**HOMEWORK 3**

11.4 What is the common characteristic of all architectural styles that are geared to supporting software fault tolerance?

A system that provides fault tolerance will include redundant and diverse hardware and software.

11.7 It has been suggested that the control software for a radiation therapy machine, used to treat patients with cancer, should be implemented using N-version programming. Comment on whether or not you think this is a good suggestion.

Using multi-version programming to evaluate radiation therapy is a good method. If we have multiple system running cohesively on a hardware, which is set in the same settings, then if these two systems calculate the same output, the output should be correct. I am not sure how many would be required to produce the same output, but based on probability, the more machines required to produce the same output, the safer it is

11.9 Explain why you should explicitly handle all exceptions in a system that is intended to have a high level of availability

This is due to if they are not handled then the software will shut down. Software developers must provide exception for anything that could be detected and possible exceptions that may arise. If the software fails and the system shuts down

12.5 A train protection system automatically applies the brakes of a train if the speed limit for a segment of track is exceeded, or if the train enters a track segment that is currently signaled with a red light (i.e., the segment should not be entered). There are two critical-safety requirements for this train protection system: The train shall not enter a segment of track that is signaled with a red light. The train shall not exceed the specified speed limit for a section of track. Assuming that the signal status and the speed limit for the track segment are transmitted to on-board software on the train before it enters the track segment, propose five possible functional system requirements for the onboard software that may be generated from the system safety requirements.

1. Check whether the signal status is green for the upcoming section of a track (a)
2. Check whether train is going faster or slower than the intended speed limit for that section of track (b)
3. If (b) calculates that the train is going faster, apply brakes gently
4. If (b) calculates that the train is going slower, speed up gently
5. If (a) is red, search for another option of track segment that has a green signal status
6. If either (a) or (b) are not within the critical safety requirements, alert the human conductor