COMP3004 Assignment 1

Yuki Nakashima 101189690

Part I: The Therac-25: 30 years later

a. No, we cannot say that software is safe by itself or not. The safety of software is contextual, where the most common accidents involving software are results of flawed software requirements rather than implementation.
b. Safety in software development should come into play from the beginning. Safety requirements should be identified before the software is created.
c. It is safer to build from scratch than to reuse software. The reason being that, much like stated before, the safety in software does not lie in the software exclusively, but the context the software is used in. Therefore, a software can be safe one context and not in another, thus making reuse of software not safer.
d. Using object-oriented technology does not always lead to safe software. As specified in the article, while object-oriented design is appropriate for data-oriented systems, they are sub-optimal for control-oriented systems such as the Therac-25. Object-oriented designs can be more difficult to test for safety.
e. From the point of view of safety, it is better to first implement error-handling and then normal behaviour. This approach to development exercises the error-handling routines the most, thus faulty error-handling routines can be better identified.

Part II: Elevator Installation

PRIMARY USE CASE: Elevator Installation

Goal in Context: Install a fully functional elevator in a building to meet transportation and safety requirements.

Scope: Elevator Installation Process

Level: Summary

Stakeholders and Interests:

Technician: wants to install the rail brackets, rails, and struts

Installation Crew: wants to install the car slings

Steamfitter: wants to install the hydraulic system responsible for moving the cars

Certified Elevator Inspector: wants to inspect and test all parameters of installed elevator to check if it meets municipal standards

Programmer: wants to program the electronics responsible for controlling the elevator system

Electrician: wants to install, wire, and connect all the electrical components of the elevator system

Preconditions:

Structural work in the elevator shaft is complete.

Necessary permits are secured.

Guarantees:

The elevator is fully functional and certified for use.

Main Success Scenario:

1. Rail Bracket and Rail Installation
2. Hydraulic System Installation
3. Computerized Motion Control System Installation
4. Car Sling Installation
5. Door Installation
6. Cab Installation
7. Electrical Work Installation
8. Elevator Inspection

USE CASE 1: Rail Bracket and Rail Installation

Primary Actor: Technician

Goal in Context: Precisely install and align rail brackets and rails in which elevators will ride on.

Scope: Rail bracket and rail installation process

Level: Subfunction

Stakeholder and Interests:

Technician: wants to precisely install rail brackets and rails.

Installation Crew: wants to aid shaft technician in installation

Preconditions:

Structural work in the elevator shaft is complete.

Guarantees:

Have elevator rail brackets and rails be setup

Main Success Scenario:

1. Install spot brackets at the topmost part of the shaft
2. Drop plumb line in the elevator pit
3. Line lower brackets with spot brackets above
4. Level and align lower brackets and install
5. Repeat steps 1-4 until all brackets are installed
6. Lower 1 ton chain hoist
7. Lower guide rails using chain hoist and install to brackets

USE CASE 2: Hydraulic System Installation

Primary Actor: Steamfitter

Goal in Context: Provide power to raise and lower the elevator in hydraulic systems

Scope: Hydraulic system installation process

Level: Subfunction

Stakeholders and Interests:

Steamfitter: wants to install hydraulics responsible for elevator movement

Preconditions:

Rail bracket and guide rails are installed

Guarantees:

Hydraulic system is up and running to be connected to electricals

Main Success Scenario:

1. Install the hydraulic pistons in the shaft
2. Install pump unit in shaft
3. Connect the pump unit to the pistons using high-pressure hoses
4. Test for leaks and ensure proper pressure levels.

USE CASE 3: Computerized Motion Control System Installation

Primary Actor: Electrician

Goal in Context: Integrate the system that regulates elevator speed, position, and stopping. As well as install temporary safety bypass run box for construction

Scope: Computerized Motion Control System Installation

Level: Subfunction

Stakeholders and Interests

Electrician: install computerized motion control system including controllers and sensors to regulate speed, position, and control

Preconditions:

Rail brackets, guide rails, and hydraulic systems are installed and ready to deploy

Guarantee:

Have a moving pistons with a safety bypass run box

Main Success Scenario:

1. Mount monitoring sensors to hydraulic pistons
2. Mount selector to hydraulic pistons
3. Install the main box containing computerized motion control panel in designated room
4. Wire the control system to the hydraulic pump, sensors, selectors, and electrical systems
5. Run a safety bypass run box to computerized motion control panel

USE CASE 4: Car Sling Installation

Primary Actors: Installation Crew

Goal in Context: Have a moving platform for cab to later be constructed on

Scope: Car Sling installation process

Level: Subfunction

Stakeholders and Interests:

Technician: wants to assure the installation and strength of platform and crossheads.

Installation Crew: wants to install a platform for basic elevator template.

Precondition:

Have rail brackets, guide rails, hydraulic system, and portion of electrical system complete

Guarantee:

Have a moving platform for the cab to sit on with corresponding crossheads and bolster channels for strength of rails.

Main Success Scenario:

1. Install sling platform onto pistons
2. Install styles inside elevator shaft
3. Install crossheads to elevator rails
4. Install bolster channels inside elevator shaft
5. Ensure platform is moving accordingly

USE CASE 5: Door Installation

Primary Actor: Installation Crew

Goal in Context: Have floor doors in place to prevent public access to elevator shaft

Scope: Door Installation process

Level: Subfunction

Stakeholders and Interests

Installation Crew: wants to install struts and doors for each floor

Preconditions:

Rail brackets, guide rails, hydraulic systems, and a moving platform are installed

Guarantee:

Have doors for each landing floor

Main Success Scenario:

1. Take precise measurements for struts
2. Drill holes for brackets to hold struts down elevator shaft
3. Install strut to brackets
4. Install hoistway sill in each level

5. Install header at each floor entrance
6. Install door box at each floor entrance
7. Install landing door at each floor entrance
8. Ensure that door aligns with hoistway sills and struts precisely

USE CASE 6: Cab Installation

Primary Actor: Installation Crew

Goal in Context: Have solid cabs on platforms

Scope: Cab Installation process

Level: Subfunction

Stakeholders and Interests

Installation Crew: wants to install cabs for each moving paltform

Preconditions:

Rail brackets, guide rails, hydraulic systems, moving platforms, and door boxes at each floor are installed

Guarantee:

Have fully built cab on moving platform

Main Success Scenario:

1. Loosely join the side and rear interior walls on top of the platform
2. Unpack dome and ceiling units
3. Install ceiling units
4. Install strike column
5. Install return column
6. Install the front panels of the car
   6.1. Install car operating station
7. Install the dome
8. Install door control and motor drive unit on top of dome
9. Tighten and check all measurements and supports
10. Install cab door
11. Install door clutch assembly
12. Install sensors that detect obstruction

USE CASE 7: Electrical Work Installation

Primary Actor: Electrician

Goal in Context: Establish a safe and functional electrical system for the elevator.

Scope: Electrical work Installation process

Level: Subfunction

Stakeholders and Interests

Electrician: wants to connect all electronics now inside cab with rest of the electrical system

Preconditions:

Rail brackets, guide rails, hydraulic systems, door boxes, and complete cabs are installed

Guarantee:

Have fully built functioning cab

Main Success Scenario:

1. Wire electricals for lights and ventilation fan above cab
2. Organize and install high voltage wiring
   2.1. Connect hydraulic pump and pistons with computerized motion control system
3. Organize and install low voltage wiring
   3.1. Connect sensors and devices to computerized motion control system
4. Inspect all elements in the elevator shaft using the inspection station on top of the cab
5. Check elevator speeds and adjust hydraulic pump accordingly
6. Complete field wiring including connecting every button and switch on end point systems such floor buttons
7. Program computer with various command and control protocols
8. Turn on full autonomy of elevator system
9. Test every function of elevator system
   9.1. Door safety sensors verification

USE CASE 9: Elevator Inspection

Primary Actor: Certified Elevator Inspector

Goal in Context: Establish a safe and functional elevator compliant of municipal standards

Scope: Elevator inspection process

Level: Subfunction

Stakeholders and Interests

Certified Elevator Inspector: wants to assure newly built elevator system is compliant with municipal standards

Preconditions:

A fully functioning elevator is installed

Minimal Guarantee:

A functioning but unsafe elevator is caught and remediated

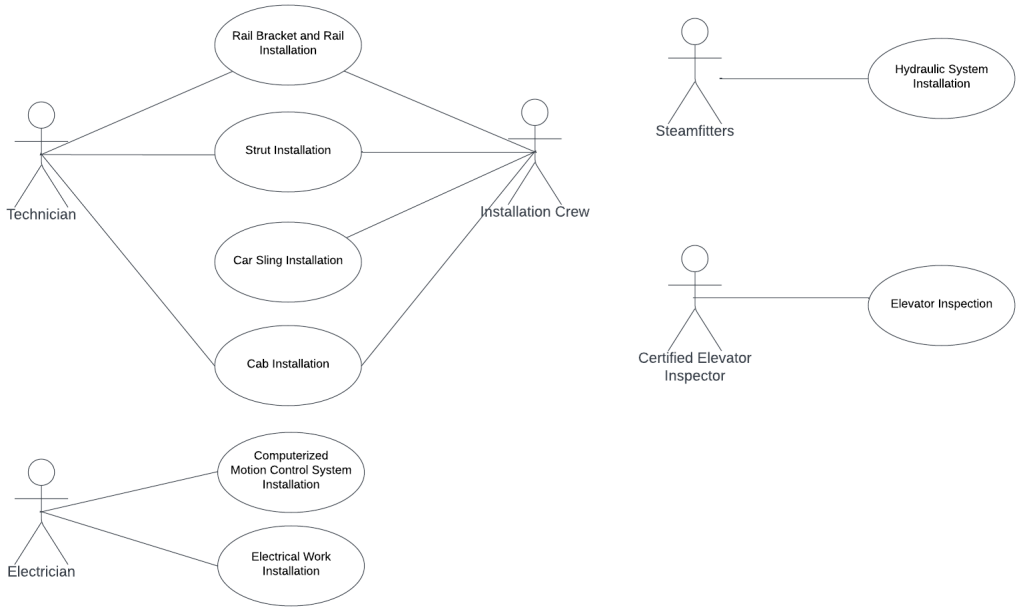
Success Guarantee:

A fully functioning safe elevator is assured

Main Success Scenario:

1. Conduct 150-point test
2. Test every single electronic device
3. Test every single safety device
4. Test every scenario the elevator will face
5. Conduct full load weight test
6. Ensure compliance with building codes and regulations

USE CASE DIAGRAM: Elevator Installation



Part III: Elevator Control System

USE CASE 1: Elevator delivering rider to a floor

Primary Actor: Rider

Goal in Context: Rider at floor N presses the up or down button requesting for an elevator, rides the elevator to the inputted floor, and arrives at floor N'.

Scope: Elevator Control System ("ECS")

Level: Summary

Stakeholders and Interests:

Rider: wants to go to a specific floor.

Building Safety Service: wants to alarmed and connected to elevator when help button is pressed.

Precondition: Rider requests an elevator at a floor.

Guarantees: Rider arrives at requested floor.

Trigger: Rider decides to go to a different floor than they are on.

Main success scenario:

1. Rider presses up/down button on floor
   1.1. Up/down button illuminates
2. ECS gets an elevator that can arrive at the Rider's floor the quickest
3. The elevator arrives at Rider's floor
   3.1. Elevator rings a bell
   3.2. Up/down button darkens.
   3.3. Elevator opens its doors and floor doors for 10 seconds
4. Rider enters the elevator
5. Rider selects a floor to go to
   5.1. Press button corresponding to another floor
6. Elevator proceeds to another floor
   6.1. Elevator rings a bell
   6.2. Elevator closes its doors and floor doors
   6.3. Elevator starts to move
   6.4. Elevator sensor is notified that it has arrived or passed a floor
   6.5. Elevator displays the (changing) current floor of elevator
7. Elevator arrives at requested floor
   7.1. Elevator displays current floor of elevator
   7.2. Elevator rings a bell
   7.3. Elevator opens its and floor doors for 10 seconds
8. Rider gets off the elevator
9. Ride arrives at destination floor

Extensions:

1a. ECS is down: up/down button does not illuminate to signify malfunction.

1b. All elevators unavailable: up/down button does not illuminate to signify malfunction.

2a. ECS cannot find an available elevator: up/down button darkens.

3a. An elevator that is going the opposite direction to rider requested direction arrives: Elevator rings bell and opens its and floors door to release riders, however up/down buttons on floor do not darken.

(3.3, 7.3)b. Floor door opens but elevator door is stuck and does not open: Floor door closes, elevator ceases all movement, and building safety service is connected through voice connection for investigation.

(3.3, 7.3)c. Elevator door opens but floor door is stuck and does not open: Elevator door closes, building safety service is connected through voice connection for investigation, and elevator proceeds to next suggested floor.

(3.3, 7.3)d. Elevator and floor door does not open: Elevator ceases all movement and building safety service is connected through voice connection.

4a. “Close door” button is pressed whilst rider is entering elevator light sensor is interrupted by entering rider, the “close door" button is overridden and the door does not close.

4b. Elevator detects overload: elevator does not move and an audio and text messages are presented to passengers asking for the load to be reduced before attempting to move.

5a. Rider presses “open door" button: elevator and floor doors are held open past the default timing until the button is released.

5b. Rider presses “close door” button: elevator and floor doors close prematurely.

5c. Rider does not select floor button, and no other rider is present: elevator does not move until a floor is selected or elevator is chosen by ECS to respond to another rider request on another floor.

5d. Rider does not select floor button, and other riders present with few floors already selected: elevator proceeds to next requested closest floor.

6a. Elevator doors are obstructed by an obstacle and the light sensor detects it: ECS stops the door from closing and opens it. If done repeatedly over a short period of time, a warning is sounded over the audio system and a text message is displayed.

6b. Floor door closes but elevator door is stuck and does not close: elevator ceases all movement, and building safety service is connected through voice connection for investigation.

6c. Elevator door closes but floor door is stuck and does not close: Elevator does not move and opens door to not give access to elevator hoistway. Building safety service is connected through voice connection for investigation.

6d. Elevator and floor door do not close: Elevator does not move and building safety service is connected through voice connection for investigation.

6e. Rider presses Help button: rider is connected to building safety service through a voice connection. If there is not response from building safety service within 5 seconds or if there is no response from a passenger a 911 emergency call is placed.

*a: “Help” button is pressed by another passenger: passenger is connected to building safety service through a voice connection. If there is not response from building safety service within 5 seconds or if there is no response from a passenger a 911 emergency call is placed.

*b. Fire button is pressed: elevator moves to a safe floor. 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.

*c. ECS receives a “Fire alarm”: ECS commands all elevators to move to a safe floor. 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.

*d. ECS receives “Power Out” alarm signal: ECS relays an audio and text messages to passengers informing them of the power outage. Each elevator is moved to a safe floor and passengers are asked to disembark via audio and text messages.

USE CASE 1 DIAGRAM: Deliver Rider to a Suggested Floor