Thomas Bahen - 260675971
Yahya Azami - 260535376
ECSE 422

Written Assignment 1

1. There are several downsides to fault masking. First, any fault masking system introduces additional components to prevent the fault from introducing an error in the system. These fault masking components need to be highly dependable in order to be effective which is typically expensive. Finally, fault masking may make the process of locating or even detecting a fault difficult which can affect how quickly faults are repaired.

2. Natural failures that could happen are things as inundations or poor weather conditions bringing down the electrical grid. Human failures could range from deleting the content of a database by accident or being the cause of a fire that wipes out local infrastructure that is hosting the content of the library system. Equipment failures might consist of the hardware being faulty (hard disks failing for example).

   To circumvent all these, having multiple backups of the whole system on the cloud so that recovery is possible would be wonderful. Restricting access to critical elements of the library system for employees and having a local generator in case power goes down could also be helpful.

3. The first example of a possible safety critical system requiring fault tolerance is a spacecraft's control system. Ideally the spacecraft should have redundancy in power supply and buses. Another example is the navigation system of a self driving car. Here redundancy is needed as well however it may take a different form. For example the sensors that inform the car of its position would need to have redundant sensors in various locations such that obstructions would not adversely affect back-up sensors.

4.

Q4. $\lambda = \frac{1}{8}$ $\quad F(t) = 1 - e^{-(1/8)t}$

$$P(T < 7 \mid 6 \leq T \leq 10)$$

$$= \frac{P(T<7) \cap P(6 \leq T \leq 10)}{P(6 \leq T \leq 10)}$$

$$= \frac{P(6 \leq T < 7)}{P(6 \leq T \leq 10)} = \frac{F(7) - F(6)}{F(10) - F(6)}$$

$$= \frac{\left(1 - e^{-(1/8)(7)}\right) - \left(1 - e^{-(1/8)(6)}\right)}{\left(1 - e^{-(1/8)(10)}\right) - \left(1 - e^{-(1/8)(6)}\right)}$$

$$= 0.2986$$

5.

a. The probability of the processor failing in the first year is

$$P(1) = 1 - e^{(-0.5)1^{0.6}} = 1 - 0.606 = 0.394$$

b. The probability of the processor failing in the year after 6 years of operation is

$$\frac{P(T<7) \cap P(T>6)}{P(T>6)} = \frac{P(7) - P(6)}{1 - 1 - e^{-0.5*6^{0.6}}} = \frac{e^{(-0.5)6^{0.6}} - e^{-0.5*7^{0.6}}}{e^{(-0.5)6^{0.6}}} = 0.135$$

6.

Q6. We have

$$R_{system}(t) = \left(1-(1-R(t))^4\right)\left(1-(1-R(t))(1-R^2(t))\right)$$

$$= \left(-R^4(t) + 4R^3(t) - 6R^2(t) + 4R(t)\right)$$
$$\left(-R^3(t) + R^2(t) + R(t)\right)$$

$$= R^7(t) - 5R^6(t) + 9R^5(t) - 6R^4(t) - 2R^3(t) + 4R^2(t)$$

at $t = 50$, $\lambda = 0.02$

$$R_{system}(50) = e^{-7(0.02)(50)} - 5e^{-6(0.02)(50)} + 9e^{-5(0.02)(50)}$$
$$-6e^{-4(0.02)(50)} - 2e^{-3(0.02)(50)} + 4e^{-2(0.02)(50)}$$

$$= 0.38103$$

7.

For clarity of calculation $R(t) = p$

The two central modules in parallel have a reliability:

$$(1-(1-p)^2) = 1-(1-2p+p^2) = 2p-p^2$$

We then add the top left module:

$$p(2p+p^2) = 2p^2-p^3$$

Then in parallel with the bottom module:

$$1-\left((1-(2p^2-p^3))(1-p)\right) = 1-(1-p-2p^2+3p^3-p^4)$$
$$= p+2p^2-3p^3+p^4$$

Finally, in series with the top right module we get:

$$p(p+2p^2-3p^3+p^4) = p^2+2p^3-3p^4+p^5$$

$$R_{system}(t) = R^2(t)+2R^3(t)-3R^4(t)+R^5(t)$$