Elevator System Specification

This document describes a basic elevator system. For simplicity we assume that there is one door (rather than two (one attached to the floor and one to the cab) which close on top of each other), no weight sensors, no emergency bells, and no buttons except those to summon the lift to a particular floor, and those for requesting a floor from inside the cab.

The elevator system has the following **sensors**:

- door is open/close
- elevator is stationary/moving
- elevator is at a particular floor
- elevator is in between floors

The elevator system has the following **control signals**:

- open/close door
- go up/down
- stop

The elevator system has the following **buttons**:

- elevator summoning (one at each floor)
- elevator floor request (one button per floor in each elevator)

Following the short description of the elevator system above, what follows gives a list of properties which the elevator system has to satisfy during normal operation. These are classified under invariants, temporal properties and real-time properties:

Invariants

- elevator never moves up/down when the door is not closed
- elevator never attempts to go above the topmost floor/below the lowermost floor
- elevator never moves unless a button press occurs which has not yet been serviced
- elevator never stops in between floors
- elevator doors are only opened once the elevator reaches a floor

Temporal Properties

- when a button (summon or floor request) is pressed, the elevator eventually services the request (Model checking only)
- multiple presses of the same button in between servicing are considered as a single request
- if an elevator is moving through a floor for which a summons button has been pressed, the elevator should service that floor. Otherwise, the elevator closest to the requested floor should service it.
- door opening/closing signals always alternate each other; there should never be two consecutive door opening/two consecutive door closing.
- if the summon button is pressed for a floor where the door is closing, the door should open again

- if the summon button is held down on a floor where the door is not closed, then the door should open and remain open

Real-Time Properties

- upon a request, after the door closes, the elevator starts moving in less than 3 seconds
- after the door has been open for 3 seconds, it closes automatically