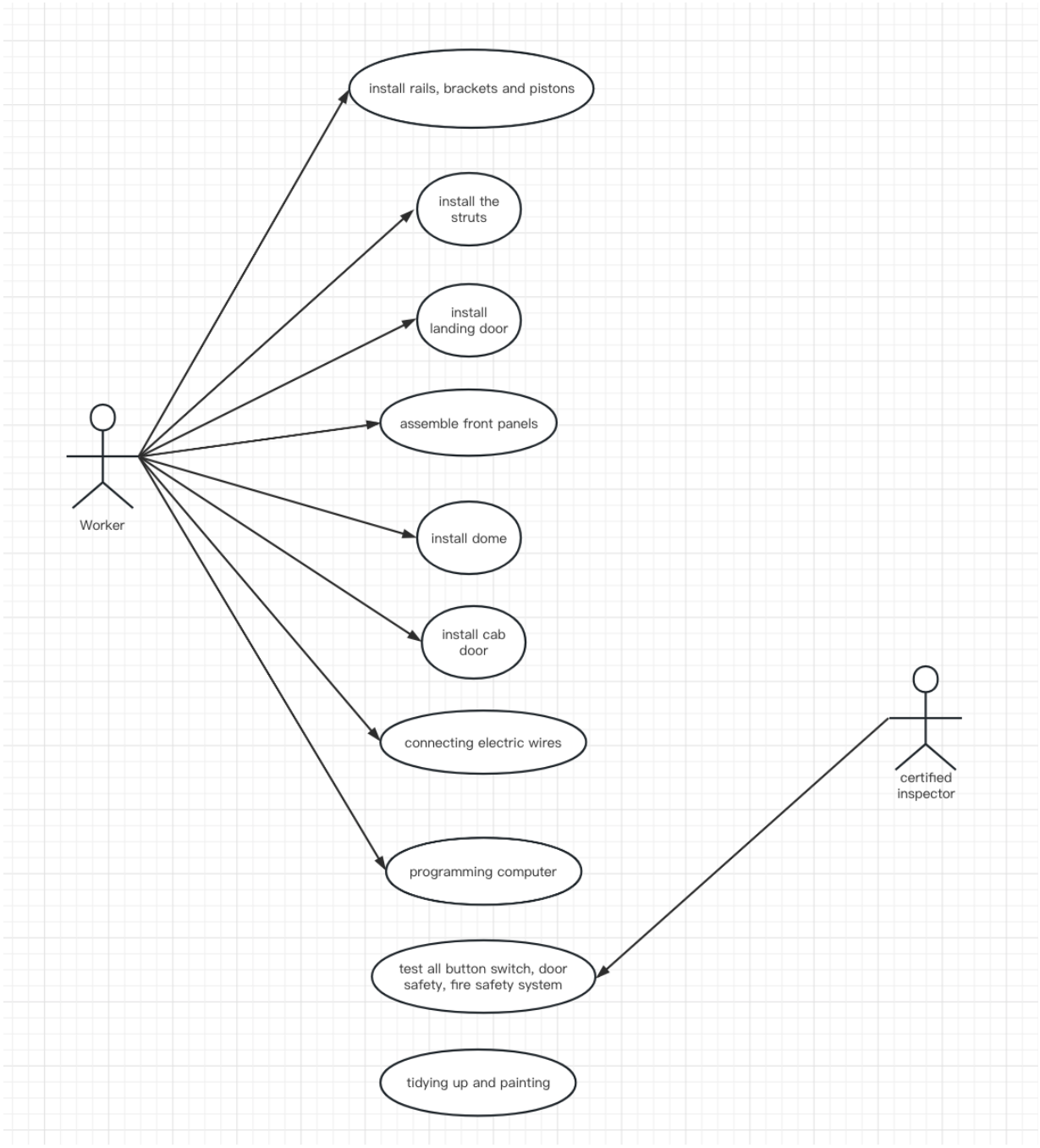
Part 1: The Therac-25: 30 Years Later (5 marks)

1. Can we say that software by itself is safe or not?
   No, software safety always depends on the context in which the software is used.
2. At what phase of software development does safety first come into play?
   At the beginning, safety can't be ensured if it isn't already there, it has to be built in from the beginning.
3. Is it safer to reuse software or build from scratch?
   No, software is only safe or unsafe within a specific context, reusing software that was safe in one system doesn't mean it will be safe when used in a different system.
4. Does using object-oriented technology lead to safer software?
   No, object-oriented design is appropriate for a data-oriented system, it leads to more difficult to test for safety, trace from requirements to code, maintain without affecting safety and assure the correctness of changes to safety-critical requirements.
5. 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?
   First error-handling and then normal behavior is better, so that error-handling routines will get the most exercise.

Part 2: Elevator installation use-case modeling (15 marks)

Name: Elevator Installation
Actors: Worker
Scenario: Installation
1、Install rail brackets
   a) Install the top first.
   b) Drop a plumb line to the elevator pit in order to accurately line the lower brackets.
2、Install rails
   a) Pre-condition: rail brackets are perfectly aligned
3、install pistons
4、Install the struts.

5、Install the landing door.
6、Install the strike column and return column.
7、Assemble front panels.
8、Install dome
9、Install cab door
10、 Connecting electric wires
11、Programming the computer with various command and control protocols
10、Test button switch, door safety sensor, fire safety system
11、Tidying up and painting


install rails, brackets and pistons
install the struts
install landing door
assemble front panels
install dome
install cab door
connecting electric wires
programming computer
test all button switch, door safety, fire safety system
tidying up and painting
Worker
certified inspector

Part 3: Elevator Control System (20 marks)

Name: Elevator Control System
Actors: Passenger
Main Success Scenario:
1.Passengers select any M elevator at any N floor.
2.Passenger presses the "Up" or "Down" button.
3.The elevator control system lights the selected button.
4.The elevator control system controls the elevator to reach the N floor, and when the bell rings, "Up" or "Down" button lights go out.
5.The elevator control system controls the elevator to open the door for ten seconds to let people leave or ride. Ring the bell and close the door.
6.Passengers choose their own destination floor (one or more) in the elevator.
7.The elevator control system controls the elevator to start moving. Stop at the target
floor and open the door (10 seconds). Passengers leave and arrive at the destination floor.

Extensions:
Notify passengers when they arrive at the floor.
1. The sensor senses and notifies.

The passenger in the elevator wants to keep the elevator door open.
1. Passengers use the "open door" button in the elevator.
2. The door will remain open beyond its default period.

The passenger in the elevator wants to close the elevator door faster.
1.Passengers use the "close door" button in the elevator.
2. The doors can be closed prematurely.

Door obstacles: the light sensor is interrupted when the door is closing.
1. the control system stops the door from closing and opens it
2. this occurs repeatedly over a short period of time
3. a warning is sounded over the audio system and a text message is displayed.

Passengers in the elevator check the current floor.
1. The elevator has a display which shows passengers the current floor of the elevator.

Overload
1.The elevator control system receives the "overload" alarm signal from the elevator.
2.The elevator does not move and an audio and a text message are presented to passengers asking for the load to be reduced before attempting to move again.

Passenger pressed the “help” button in the elevator.
1. The control system receives a “Help” alarm signal from an elevator.
2.The passenger is connected to building safety service through a voice connection.
3.If there is no response from building safety within 5 seconds or if there is no response from a passenger, a 911 emergency call is placed.

Fire
1. The control system receives a “Fire” alarm signal from the building or a “Fire” alarm signal from the elevator itself.
2. Control all elevators to move to a safe floor.
3. In both cases 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.

Power Out
1. The control system receives a “Power Out” alarm signal.
2.Use battery backup power.
3. an audio and a text message are presented to passengers informing them of the power outage.
4. Each elevator is then moved to a safe floor and passengers are asked to disembark via audio and text messages.