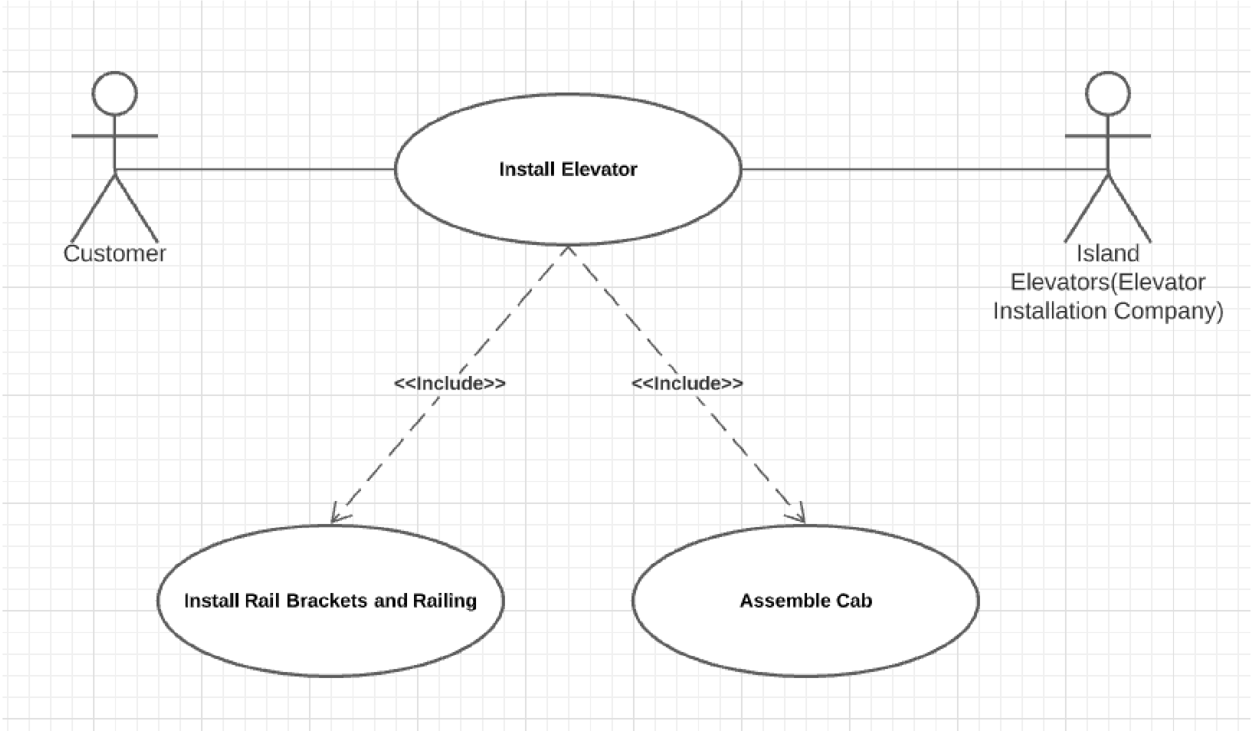
Part 1

a. We can not say that software on its own is safe or unsafe. Its safety is dependent on the context in which the software is run in. [1]
b. It should come into play during the design of the software.
c. Reusing software because it has already been tested does not make it safe or unsafe. What makes the software safe is looking at the software and the context it will be used in, so, I believe, that building the software from scratch will allow you to account for its safety in its design
d. No, it does not. In fact, the article states that OO technology is not appropriate for control-oriented systems and is more difficult to test for safety. [1]
e. It is better to implement the error-handling code first because, as stated by Leveson [1], it will receive more focus if it is written beforehand.

Part 2


Customer
Install Elevator
Island Elevators(Elevator Installation Company)
<<Include>>
<<Include>>
Install Rail Brackets and Railing
Assemble Cab

Use Case 1: Install Elevator
<u>Primary Actor:</u> Customer
<u>Scope:</u> Elevator installation company(“Island Elevator”)
<u>Level:</u> Summary
<u>Stakeholders and interests:</u>
Customer - have a working elevator installed in building
Island Elevator - install elevator and get paid for installation
Elevator Inspector - ensure that elevator passes safety tests
<u>Precondition:</u> Elevator shaft in building is properly framed according to architectural drawings

Minimal Guarantees: Unsafe elevator system will be identified and not used
Success Guarantees: Elevator is installed, passes inspection and is ready to be used by client
Trigger: Customer requests installation of elevator system
Main Success Scenario:

1. Install rail brackets and railing in elevator shaft(See use case 2)
2. Install selector and place position magnets on selector tape relative to floors
3. Install computerized motion control system
4. Instal temporary runbox
5. Install car sling
6. Set entrances
7. Measure placements of entrances
8. Install struts
9. Assemble cab(See use case 3)
10. Complete door frame
11. Install landing doors
12. Install cab
13. Check elevator speeds are compliant with elevator code
14. Connect wiring for car control board, buttons/switches at floor landings, connections to control board
15. Verify buttons and switches are functioning to code
16. Check various safety systems
17. Paint elevator
18. Elevator is inspected by certified elevator inspector

Extensions:

2a. Position magnets are misaligned to respective floors
    2a1. Place the magnets relative to floors and measure
    2a2. Magnets should be aligned to floors and use case continues
7a. Entrance placements are not properly aligned within ¼” of rails
    7a1. Reinstall entrances and measure again
    7a2. Entrances are now aligned and use case continues
13a. Elevator speeds are not compliant with elevator code
    13a1. Adjust elevator speeds
    13a2. Check elevator speeds
    13a3. Elevator speeds are now compliant with elevator code and use case continues
15a. Buttons and switches are not functioning to code
    15a1. Reinstall buttons and switches
    15a2. Should be functioning to code
16a. Safety system fails
    16a1. Reinstall related parts
    16a2. Safety system should pass
18a. Elevator fails inspection and is not certified by elevator inspector
    18a1. Elevator can not be used by customer and use case ends

Use Case 2: Install Rail Brackets and Railing
Primary Actor: Elevator technician
Scope: Elevator system
Level: Summary
Stakeholders and interests:
Elevator technician - properly installs rail brackets and railing according to spec
Customer - have a working elevator installed in building
Island Elevator - install elevator and get paid for installation
Elevator Inspector - ensure that elevator passes safety tests
Precondition: Elevator shaft is properly framed according to architectural drawings
Minimal Guarantees: improperly installed rail bracket and railing will be identified and not used
Success Guarantees: rail brackets are properly installed
Trigger: Elevator shaft framing is complete
Main Success Scenario:

1. Install spot brackets at top most part of shaft
2. Drop plum line to elevator pit
3. Install rail brackets on both sides of each floor
4. Measure real brackets alignment
5. Place guide rail with chain hoist

Extensions:
4a. Rails are misaligned more than 1/64”
4a1. Reinstall rail brackets and measure again and use case continues
5a. Chain hoist is not 1 tonne
5a1. Replace chain hoist with 1 tonne version

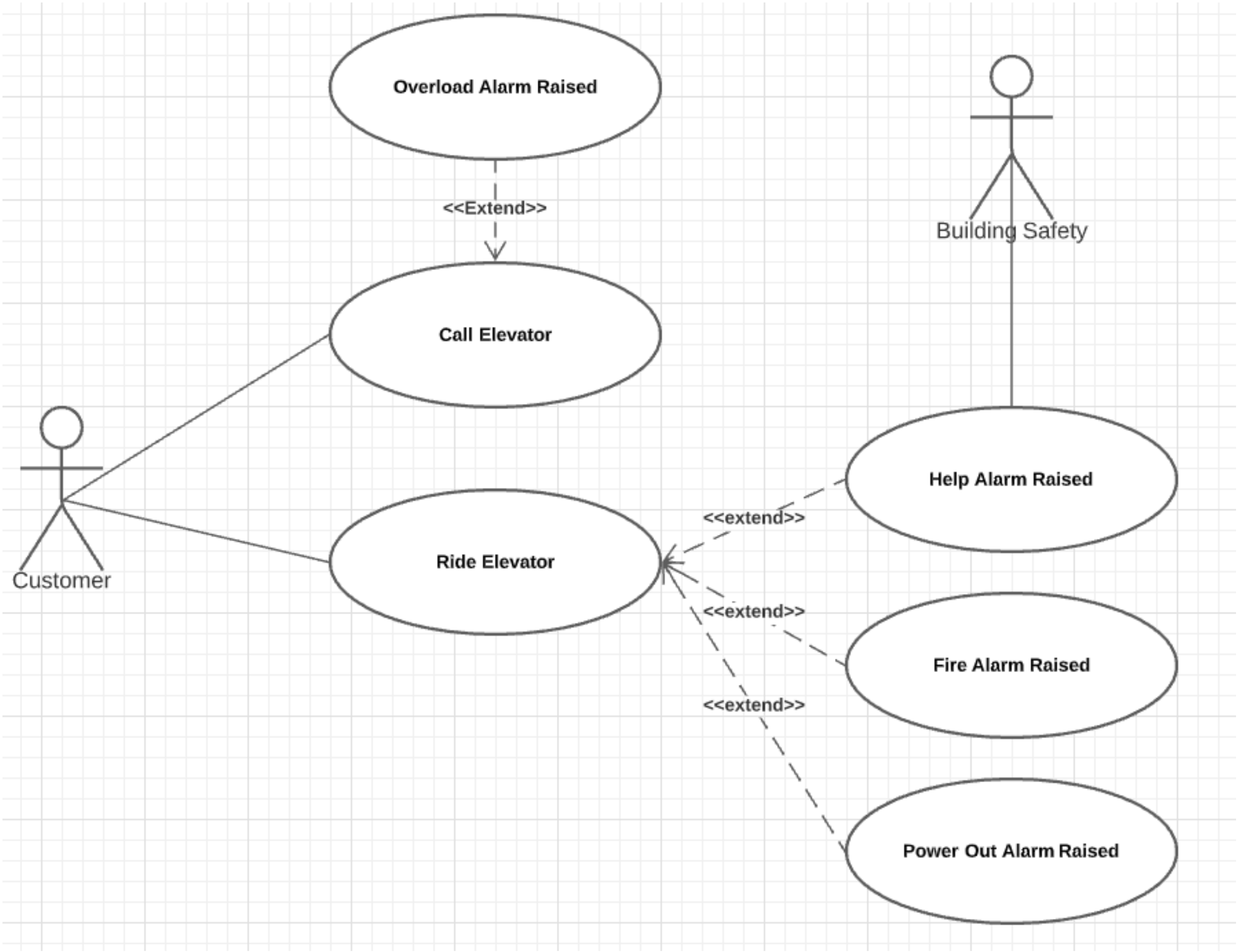
Use Case 3: Assemble Cab
Primary Actor: Elevator technician
Scope: Elevator system
Level: Summary
Stakeholders and interests:
Elevator technician - properly assembles cab
Precondition: Struts are properly installed, all cab parts are at site
Minimal Guarantees: improperly installed or incomplete cab will be identified and not used
Success Guarantees: cab is properly installed and can be used with rest of elevator system
Trigger: Elevator shaft framing is complete
Main Success Scenario:

1. Loosely join side and rear interior walls on top of platform
2. Unpackage dome and ceiling units
3. Assemble front panel of cab
4. Attached dome
5. Join door motor drive unit to cab
6. Anchor parts to platform

Extensions:

6a. Parts are not properly anchored
6a1. Cab is re-anchored to dome
6a2. Use case continues

Part 3



Use Case 1: Call Elevator

<u>Primary Actor:</u> Customer
<u>Scope:</u> Elevator system
<u>Level:</u> User Goal
<u>Stakeholders and interests:</u>
Customer - wants to board elevator
Building owners - want to make sure that elevator is safe for all customers who ride it
<u>Precondition:</u> Customer is at floor with elevator access
<u>Success Guarantees:</u> Elevator reaches customer’s floor for boarding
<u>Trigger:</u> Customer wishes to board elevator to go to a different floor
<u>Main Success Scenario:</u>

1. Customer presses either “up” or “down” button
2. Button illuminates

3. Elevator arrives to Customer’s floor, rings a bell, and opens its doors
4. Elevator doors remain open for 10 seconds allowing the customers to board or exit
5. Customer boards elevator
6. Elevator bell rings again and door closes with passengers inside elevator

Extensions:

4a. Passenger presses “close door” button within the elevator
 4a1.Elevator closes before 10 second time limit

5a. Passengers/cargo load exceeds carrying capacity
 5a1. Overload alarm is raised (Use Case 4)
 5a2. Passengers disembark until load does not exceed carrying capacity of elevator or use case ends

6a. Light sensor is interrupted while door is closing
 6a1. Control system stops elevator door from closing
 6a2. Obstruction is removed, door is closed and use case continues or a warning is sounded over the audio system and a text message is displayed

6b. Passenger presses “open door” button within the elevator
 6b1. Elevator door remains open as long as button is depressed
 6b1. Step 6 in use case is repeated

Use Case 2: Ride Elevator

Primary Actor: Customer

Scope: Elevator system

Level: User Goal

Stakeholders and interests:

Customer - wants to ride elevator to desired floor

Building owners - want to make sure that elevator is safe for all customers who ride it

Precondition: Customer is a passenger within the elevator

Success Guarantees: Customer reaches desired floor

Trigger: Customer has boarded the elevator

Main Success Scenario:

1. Passenger selects one or more floors using panel of buttons that includes every floor in building that elevator goes to
2. Elevator proceeds to floors selected
3. Elevator display shows current floor elevator is on
4. Elevator arrives to selected floor(s)

Extensions:

2a. Fire alarm is raised from outside or within the elevator
 2a1. Elevator overrides selected floors and travels to a safe floor
 2a2. Audio and text message are displayed to passengers informing them that it is an emergency and they must disembark when elevator reaches the safe floor
 2a3. Elevator reaches the safe floor

2b. Power is cut
 2b1. Elevator uses backup power source
 2b2. Control system receives a “Power Out” alarm signal

2b3. Elevator overrides selected floors and travels to a safe floor
2b4. Audio and text message is presented to passengers informing them of the power outage.
2b5. Elevator reaches the safe floor
2b6. Another audio and text message is displayed asking passengers to disembark

Use Case 4: Overload Alarm Raised

Primary Actor: Customer
Scope: Elevator system
Level: Summary
Stakeholders and interests:
Customer - wants to ride elevator to desired floor
Building owners - want to make sure that elevator is safe for all customers who ride it
Precondition: Passengers/load exceed carrying capacity of elevator
Success Guarantees: Customer reaches desired floor
Trigger: Passengers/load exceed carrying capacity of elevator
Main Success Scenario:

1. Sensors indicate passengers/cargo exceed carrying capacity
2. Elevator stops moving
3. Audio and text messages are displayed to passengers asking for the load to be reduced
4. Passenger’s disembark elevator, reducing load below carrying capacity of elevator

Extensions:

4a. Passenger’s do not disembark elevator and load is not reduced
4a1. Use case is repeated

References

[1] N. Leveson, “The Therac-25: 30 Years Later,” *The IEEE Computer Society*, pp. 8–*11*, Nov. 2017. Accessed on: Oct. 03, 2021. [Online]. Available: https://brightspace.carleton.ca/d2l/le/content/61834/viewContent/2220174/View