Assignment 1
COMP3004
Ryan Lo (101117765)

Due Sun Sep 25th 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 worthone 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?**

   Software by itself isn't safe or unsafe. It mainly depends on the context in which the software is being used. Most of the time software is flawed from its requirements and not the implementation. It depends on the number of safety requirements and the error-handling behaviors that are implemented. But most of the time, software is not safe.

b. **At what phase of software development does safety first come into play?**

   Safety first comes into play at the beginning of development. It can't be ensured if it isn't already there. If we want to reduce software-related accidents, we have to focus less on assurance and more on identifying the safety-critical requirements and building safety into the machines from the beginning of development.

c. **Is it safer to reuse software or build from scratch?**

   It is safer to build the software from scratch. Reusing software or using commercial off-the-shelf software does not increase safety just because the software has been used extensively. Reusing software that was safe in one system doesn't mean it will be safe when used in a different system. Safety is a quality of the system in which the software is used; it's not a quality of the software itself.

d. **Does using object-oriented technology lead to safer software?**

   Object-oriented technology does not lead to safer software. Object-oriented design is appropriate for data-oriented systems, it's not appropriate for control-oriented systems. The resulting software is more difficult to test for safety, trace from requirements to code, maintain without affecting safety, and assure the correctness of changes to safety-critical requirements. There is no one best way to design software for all types of systems.

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?

From the point of view of safety, error-handling should be implemented first then normal behavior. Ways to detect or prevent software errors should be designed in from the beginning. If written first, error-handling routines will get the most exercise. Many (and perhaps most) errors in operational software lie in the error-handling routines themselves. Programming languages that provide error protection, such as strong type checking, aren't always popular or used in safety-critical systems but are necessary for safety-critical systems.

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.

Use CASE 1: Installing an Elevator

Primary Actor: Elevator Installer
Scope: Island Elevator
Level: Summary
Stakeholders and Interests:
Elevator constructor – get the elevator working
Client – to have a working elevator
Precondition: none
Minimal guarantees: Elevator works but not perfect
Success guarantees: Elevator is installed correctly with no errors
Trigger: Client wants an elevator installed
Main success scenario:

1. Rail brackets installation
   - Spot brackets installation at topmost part of the shaft
   - Drop a plumb line to the elevator pit to line up lower brackets
   - Straighten rail brackets, leveled, and aligned
   - Install all other rail brackets.
2. Guide rails installation
   - Attach guide rails carefully guided into place
3. Computerized motion control system install
   - Installation of temporary run box to move the platform under construction
4. Car sling installation
   - Platform styles cross heads and both channel
5. Entrances/Door installation
6. Cab installation
7. Electrical Work
8. Programming of the elevator

Extensions:

1a. Rail brackets not set properly

1a1. Rail brackets will be off and every other item in the entire installation is set to the rail distance will be off also

4a. Car sling not put in correctly

4a1. Not proper and safely running elevator

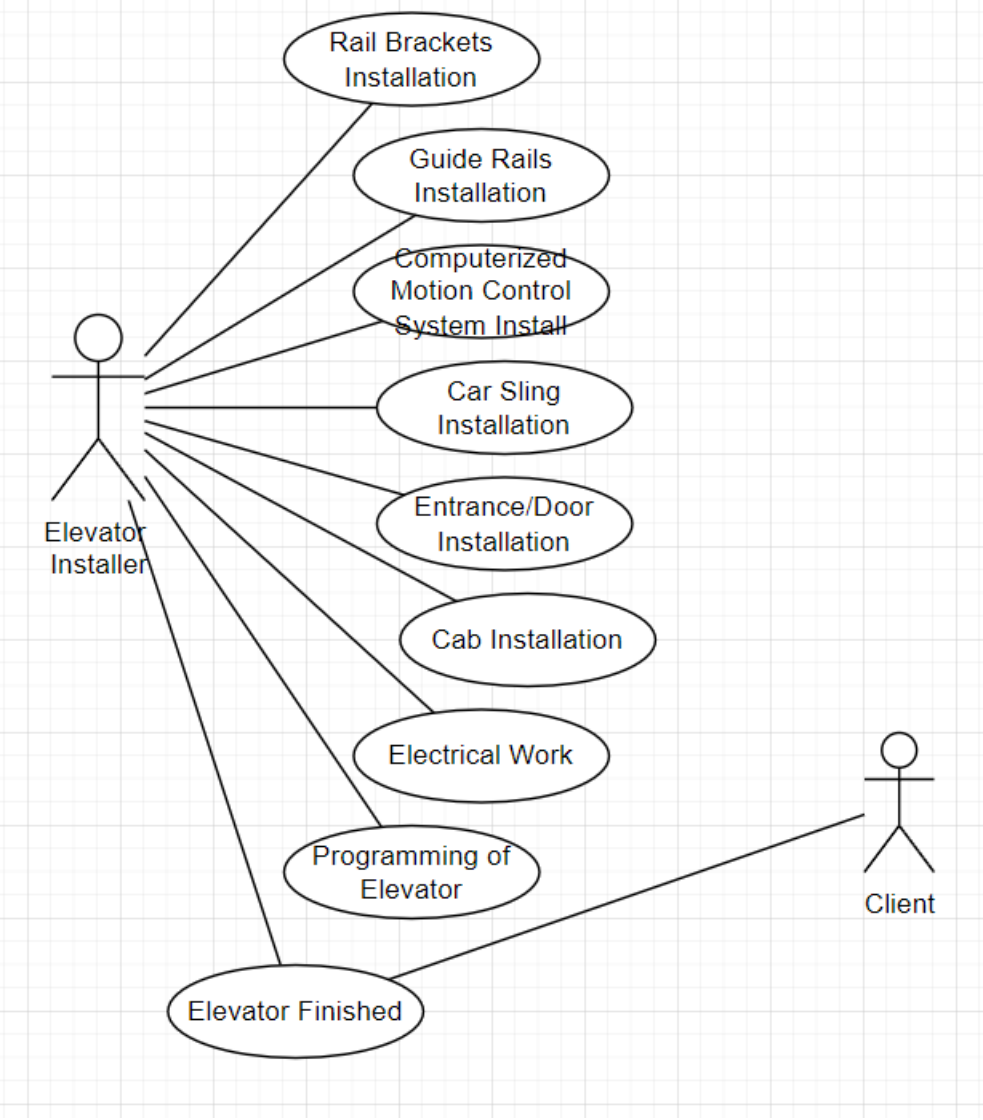
5a. Struts not installed well

5a1. Collision occurs

5a2. Doors that don't work

8a. Elevator does not work as it's supposed to

Use Case Diagram:



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.

1.

Use CASE: Using an Elevator

Primary Actor: Passenger
Scope: The building
Level: Summary
Stakeholders and Interests:
Passenger – wants to move to destinated floor
Building Safety – helps in case of emergency
911 – helps in case building safety does not respond
Precondition: elevator working
Minimal guarantees:
Success guarantees: passengers move to destinated floor safely
Trigger: passenger takes the elevator
Main success scenario:

1. Elevator button gets pressed
2. Elevator arrives and passengers board
3. Passengers select destination floor(s)
4. Doors close
5. Elevator takes off
6. Elevator arrives at the destinated floor

Extensions:
2a. Passengers overload
    2a1. Elevator load needs to be reduced
3a. Fire alarm goes off
    3a1. Elevator moves to safe floor
3b. Power goes out
    3b1. Elevator moves to safe floor
4a. Doors do not close
    4a1. Obstacle in the way
    4a2. Doors reopen to clear obstacle
5a. Elevator does not take off
    5a1. Help button is pressed
    5a2. Building safety response?
    5a3. 911 call

2.

Use Case Diagram