Comp 3004 Take Home Exam

April 27, 2020

Harris Ahmad

101055312

Part 1

A) Can we say that software by itself is safe or not?

- Base of the Therac article there is a clear realization that software alone is not safe at all but software which meets all of the software requirements is safe because the therac-25 had design and software implementation of the therac-20 there were issues with the requirements not being met the reason for the death of those people due to increased radiation.

B) At what phase of software development does safety first come into play?

- Safety plays a role through out but is carried out mostly in the requirements such as when a safety requirement is given the coder must implement it to make sure that, that is not an issue when device users are interacting with the device.

C) Is it safer to reuse software or build from scratch?

- Depending on the software it is realisable if it can be enhanced or a completely new version should be built. With the therac-20 to therac-25 it would have been good to realize all the new features and new error handlers from scratch because it is working with new tech but if you are working with the same tech and just adding more features to the design while considering the safety requirements for those new features it might be safer but those new features could impact old, there is definitely allot more to look out for when reusing software.

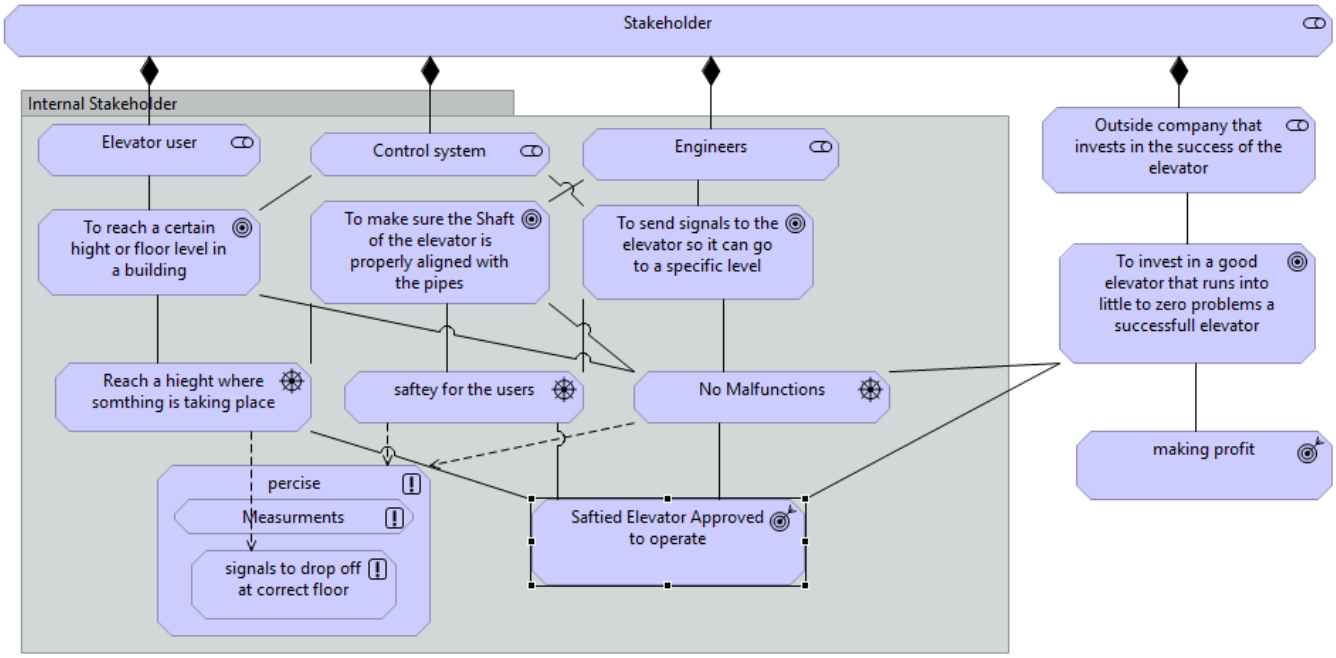
D) Does using object-oriented technology lead to safer software?

- Object-oriented programming is believed to be safer with the requirements but not all requirements are satisfied there could be a flawed requirement which impacts your software allot. If the requirements are perfect with no flaws OO is in fact safer

E) Is it better, from the point of view of safety, to first implement normal and second errorhandling behavior, or first error-handling and then normal behavior?

- Based off the article I believe it is safer to implement normal and second error handling because when implementing software you have to account for all the changes and once all the changes are made it would be a good idea to do the error handling because it will then account for all the changes you have made to the software and provide a safer output.

Part 2



As you can see from the image above there are multiple stakeholders to this elevator installation process, each with relations to one another through common goals and common drivers (concerns). There are a few internal Stakeholders (who hold the highest concern for this process) shown as, Elevator User, Control System and Engineers/Electricians. The one external stakeholder is those looking to make an investment towards one elevator company that is coming out with the most success.

To reach a certain height or floor level in a building is a basic but the most important goal in this elevator process. Stakeholders which see this goal are the elevator users and the control system operator. The concerns driving towards these goals are to ensure the floor level is reached where anything can take place and a main driver of having no malfunctions to ensure safety. All of the mentioned stakeholder, goals and drivers all refer to the core principle of being precise this means everything including measurements to signals that are sent to the elevator telling it to reach a certain height, everything must be on point. Following the principles and drivers the final outcome of this process should lead towards a safety certified elevator approved of running.

To make sure the shaft is properly aligned with the piping on the inside of the elevator is a main stressed goal for only the engineers that are at work here. This is

a high priority goal and as such has high priority drivers which are mainly, the safety of the users and to get each user to the proper floor level. All of this will lead to the same core principles of being precise and the outcome of a working elevator.

Sending waves of signals to the elevator is the most precise goal taken place by engineers and the control system operators because it is very important that every button on the elevator acts the way it should, the concern(driver) being here is to make sure no malfunctions take place and the safety of the user. The outcome will be again an approved operating elevator, if the principal of being precise is followed.

Elevator investors who are basically an outside concern for this elevator installation process have the main goal of investing in an operating elevator which is running successfully. This goal is driven by seeing an elevator with little to no malfunctions and will have the outcome of not only an approved elevator but also making profit from the elevator company.

Part 3

Use Case 1: Basic use

Description: this use case describes how users would reach any floor

Actors: Elevator users

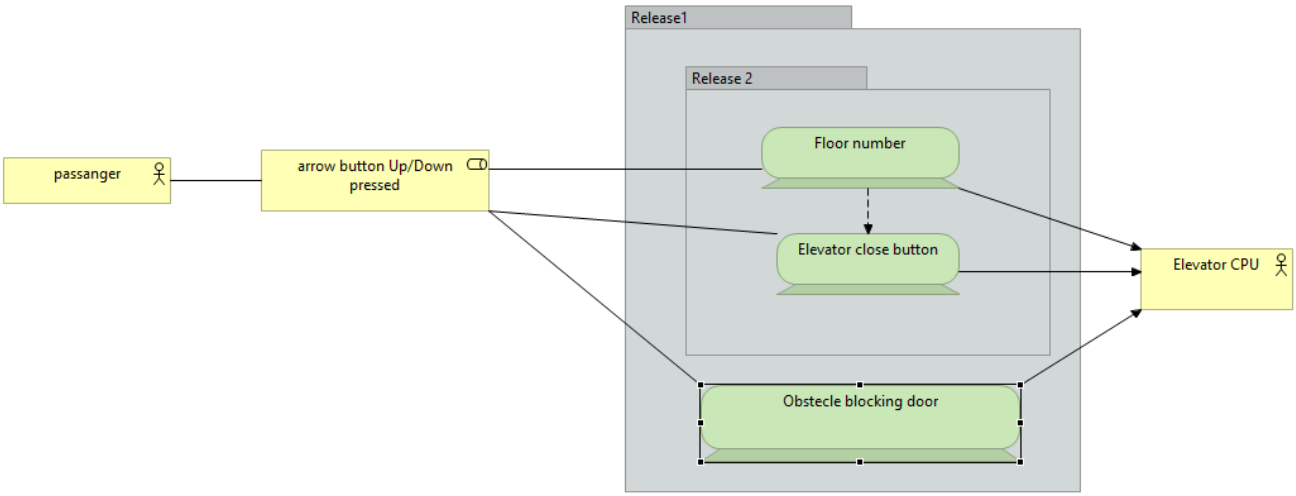
Trigger: User presses the up or down button on the outside of the elevator

Pre-Condition: The elevator is pre tested and safety checked for passengers to board and to operate

Main Sequence:
1. User presses up or down button on elevator sending a signal to the elevator CPU
2. upon arrival the elevator sends a noise to passenger to let passenger know it has arrived
3. Now user enters and is shown multiple options on a board panel, the user presses one of the buttons and the elevator door shuts
4. Another signal is sent to the mother board CPU of the elevator and the elevator is commanded to move based off the button pressed
5. elevator reaches the destined floor and a noise is again presented to make the passenger aware
6. user steps off and elevator door proceeds to shut behind him continuing to next passenger

Post condition: if objects are placed Infront of the door sensor the door will not shut as a safety precaution

Resulting event: The passenger gets off at desired floor



Use Case 2: Help

Description: this use case describes the procedure to take when a passenger is in emergency assistance

Actors: Elevator users

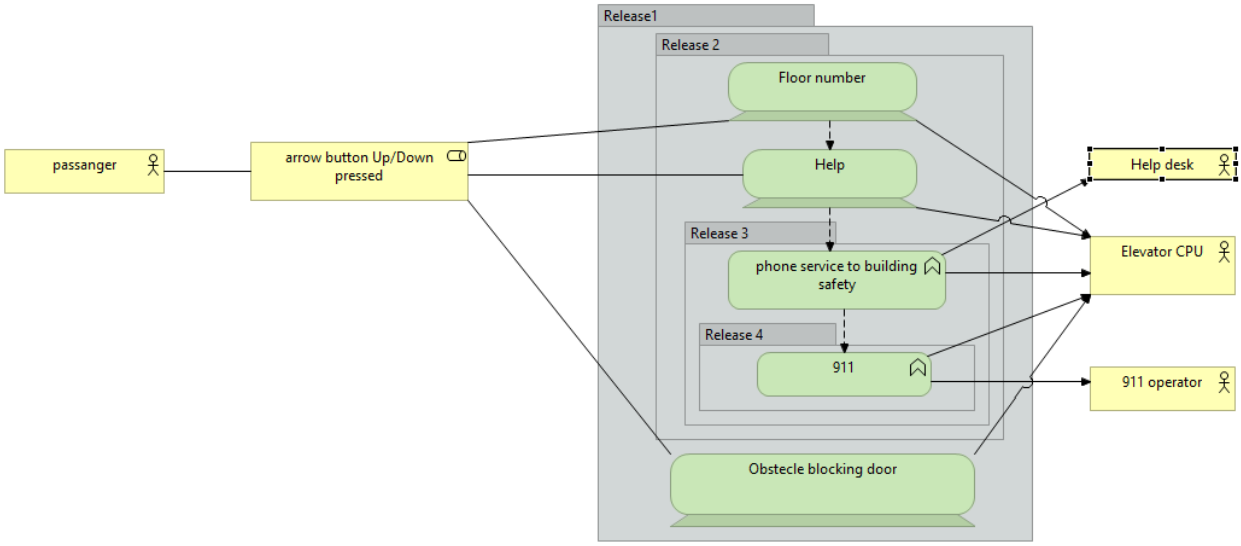
Trigger: User presses the help button in elevator panel selection

Pre-Condition: The elevator is pre tested and safety checked for passengers to board and to operate

Main Sequence:
1. User presses up or down button on elevator sending a signal to the elevator CPU
2. upon arrival the elevator sends a noise to passenger to let passenger know it has arrived
3. Now user enters and is shown multiple options on a board panel, the user presses one of the buttons and the elevator door shuts
4. Now an emergency has happened and the passenger needs help he/she presses the help button clearly indicated
5. the CPU of the elevator notices this and connects user to building safety services respond with in 5 sec
6. In the case 5 sec is exceeded and there is no response the system places an emergency call to 911
7. passenger is connected and can relay message to 911 through voice box and can hear through speakers

Post condition: if objects are placed Infront of the door sensor the door will not shut as a safety precaution

Resulting event: The passenger gets help!



**release 4 is activated only after 5 sec if release 3 is not realized

Use Case 3: Fire

Description: this use case describes the procedure for when a fire occurs

Actors: Elevator users

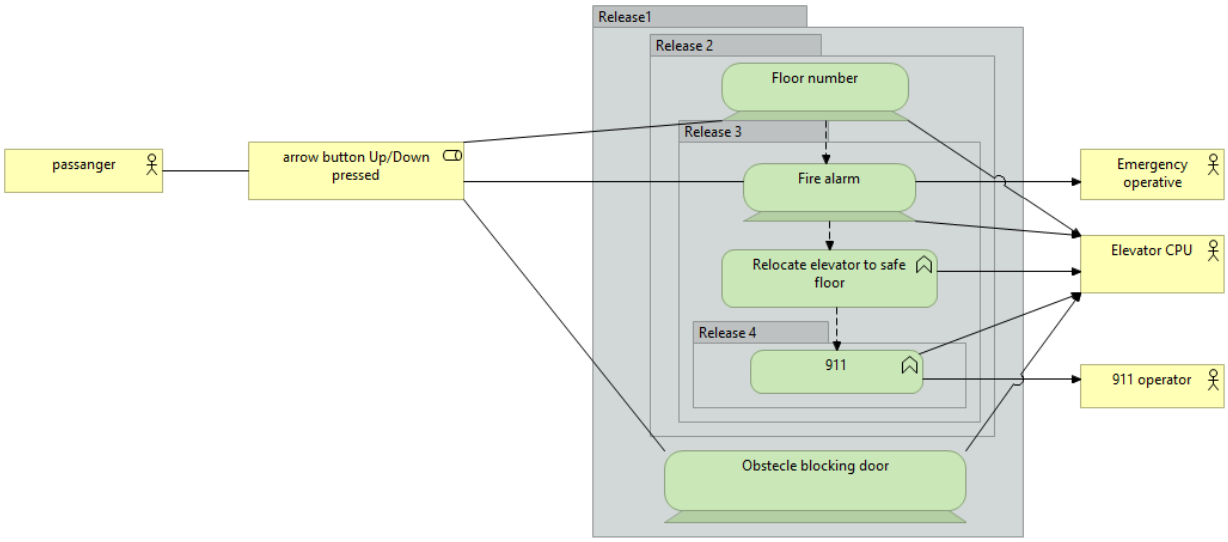
Trigger: a fire alarm in the building is pressed or detected

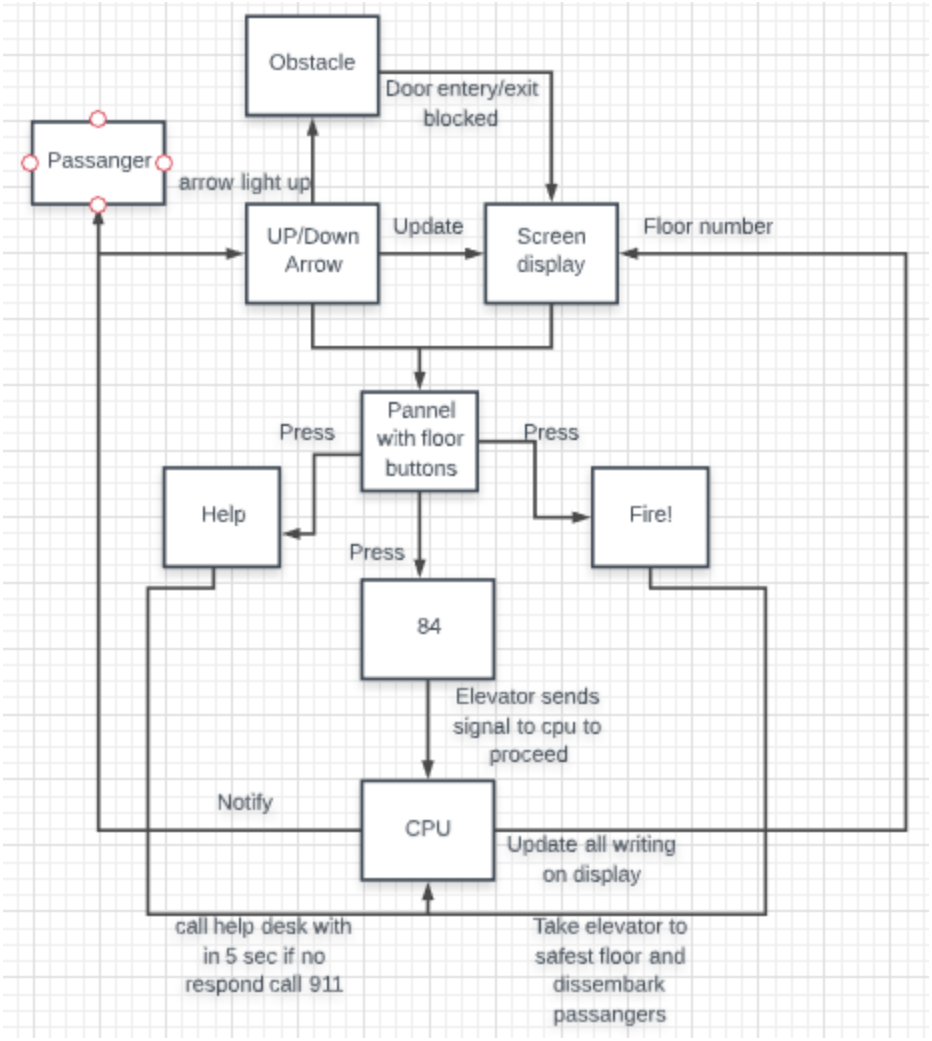
Pre-Condition: The elevator is pre tested and safety checked for passengers to board and to operate

Main Sequence:
1. User presses up or down button on elevator sending a signal to the elevator CPU
2. upon arrival the elevator sends a noise to passenger to let passenger know it has arrived
3. Now user enters and is shown multiple options on a board panel, the user presses one of the buttons and the elevator door shuts
4. Now an emergency has happened there is a fire, the elevator receives commands immediately to proceed to a safe floor
5. The elevator sends out a pre recorded message through audio and text which is displayed on a screen that an emergency has occurred and to leave as soon as a floor is reached
6. if the fire alarm is pressed from with in the elevator repeat step 5
7. The floor is reached and passengers disembark

Post condition: if objects are placed Infront of the door sensor the door will not shut as a safety precaution

Resulting event: The passengers are all able to tell there is an emergency and exit!




Obstacle
Door entery/exit blocked
Passanger
arrow light up
UP/Down Arrow
Update
Screen display
Floor number
Pannel with floor buttons
Press
Press
Help
Fire!
Press
84
Elevator sends signal to cpu to proceed
Notify
CPU
Update all writing on display
call help desk with in 5 sec if no respond call 911
Take elevator to safest floor and dissembark passangers