Assignment 1

Due Sunday Sep 24th at 11:59pm as a single pdf file submitted on Brightspace

Part 1: The Therac-25: 30 Years Later (5 marks)

Read the article "The Therac-25: 30 Years Later" by Nancy G. Leveson

Answer these questions by providing a brief explanation in a sentence or two. Each question is worth one mark. Note that a one-word answer (e.g., yes, no, maybe) will receive 0 marks.

a. Can we say that software by itself is safe or not?
b. At what phase of software development does safety first come into play?
c. Is it safer to reuse software or build from scratch?
d. Does using object-oriented technology lead to safer software?
e. Is it better, from the point of view of safety, to first implement normal and second error-handling behavior, or first error-handling and then normal behavior?

Part 2: Elevator installation use-case modelling (15 marks)

Watch Master Craftsmen - Elevator Installation

https://www.youtube.com/watch?v=BsY6CMCdtkc

Develop a use case model (use cases and use case diagram that relates these use cases) for the process of installing an elevator as presented in the video.

Part 3: Elevator Control System (20 marks)

Based on the elevator system specification below and corresponding parts of the Master Craftsmen video above develop:

1. Use cases that capture normal and exception-handling use, i.e. safety features.
2. The use case diagram that relates these use cases (from step 1).

Notes: To format your use cases, refer to Chapter 1 of "Writing Effective Use Cases" and for use case diagrams refer to http://www.agilemodeling.com/essays/umlDiagrams.htm.

Elevator system specification

A building is serviced by a group of M elevators (also called cars). On each of the N floors is a pair of buttons marked "up" and "down". When a button is pressed it illuminates, and remains illuminated, until an elevator arrives to transport the customers who, at this floor, have requested an elevator going in a certain direction. When the elevator arrives, it rings a bell, opens its doors (the elevator and floor doors) for a fixed time (10 seconds) allowing people to exit or board, rings the bell again, closes its doors

and proceeds to another floor. Once on-board passengers select one or more destination floors using a panel of buttons; there is one button for every floor. The elevator has a display which shows passengers the current floor of the elevator. There is also a pair of buttons on the elevator control panel marked “open door” and “close door”. These buttons can be used by a passenger to override the default timing of the doors. The door will remain open beyond its default period if the “open door” button is held depressed; the doors can be closed prematurely by pressing the “door close” button. Inside the elevator there is also a help button linked to building safety service.

Each elevator has a sensor that notifies it when it arrives at a floor. (The elevator control system should ensure that the group of elevators services all (floor and on-board) requests expeditiously.)

Each elevator has a display and an audio system. The display shows the current floor number and warning messages that are synced with audio warnings.

Safety features:

Help: The control system receives a “Help” alarm signal from an elevator indicating that the “Help” button has been pressed. In that case, the passenger is connected to building safety service through a voice connection. If there is no response from building safety within 5 seconds or if there is no response from a passenger a 911 emergency call is placed.

Door obstacles: If the light sensor is interrupted when the door is closing, the control system stops the door from closing and opens it. If this occurs repeatedly over a short period of time, a warning is sounded over the audio system and a text message is displayed.

Fire: The control system receives a “Fire” alarm signal from the building and commands all elevators to move to a safe floor. Similarly, a “Fire” alarm signal from the elevator itself will cause that elevator to go to a safe floor. In both cases an audio and text message are presented to passengers informing them of an emergency and asking them to disembark once the safe floor is reached.

Overload: The control system receives an “Overload” alarm signal from an elevator if the sensors indicate that the passenger or cargo load exceeds the carrying capacity. In that case, the elevator does not move and an audio and a text messages are presented to passengers asking for the load to be reduced before attempting to move again.

Power out: The control system receives a “Power Out” alarm signal. In that case, an audio and a text messages are presented to passengers informing them of the power outage. Each elevator is then moved to a safe floor and passengers are asked to disembark via audio and text messages. The battery backup power is sufficient to do all of this.