Homework 1

Name: _____ **NetID:_____**

This homework is composed of four questions. 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 ~~12~~th 17th in class.

Q1: The page below has links to three major civilian nuclear accidents; (i) Chernobyl Accident, (ii) Fukushima Daiichi Accident, and (iii) Three Mile Island Accident.

https://www.world-nuclear.org/information-library/safety-and-security.aspx

Please read the description of each accident and choose (for each accident) one or two primary failure causes from the list below. This list enumerates some of the typical failure causes for cyber-physical systems. Explain why you picked the specific cause(s) in each case.

Primary causes:

(a) Human error, including miscommunication, not following procedure, etc.

(b) Reuse of a software component designed for a previous system that differed in fundamental assumptions from the system in which it was reused

(c) Failure to model corner cases in the physical environment: Events in the physical environments created unexpected correlations between failures that were thought to be independent during design.

(d) A combination of seemingly minor technical malfunctions that escalated to a catastrophic system failure

(e) A fundamental flaw in design that contributed to an unexpected positive feedback cycle. (Unexpected positive feedback is when measures designed to negate some unwanted effect actually contribute to it instead.)

Answers (2 points each, 6 points total):

(i) Chernobyl: Causes (choose one or two letters from the above): _____

Explain primary cause (if more than one, explain each in order of significance):

(ii) Fukushima: Causes (choose one or two letters from the above): _____

Explain primary cause (if more than one, explain each in order of significance):

(iii) Three Mile Island: Causes (choose one or two letters from the above): _____

Explain primary cause (if more than one, explain each in order of significance):

Q2: An autonomous navigation system consists of a primary-backup arrangement connected to the outside by a network bus. Both the primary and the backup modules have reliability r_m=0.942. The network has reliability r_N=0.98. What is the reliability of the entire system? (Note: compute system reliability with accuracy of four digits after the decimal point. Assume that, for the system to work properly, at least one of the primary or the backup has to work, in addition to the network.)

Answer (2 points):

Write system reliability equation (in terms of r_N and r_m) here:

→

Final numeric answer here: _____

Q3: A component of reliability, r(t), has a mean time to failure of 3 years. Which system configuration would have a higher chance of remaining operational after 1 year only? (Note that, triple modular redundant systems remain operational as long as (at least) two of three components remain operational.)

a) The component by itself

b) A triple modular redundant system, made of three such components (with independent failures)

Answer (a or b): _____ (1 point)

Q4: Repeat the above at a point in time that is 10 years later:

Answer (a or b): _____ (1 point)

Thank you and good luck!