Name_____ **NetID**_____

Homework 2: Please work on the homework independently. It is due Tuesday, Sept 20th, in class.

Q1: Please find the best answer to each of the following questions. (7 points)

1. A control loop made of a sensor, controller, and actuator is designed. The control function is critical. Which of the following design alternatives is better in terms of the dependency structure (in the sense of minimizing dependencies of critical functions)?

a) Wireless network control is used. The sensor and actuator are at the controlled plant. The controller is remotely hosted at a protected central location. A wireless network connects the controller to the sensor and actuator.

b) Internet control is used. The sensor and actuator are at the controlled plant. The controller is remotely hosted at a cloud server on the Internet. TCP/IP is used to connect the controller to the sensor and actuator over the Internet.

c) The sensor, controller, and actuator are hosted in a single physical unit at the plant, shielded from external interference.

2. Which of the following will likely have a higher reliability in the long term, if reliability is defined as being able to guarantee safety-critical functions only?

a) A system composed of a single component unit

b) A system composed of three redundant components

c) A system composed of a single component backed up by a simplified version of that component that carries out its safety-critical functions?

3. Which of the following items may contribute to decreased software reliability (check all that applies)?

a) Shorter product development (and time-to-market) cycles

b) Increased coupling between components

c) Increased system size

d) Component re-use (e.g., when components developed for one application environment are reused in another)

e) All of the above

4. A system has an average mean time to failure of 2 years. What are the chances that the system will remain operational for at least two years? (Pick the nearest number to the correct answer)

a) 100%

b) 67%

c) 50%

d) 35%

e) 17%

5. In the above system, what are the chances that it remains operational for 1 year?

a) 100%

b) 73%

c) 60%

d) 50%

e) 33%

6. A robot's camera can distinguish obstacles when they are within 8ft (or closer) from the robot. The maximum speed of the robot is 2ft/s. It takes 0.5s to stop the robot once a stop command is issued. A single-core microcontroller runs the robot software. If the time it takes to process a camera frame on this core is 1.3s, which of the values below would you recommend for the period at which frames should be acquired and image processing should occur?

a) 1 second

b) 2 seconds

c) 3 seconds

d) Any of the above will work well

e) Either (b) or (c), but not (a)

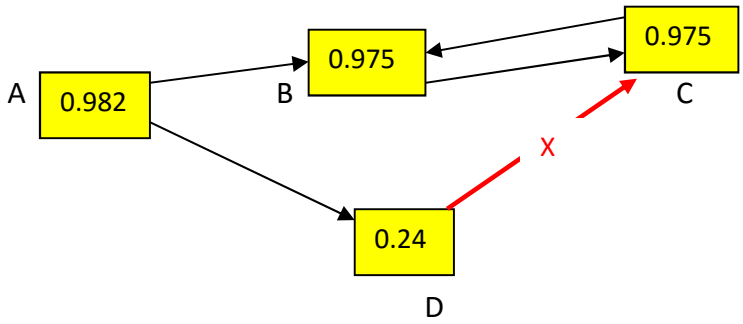
7. If the core in question (6) above was slower, such that it took 4.5 seconds to process a single camera frame, what is the maximum safe speed for the robot to prevent collisions?

0.84 ft/sec (See below).

Answer: Note that, frame acquisition must occur at a period of at least 4.5 sec (to allow for processing to complete before the next frame is acquired).

In the worst case, a frame is acquired right before the robot enters the 8 ft range (and so the obstacle is missed). One period later (i.e., after 4.5 sec), the next frame is acquired (now within range of the obstacle). It takes 4.5 more seconds to process it and detect the obstacle, and then 0.5 more seconds to stop. Hence, a robot that approaches an obstacle may keep moving for at most 4.5 + 4.5 + 0.5 =9.5 seconds (from entering detection range) before it stops. The range is 8 ft. Therefore, to prevent collisions, the robot should cover less than 8 ft in 9.5 seconds. In other words, speed should be lower than 8/9.5 = 0.84 ft/sec.

Q2: In the diagram below, each box represents a component. A link from component X to component Y indicates that Y depends on X. In other words, a failure in X causes a failure in Y. Each box is labeled by its reliability, when executed independently. **(3 points)**



a) Assuming that safety-critical components are more reliable, and that non-critical components are less reliable, are dependencies in the above system well-formed? (Only Yes/No please). If "Yes", skip part **b**.

Answer: _____No____

b) If your answer above was "No", clearly mark in the figure the link or links that violate(s) well-formed dependencies. (Put a clear "**X**" in the middle of each such link.)