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): **(a), (e)**

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

The first sentence in the description of the Chernobyl accident says: “The Chernobyl accident in 1986 was the result of a *flawed reactor design* that was operated with *inadequately trained personnel*”. Subsequent paragraphs explain both problems:

The design flaw: Positive void coefficient, resulting in increased power output with the addition of cooling water (which is the opposite of what you need when the reactor is already overheating).

The human error: According to the description “The operators deliberately and in violation of rules withdrew most control and safety rods from the core and switched off some important safety systems”.

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

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

An unusually strong earthquake hit Japan followed by a tsunami. The reactor would have withstood either the earthquake (one failure mode) or the tsunami (another failure mode) alone, but not the combination of both. (Note that these were not independent events: the earthquake caused the tsunami.) The earthquake disabled the external power supply to the reactor whereas the tsunami flooded the back-up generators in the basement causing a loss of power that lead to inability to properly cool the reactor: “six external power supply sources were lost due to earthquake damage, so the emergency diesel generators located in the basements of the turbine buildings started up”… “41 minutes later, at 3:42 pm, the first tsunami wave hit, followed by a second 8 minutes later. These submerged and damaged the seawater pumps … drowned the diesel generators and inundated the electrical switchgear and batteries, all located in the basements of the turbine buildings” … “there was a station blackout”.

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

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

We covered this example in class.

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:

→ $\mathbf{R = (1 - (1 - r_N)^2)\ r_m}$

Final numeric answer here: **0.9767**

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): (b) (1 point)

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

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

Thank you and good luck!