Justin Mang 556002335 – Elevator - Assignment 3 - CMPT 477 Summer 2018

Assumptions About the Environment:

1. Calls to the elevator from floors (i.e., floor button) are eventually serviced.

2. Calls from within the elevator (elev. button) are eventually serviced.

3. The elevator never moves with its doors open.

4. The elevator doors remain open until there is a request to use it.

5. It takes exactly 2 time units for the elevator to move between two consecutive

floors.

6. If there are no requests for another floor, the elevator should not move.

7. The elevator cannot change direction between floors. Additionally, create

8. The elevator will eventually service requests to all floors (FAIRNESS).

9. The elevator works on a 2 time unit system, meaning that calls cannot be interpreted during its "in-between" state, 0.

10. Elevator can only service floors 1,2, and 3. Floor 0 represents an "in-between" state and cannot be serviced.

Modelling Decisions:

-- The elevator never moves with its doors open

SPEC

AG (!(m=1 & d=TRUE) & !(m=2 & d=TRUE))

-- The elevator doors remain open until there is a request to use it

SPEC

AG A[d=TRUE U (fc=1 | fc=2 | fc=3 | ec=1 | ec=2 | ec=3)]

-- It takes exactly 2 time units for the elevator to move between two consecutive floors

-- transition between floors: if floor moving up/down then inbetween and time interval state followed by next floor and reset on time interval

SPEC

AG (((f=1)&(m=1)) -> AX ((t=1&f=0&m=1) -> AX(t=0&f=2&m=0)))

SPEC

AG (((f=2)&(m=1)) -> AX ((t=2&f=0&m=1) -> AX(t=0&f=3&m=0)))

SPEC

AG (((f=2)&(m=2)) -> AX ((t=1&f=0&m=2) -> AX(t=0&f=1&m=0)))

SPEC

AG (((f=3)&(m=2)) -> AX ((t=2&f=0&m=2) -> AX(t=0&f=2&m=0)))

-- If there are no requests for another floor, the elevator should not move.

SPEC

AG (((fc=0) & (ec=0)) -> m=0)

-- The elevator cannot change directions between floors.

SPEC

AG ((((!(t=0)&(m=1)) -> AX!(m=2)) | ((!(t=0)&(m=2)) -> AX!(m=1)))

-- Calls to the elevator from floors are eventually serviced

SPEC

AG ((fc=1) -> AF (f=1))

SPEC

AG ((fc=2) -> AF (f=2))

SPEC

AG ((fc=3) -> AF (f=3))

-- Calls to the elevator from within the elevator are eventually serviced

SPEC

AG ((ec=1) -> AF (f = 1))

SPEC

AG ((ec=2) -> AF (f = 2))

SPEC

AG ((ec=3) -> AF (f = 3))

Additional Properties:

-- Additional: The elevator cannot go below 1

SPEC

AG ((f=1) -> AX!(m=2))

-- Additional: The elevator cannot go above 3

SPEC

AG ((f=3) -> AX!(m=1))

Verification Time for Properties:

< 0.5 seconds