Name: _____ **NetID:_____**

This homework is composed of four questions (20 points). Please work on the homework independently. Please print out this PDF file and fill-in answers within the spaces provided. The homework is due in hard copy on Sept 21th in class.

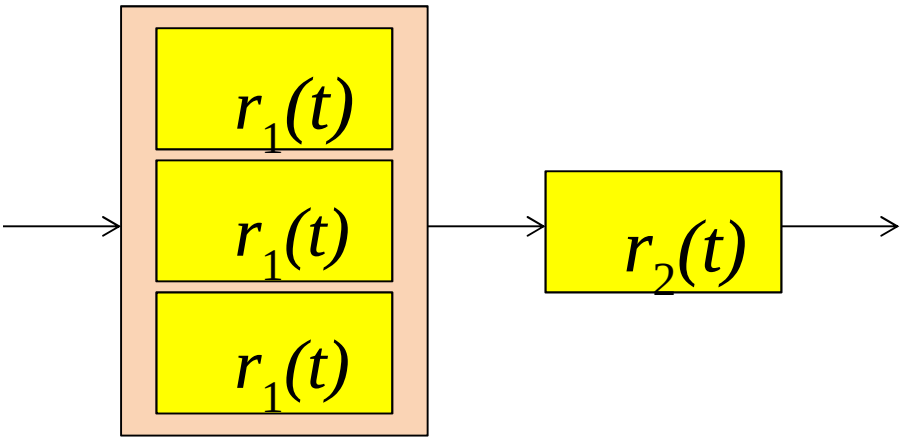
Homework 1

Q1: In March 2011, a massive Earthquake hit the coast of Japan, followed by a large tsunami. The Earthquake and the tsunami contributed different types of damage to the Fukushima nuclear reactor, setting off a series of events that ultimately led to core meltdown. Using Web resources at your disposal, plot a diagram showing the sequence of events that led to reactor failure. For an example of such a diagram, see lecture slides on the Three Mile Island reactor meltdown. **(5 points)**

Q2: The collision avoidance system in an autonomous vehicle consists of an obstacle detection function that has triple-modular-redundancy, followed by a speed control function, as shown below. Each individual version of the obstacle detection function has reliability r_1=0.87. Each version performs detection and raises an alarm if an obstacle is found that requires the vehicle to stop. You can assume that a failed component becomes silent and does not give any output. Hence, the speed control function stops the vehicle if at least *one* of the obstacle detection functions has raised an alarm. It has reliability r_2=0.96.

a) Which of the above components have to be functional in order for the car to successfully stop at obstacles? **(2 points)**

b) What is the reliability of the entire system? Please show your steps. **(3 points)**



Q3: You are to rank three architectural choices for building a NASA space exploration probe, where component repair and replacement are impossible. The system is to be composed of one or more components as will be described below. Assume that the reliability of a single component is given by the function, $r(t)=e^{-\lambda(C/E)t}$, where C is component complexity and E is the budget allocated to writing the component. Let t be measured in units of years. Assume that the mean time to failure of a component of unit complexity given a unit budget is ten years. Let us also assume that when multiple components are to be developed, your total budget is divided equally among them. For simplicity, assume that your total budget always adds up to 1. You are asked to rank three architectural choices in two cases: (i) the case of short missions (where the mission is to last three years), and (ii) the case of long missions (where the mission is to last 20 years). For purposes of this ranking, an architecture is deemed "better" if retains a higher reliability by the end of the mission. The three architectures compared are:

1. Architecture #1 (single component): An architecture composed of a single do-it-all component of complexity $C=1$.
2. Architecture #2 (TMR): A traditional triple-modular-redundancy architecture composed of three components of redundant functionality (of which at least two must be functional for the system to work), each of complexity $C=1$. Assume that the development effort (and budget) is *divided equally* among the three components.
3. Architecture #3 (Simplex): A system composed of one do-it-all component of complexity $C=1$ and another basic safety component of complexity $C=0.12$. The system remains safe as long as at least one of the two components works. Assume that the development effort (and budget) is *divided equally* among the two components.

Please attach more sheet as needed to show your reliability computations for each of the above three architectures and each type of mission. From these computations, fill in the computed reliability values in the table below and circle the best architecture for each type of mission.

(6 points)

The Reliability Table	Short Missions (3 years)	Long Missions (20 years)
Architecture #1 (single)		
Architecture #2 (TMR)		
Architecture #3 (Simplex)		

Q4: You are to design an improved pain control system for post-surgery patients in hospitals. In this system an infusion pump controls release of a pain medication (morphine) intravenously into a patient's bloodstream. There are two ways to request the medication. One is by pushing a button on a special handheld device. When the patient is awake, they can push the button to indicate being in-pain. However, when the patient is asleep, clearly they can't push the button. Instead, your system monitors their sleep via a smart camera that can detect "tossing and turning". If the camera runs experimental software that detects when the patient is not comfortable (e.g., moving a lot in their sleep), and if so, it request medication. The following components are available:

1. A push-button controlled by the patient to signal pain. The device has three interfaces: Bluetooth, WiFi, and USB. You are free to choose one to use.
2. A smart camera with integrated "discomfort detection" software that signals patient discomfort. It also has three interfaces: Bluetooth, WiFi, and USB. You are free to choose one to use.
3. USB cables
4. A laptop with WiFi, Bluetooth, and USB interfaces
5. The infusion pump with an internal processor and a WiFi interface (no Bluetooth or USB).
6. Control software to control amount of medication released.

a) Draw a diagram showing your architecture. The architecture should be as safe for the patient as you can make it. The diagram should show which of components 1 through 5 you will use (as rectangular boxes), and how they are interconnected (as lines between communicating boxes labeled by the mode of communication, such as WiFi, USB, or Bluetooth). It should also show where the control software (component 6) will run. If it runs on more than one component, indicate the software function of each. **(2 point)**

b) In your architecture, which components comprise the safety core (i.e., have to be very reliable for safety requirements to be met)? **(1 point)**

c) What constitutes a *safe state* in this system? **(1 point)**