the system is still running. However, the mechanic is unsure when to schedule the planned maintenance. In a first attempt, he schedules the replacement in an interval of 450h of life time if no failure happened before.

Use a simulation fault tree in BlockSim to calculate the optimum replacement time (search for this icon ).