18-540
Distributed Embedded Systems
Test #3
SOLUTIONS
December 6, 2000

Name (please print): _____________________________________________________

Instructions: DO NOT OPEN TEST UNTIL TOLD TO START
This test lasts from 12:30 PM to 2:20 PM (normal class hours)

The test is composed of 4 problems adding up to 100 points overall. The point value is indicated for each sub-problem. Attempt all problems and budget your time according to the problem’s difficulty. Show all work in the space provided. If you have to make an assumption then state what it was. Answers unaccompanied by reasonable supporting work will not receive full credit. The exam is closed book, closed notes, and “closed neighbors” but you are permitted a single 8.5”x11” piece of paper with notes on both sides. You are required to erase any course-relevant material from your calculator prior to the start of the test. Please print your initials at the top of each page in case the pages of your test get accidentally separated. You may separate the pages of the test if you like, and re-staple them when handing the test in.

Good luck!
Grading Sheet

1) (20) ___________________

2a) (9) ___________________
2b) (20) ___________________

3) (24) ___________________

4) (27) ___________________

TOTAL: ___________________ points out of 100
Example System.

The example system used for this test is the elevator solution sheets handed out during the course of the semester for the course project. Relevant sheets are included in this test package and are UNCHANGED from solution materials that have been posted on the course web site.
1. **Failure Mode Effects Analysis (FMEA)**

   **Grading:** (20 points – 1 point per box; no partial credit)

   Perform an FMEA for the elevator system as described below. *Unless otherwise indicated*, assume that any failure is a complete and total failure resulting in a situation as if the failed component were not installed in the first place (*i.e.*, fail fast, fail silent). Assume that no failure management code has been implemented – this is just failures happening to the baseline elevator.

   Fill out the table by putting “YES” or “NO” in every appropriate box for the specified failure mode, or put in “N/A” for “not applicable.” Put a decimalized number (e.g., “2.1”) for the behavior number in the right-most column. Answer all questions assuming the general case, (for example, if a Hall Call button were broken, assume that some passenger would actually want to press it at some point). Remember, these answers apply to the example solution provided and **NOT** to how you implemented the project yourself.

   **Important note:** challenges to the answer key will ONLY be considered if they are backed up by annotations on the NEXT PAGE (i.e., all challenges must be supported by what you were thinking during the test). However, even correct guesses will receive full credit regardless of comments on the next page. Note that some answers can be “either” or “N/A” – those are free points for you.

<table>
<thead>
<tr>
<th>FAILED COMPONENT</th>
<th>FAILURE MODE</th>
<th>Eventually, will the following happen? Write “YES” or “NO” in each and every blank box below.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Elevator makes unnecessary stops (YES/NO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Passenger not able to enter/leave car until it happens to stop at floor by accident (YES/NO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Elevator unable to stop at some particular floor (YES/NO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Emergency brake will be activated (YES/NO)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If emergency brake activated, which Safety Behavior causes this? (2.x...)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HallCall[MaxFloor, down]</th>
<th>FAIL SILENT</th>
<th>1 NO</th>
<th>2 NO</th>
<th>3 NO</th>
<th>4 NO</th>
<th>5 N/A</th>
</tr>
</thead>
<tbody>
<tr>
<td>CarCall[3]</td>
<td>STUCK True</td>
<td>6 NO</td>
<td>7 NO</td>
<td>8 NO</td>
<td>9 NO</td>
<td>10 N/A</td>
</tr>
<tr>
<td>AtFloor[1,Down]</td>
<td>FAIL SILENT</td>
<td>11 NO</td>
<td>12 NO</td>
<td>13 YES</td>
<td>14 YES</td>
<td>15 or 2.3</td>
</tr>
<tr>
<td>DoorClosed[Left]</td>
<td>FAIL False</td>
<td>16 Either</td>
<td>17 NO</td>
<td>18 YES</td>
<td>19 YES</td>
<td>20 2.1</td>
</tr>
</tbody>
</table>
Rationale for answers to question #1. *Only* text in these boxes will be considered if an answer is challenged. *Solutions will Vary, see TA for specific issues on the grading of this item*
2. Dependability

A significant portion of the budget for maintaining elevators is spent on the time mechanics spend driving between repair jobs. This is a prime motivation for doing preventive maintenance and adding redundancy to increase reliability, thus eliminating the need for unscheduled repair visits. Because mechanics have to visit each elevator once a month to do adjustments and safety checks, it is highly advantageous to also do any repairs during that same visit. Note that most elevators are repaired under a maintenance contract, so any cost savings increase profitability for the repair service vendor, and any excess costs due to repeated mechanic visits must similarly be absorbed by the service vendor, reducing profits.

For this problem assume:

- Elevators are built by the factory with a single door motor shared by both doors – the independent door motors in the project assignment cost $500 to add, and this cost is absorbed by the maintenance company as a long-term investment in improving reliability. (If the single motor version fails the car traps passengers.)
- An emergency trip to an elevator by a mechanic costs $200 due to disruption in schedule and overtime pay.
- A non-emergency trip can be scheduled for the next business day when only one of two doors fails. A non-emergency trip costs $150.
- A mechanic visits every elevator every 30 days (= 1 “month” for this problem) for preventive maintenance and there is no extra cost for making a repair as well on such a visit.
- The failure rate of an elevator door motor is 237 failures per million operating hours (lambda = 237 * 10^{-6} per hour), and is the same per motor for single and dual motor elevator doors. Assume operation 20 hours/day, 30 days per month (and assume that the lambda is with respect to general elevator use, not just for the times the door motor is actually spinning).

2a) (9 points)
If the elevator were unmodified (i.e., for an elevator with only a single door motor), how many months on average would it take per elevator to incur $500 in costs from emergency trips, assuming one emergency trip were required for each and every door motor failure. This computes the break-even point for investing in the second motor. (Answer should be in # of 30-day “months”.)

\[
20 \text{ hours/day} \times 30 \text{ days} = 600 \text{ hours/month} \times 237 \times 10^{-6} = 0.142 \text{ failures/month.}
\]
\[
$500 = 2.5 \text{ emergency trips.} \quad 2.5 / 0.142 = 17.6 \text{ months to break even}
\]
2b) (30 points)
A new design is proposed that involves adding both a second motor and a cross-coupling device so that both doors will open even if one motor has failed. It is hoped that this will enable deferring motor maintenance until the next regularly scheduled maintenance visit, reducing costs. However, if elevator doors completely fail before they are repaired it will cause serious problems with customer relations. The cross-coupling device has a failure rate lambda of 24 per million operating hours (ten times better than the motors). Given that both doors are working after each maintenance visit, what is the probability that the cross-coupled door mechanism will still be able to operate the doors at the time of the next maintenance visit? (This is asking for a probability value that the doors won’t fail completely between maintenance visits; carry all computations to 6 significant digits.)

This is a parallel + serial system, and mission time is 20 * 30 = 600 hours.

\[
R(600)_{motor} = e^{-\lambda_{motor} \times t} = e^{-600 \times 2.37 \times 10^{-6}} = 0.867448
\]

\[
R(600)_{coupler} = e^{-\lambda_{coupler} \times t} = e^{-600 \times 24 \times 10^{-6}} = 0.985703
\]

Reliability of pair of motors is \(1 - (1 - R(600)_{motor})^2\) = \(1 - (1 - 0.867448)^2\) = 0.982430

Reliability of serial system (pair of motors + cross-coupler) = \(R(600)_{motor\_pair} \times R(600)_{coupler}\) = 0.982430 * 0.985703 = 0.968384

what this means in practice is that you’ll get a complete door failure on every elevator about once every 31.6 months if you don’t repair motors as they fail instead of waiting for the next monthly maintenance visit.
3. Testing

(24 points; 8 points per each of three arc traversals)
Project assignment #4 on testing is attached. Complete the MODULE TEST portion of that assignment (and NOT the system test) below, only for the DISPATCHER (11) shown in the solution design attached to this test.

The format of this answer for full credit is the contents of a test file that covers ALL THREE of the arcs on the dispatcher design.

Answers will Vary, any solution that tested each arc was acceptable.
4. **Following instructions**

(27 points; 3 points per page for a total of 9 pages)

Print your initials on each and every page of this test in the designated location.

Yes, we are serious – we have yet to get a complete set of tests with initials at the top of each page as requested. Ability to follow documentation requirements is just as important as design knowledge in the Real World.