Kenji Isak Laguan 101160737

Part 1 The Therac-25: 30 Years Later

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

Software is safe or unsafe by itself as safety depends on context in which the software is used. Almost all accidents with software is because of flawed software requirements and not how it was implemented. Even though software is satisfying the requirements given it still can be not safe. The part that determines whether a software is safe or unsafe is the safety-critical software requirements. Where there are some requirements not identified that would be detrimental to safety but wasn't implemented.

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

Safety should come into play at the beginning phase of developing the software. Safety cannot be guaranteed if it wasn't already there being implemented from the beginning.

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

It most likely is safer to build from scratch. This is because the assumption of reusing software is safer. What might be safe for one application of the software may not be safe in a different one. The safety lies in the quality of system the software is used and not the software itself. Reusing software and ensuring it is up to today's standards and make modifications that meets the safety-critical requirements of the differing system can be possible. But building from scratch would be safer as safety should be implemented from the beginning.

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

No it doesn't as this technology is appropriate for data-oriented systems, but not for control-oriented systems. That technology causes: the increased difficulty in testing the software for safety, tracking requirements to code, maintaining software without compromising safety, and ensuring the accuracy of modifications to safety-critical requirements.

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 a safety standpoint, it is better to implement error-handling first as it should be designed and implemented from the beginning, then normal behavior. As many errors are due to the error-handling routines. But having them implemented first allows the error-handling routines to run more and prevent unforeseen errors in future normal behavior coding.

Part 2 Elevator Installation Use Case Modelling:

Use Case: Install an Elevator

Primary Actor: Elevator Installers, Plumbers, Electricians, Carpenters

Actor(s):

Elevator Installers (general) – used as umbrella term when not sure which trades men is used.

Electricians, Plumbers, Carpenters

Precondition: Elevator shaft is already framed in the building.

Goal/Postcondition: The elevator is successfully installed and will pass inspection.

Main success scenario:

1. Installers install the Brackets and Rails
    a. Drop a plumb line in the elevator shaft to be used for aligning spot and rail brackets.
    b. Install spot brackets (aligned and levelled) at the top of the elevator shaft.
    c. Install rail brackets (aligned and levelled) on each side of every floor.
    d. Attach the guide rails to the rail brackets using a chain hoist.
2. Installers Install the guide shoes onto the guide rails.
3. Plumbers Install the plumbing.
    a. Install the hydraulic pump.
    b. Install the hydraulic pistons on each side.
    c. Fill the system with oil.
4. Installers Install the piston sensors on each side.
5. Installers Install the selector tape and the position magnets.
6. Installers Install the selector device.
7. Electricians Install the computerized motion control system.
    a. Add in control jumpers. (These bypass safety devices during construction)
    b. Wire in the temporary run box (to move the elevator during construction)
8. Installers and Carpenters Install the Car Sling onto the pistons and rails (both square and plumb)
    a. Carpenters Install the platform.
    b. Installers Install the stiles.
    c. Installers Install the cross heads.
    d. Installers Install the bolster channel.
9. Installers Install Struts
    a. Take precise measurements for the struts.
    b. Install the struts at each landing of floors.
    c. Install the brackets for the struts (holds them into place).
10. Installers Install Entrances
    a. Install the Hoistway sill at each entrance at each level.

    b. Install the Cab sill at this phase.
    c. Align the Hoistway sill and Cab sill.
11. Installers Install the Door Box.
    a. Install the Landing Header at the top of the entrance at each landing (completes the frame for the Door Box).
    b. Install Door Box then secure it top and bottom.
12. Installers Install the Landing Door
    a. Install the Landing Door (which has rolling casters) onto the Landing Header.
    b. Install the Gibbs onto hoist sill (these keep the landing door on the tracks).
    c. Verify alignment and level of the header and hoist sill.
    d. Verify the door slides with ease.
13. Installers Assemble the Cab.
    a. Loosely join the sides and rear interior walls and place on top of platform.
    b. Unpack and assemble the dome and ceiling unit (to finish the top of the elevator).
    c. Install the strike and return columns.
    d. Assemble the front panels of the car (includes car operating station) and place onto the platform.
    e. Attach the dome.
    f. Place the door control and motor drive unit atop the front of the cab. Join them with the front walls and the dome.
    g. Tighten all parts, double check for square and anchor the cab onto the platform.
    h. Attach the cab door onto the door operator, make any adjustment until door is moving smoothly.
    i. Install Gibbs onto cab door (to keep cab door in line with cab sill).
    j. Install the door clutch assembly and make any adjustments needed.
    k. Install the locking mechanism for the door and adjust for proper operation.
    l. Install Obstruction Sensors onto the door.
14. Electricians Install the Electrical Wirings.
    a. Install the wirings on top of the elevator for the lights and ventilation fan.
    b. Install high voltage wiring connected to the various electrical systems needed.
    c. Install low voltage wiring for connections between computer and the devices and sensors.
    d. Install the bulk cable wiring for the computer and control systems.
    e. Field wire all remaining car control systems.
    f. Remove the control jumpers (that was installed in step 7a).
    g. Remove the temporary run box (that was installed in step 7b).
15. Installers Adjust and fine tune the elevator to make sure it’s up to code.
    a. Control the elevator form the inspection station on top of the car.
    b. Do a complete inspection of all the elements inside of the elevator shaft. Verifying co compliant operation as they go.
    c. Any minor adjustments needed for door latches and sensors are corrected/repaired by Constructors.

d. Fine tune elevator speeds by adjusting hydraulic pump valves till the speed is compliant to engineer specs and elevator code.
e. Finish remainder controller wiring and control systems wiring this marks the wiring completed.
f. The computer sets the elevator to fully automatic control.
g. All the elevator buttons, switches, and systems are tested to ensure proper function to code.
h. Door safety sensors are tested to verify working order and the door opens when an obstacle interrupts the light curtain.
i. Fire safety systems are tested to verify if the elevator recalls to the proper floors in case of an emergency.
j. Correct any other discrepancies.
k. Tidy up anything needed and finish painting.

16. The elevator is finished the installation.
17. For the client to use the elevator an inspection for the elevator needs to be performed to get its license.

Extensions:

1-15a. Any part of the elevator that wasn't installed, plumbed, wired, aligned, or levelled correctly.

1-15a1. Restart the work of that step as its needed to ensure proper installations.

Use Case: (step 17. from Install an Elevator use case) Inspect an Elevator

Primary Actor: Elevator Inspector

Actor(s): Elevator Inspector

Precondition: Elevator is finished installation.

Goal/Postcondition: The elevator successfully passes inspection and gets licensed.

Main success scenario:

1. Schedule an inspection with a certified elevator inspector that's recognized by the authority that has jurisdiction in this municipality.
2. When the inspection happens, the inspector will perform a 150 point test.
    a. Inspect every electronic device.
    b. Inspect every safety device.
    c. Go through every scenario that may or may not encounter the elevator plus the passenger(s) over the course of the lifetime of the equipment.
    d. Do a full load weight test to make sure the elevator stops at the floor and the doors open at the floor where people can enter and exit safely.
3. If the elevator passes the 150-point test/inspection, issue the license for the elevator.

Extensions:

1a. Scheduling conflict.

1a1. Reschedule the inspection.

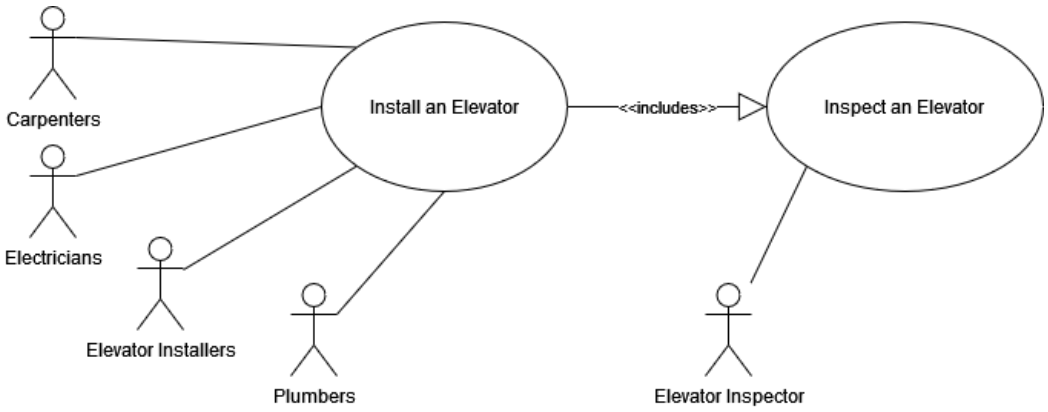
2a. If any of these tests do not pass inspection

2a1. Continue with inspection and note what needs to be fixed.

3a. Failed the inspection.

3a1. Let client know what needs to be fixed and do not issue a license.

Use case Diagram:



Part 3: Elevator Control System

Use Case: Using an elevator to travel from floor A to floor B.

Primary Actor: Passenger

Actor(s): Passenger

Precondition: There is at least one working/operating Elevator in the group of M elevators in the building. A fire hasn't occurred. A power outage hasn't occurred. A crisis hasn't occurred.

Goal/Postcondition: The Passenger arrives safely at floor B using an elevator.

Main success scenario:

1. On floor A, passenger walks up and presses an elevator button.
    a. If floor B is below floor A, then press the down button.
    b. If floor B is above floor A, then press the up button.
2. Once the elevator arrives.
3. Wait for the doors to open.
4. Board the elevator.
5. Wait for elevator door to fully close in 10 seconds or press the close door button,
6. Press the floor B button on the panel of buttons inside the elevator.
7. Wait till the elevator travels to designated floor B.
8. Once the elevator has arrived at floor B (verified by looking at the display that marks the current floor inside the elevator or listening to the audio message played at the floor).
9. Wait for the doors to open.
10. Exit the elevator onto floor B.

Extensions:

1a. If elevator button doesn't illuminate.
    1a1. Call a different elevator and restart the use case.

4a. If there are passengers.
    4a1. If there is no more room in the elevator as none need to leave, then call a different elevator and restart the use case.
    4a2. If there is room in the elevator as some passengers left, then board the elevator.

4b. The Overload alarm signal activates.
    4b1. Exit the elevator as the load is too much for the elevator to handle and call a different elevator to restart the use case.

5a. A light sensor picks up any obstacle that blocks the door closing and cause it to open again.

5a1. The passenger may wait for the door to close again in 10 seconds once the obstacle is cleared.

5a2. The passenger may press on the close door button once the obstacle cleared.

5a3. If the sensor picks up the obstacle repeatedly to which a warning is played. Clear the obstacle if there is any and wait for the doors to close or exit the elevator to call a different elevator and restart the use case.

6a. If floor B button is already illuminated

6a1. Passenger may choose to not press floor B button or press floor B button. (Assuming that this elevator buttons illuminate as well.)

7a. A fire has occurred during elevator travel and the control system receives a fire alarm signal; thus, the fire safety feature is enabled.

7a1. Once the elevator arrives to a safe floor, follow the informed message of the elevator to exit the elevator, and take the stairs if needed to exit out of the building.

7b. A power out has occurred during elevator travel and the control system receives a power out alarm signal; thus, the power out safety feature is enabled.

7b1. Once the elevator arrives to a safe floor, follow the informed message of the elevator to exit the elevator.

7c. An unexpected crisis occurs that's not detected by the control system.

7c1. A passenger is in crisis, press the help button which sends an alarm signal to the control system. Await response from building safety within 5 seconds. If there is no response from a passenger, await a response from 911.

7c2. The elevator gets stuck, press the help button which sends an alarm signal to the control system. Await response from building safety within 5 seconds. If there is no response from a passenger, await a response from 911.

7d. The elevator arrives at a floor and the doors opens at a floor that isn't floor B.

7d1. Stay inside the elevator and press the close door button or let the door close in 10 seconds.

Use case Diagram: