**Assignment 1**

**Part 1: The Therac-25: 30 Years Later**

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

No, software is not inherently safe or unsafe. Safety depends more heavily on the context in which the software is used.

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

At the earliest possible phase. Ideally, before the actual software development starts. This way, the code itself is developed with safety in mind and not simply “accounted for”.

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

Generally, it is safer to rebuild from scratch although it heavily depends on the context. It is wrong to assume that just because one iteration of the software was safe, that it can be reused in another context and be just as safe. While rebuilding software for every context is not realistic, a balance must be struck and it must always be adapted to fit new use cases.

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

In some situations; the article mentions that it could be more suitable for data-oriented systems, but maybe not for control-oriented systems.

1. *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?*

Most errors occur in the error-handling behavior of the program, so designing them first ensures they get the proper amount of emphasis and care.

**Part 2: Elevator installation use-case modelling**

**Primary Actor:** Elevator Construction Team (“ECT”)

Scope: Elevator Installation Process

Level: User goal

Stakeholders and Interests:

* Elevator Construction Team: wants to be successful and efficient in installing the elevator
* Elevator Manufacturer: wants their elevator to be installed safely and properly
* Building Owner(s): wants the elevator to be functional for accessibility

**Precondition:**

* All required materials (brackets, tools, etc.) are available to the construction team
* All materials bought from the manufacturer are free of defects

Minimal guarantee:

* The elevator components are assembled using the proper safety regulations

**Success guarantee:**

* The elevator is installed, function, and meets all safety and operational standards

**Main Success Scenario:**

1. ECT installs the rail brackets as straight and accurately as possible
2. ECT attaches the guide rails are attached using a one ton chain hoist
3. ECT installs the car sling and ensures proper alignment
4. ECT installs and calibrates entrances on each floor using magnetic tape
5. ECT installs the support struts for the elevator
6. ECT installs the door box mechanism
7. ECT installs the landing doors on each floor
8. ECT assembles the elevator cab, ensuring its safety and structural integrity
9. ECT performs electrical wiring to power and connect the elevator to its components
10. ECT performs a comprehensive inspection of the installed elevator, components, and systems to ensure it meets safety regulations.

**Extensions:**

1a. Rail brackets are not properly aligned during installation

1a1. ECT stops the installation, adjusts the rail brackets to ensure accurate alignment

2a. Guide rails are not securely attached

2a1. ECT stops the process, re-attaches the guide rails securely

4a. Magnetic tape calibration is inaccurate, causing misalignment of entrances

4a1. ECT rechecks and recalibrates the entrances, moving the magnetic tape as required

9a. Electrical connections are faulty or not properly connected

9a1. ECT troubleshoots the issues and rectifies the electrical connections

10a. Inspection reveals non-compliance with safety regulations

10a1. Non-compliance issue is revealed to the team and rectified accordingly

A diagram of a system

Description automatically generated

**Part 3: Elevator Control System**

**Primary Actor:** Elevator User

Scope: Elevator Usage Process

Level: User goal

Stakeholders and Interests:

* Elevator User: wants safe and reliable use of the elevator
* Building Staff: wants to assist the elevator user to have an overall good experience with building facilities

**Precondition:**

* The elevator is installed correctly and operational
* Power to the building is supplied
* The elevator is not currently under maintenance

Minimal guarantee:

* The elevator responds to user commands such as selecting floors and opening/closing doors when powered and not under maintenance

**Success guarantee:**

* Users can enter the elevator, select desired floors, and exit the elevator safely and efficiently

**Main Success Scenario:**

1. User enters the elevator lobby and waits for the elevator
2. User enters the selected elevator and selects the desired floor using the control panel
3. Elevator doors close, and the elevator moves to the selected floor
4. Elevator doors open at the selected floor, and the user exits

**Extensions:**

1a. Elevator cabin exceeds maximum capacity

1a1. Users exit the elevator and wait for the next available cabin.

1b. Users with mobility challenges experience difficulty

1b1. Users press the 'assistance' button or use the intercom to request assistance.

1b2. Building staff provides necessary assistance to the user.

2a. Power outage occurs while in the elevator

2a1. Emergency lights and communications systems activate.

2a2. Users are informed of the situation and advised to stay calm and wait for assistance.

2b. Elevator stops moving during transit

2b1. Users press the emergency button or call for help using the intercom.

2b2. Users are informed about the situation and advised to wait for assistance.

2c. Control panel/buttons do not respond

2c1. Users try pressing the button again.

2c2. If unsuccessful, users use the emergency communications system.

2d. Mechanical failure occurs (e.g. door jam)

2d1. Users press the emergency button or call for help using the intercom.

2d2. Users are informed about the situation and advised to wait for assistance.

A diagram of an elevator

Description automatically generated