

An Event-B Specification of Elevator

A machine for testing the basics of code generation. It can move an elevator up and down between limits specified by constants.

1	CONTEXT	HouseContext	2
1.1	DIR		2
1.2	down	max_floor up	2
2	MACHINE	Elevator	3
2.1	curr	dest dir	3
2.2	moveUp		3
2.3	moveDown		3
2.4	enterDest	(d)	3
2.5	startMovingUp		4
2.6	startMovingDown		4

CONTEXT **HouseContext**

1

SETS

1.1

DIR The direction of travel

CONSTANTS

1.2

up Moving up

down Moving down

max_floor The house has no more than these number of floors.

AXIOMS

axm_01: partition(**DIR**, {**up**}, {**down**})

axm_02: **max_floor** $\in \mathbb{N}$ The maximum floor is a number.

axm_03: **max_floor** = **10**

END

SEES HouseContext

VARIABLES

2.1

curr Current floor
dest Destination floor, stop when *curr* == *dest*
dir Direction of movement

INVARIANTS

inv_1: *curr* ∈ ℕ
inv_2: *curr* > 0
inv_3: *curr* ≤ *max_floor*
inv_4: *dest* ∈ ℕ
inv_5: *dest* > 0
inv_6: *dest* ≤ *max_floor*
inv_7: *dir* ∈ DIR

EVENT INITIALISATION

THEN

init_1: *curr* := 1
init_2: *dest* := 1
init_3: *dir* := up

END

EVENT moveUp

2.2

WHERE

grd_1: *dir* = up
grd_2: *curr* < *max_floor*
grd_3: *curr* ≠ *dest*

THEN

act_01: *curr* := *curr* + 1

END

EVENT moveDown

2.3

WHERE

grd_1: *dir* = down
grd_2: *curr* > 1
grd_3: *curr* ≠ *dest*

THEN

act_01: *curr* := *curr* - 1

END

EVENT enterDest

2.4

ANY

d

WHERE

grd_1: *d* ∈ ℕ
grd_2: *d* > 0
grd_3: *d* ≤ *max_floor*

THEN

act_1: $dest := d$

END

EVENT startMovingUp

2.5

WHERE

grd_1: $dest > curr$

gtd_2: $dir = down$

THEN

act_1: $dir := up$

END

EVENT startMovingDown

2.6

WHERE

grd_1: $dest < curr$

gtd_2: $dir = up$

THEN

act_1: $dir := down$

END

curr, 3

dest, 3

dir, 3

Elevator, 3

enterDest, 3

HouseContext, 2, 3

INITIALISATION, 3

moveDown, 3

moveUp, 3

startMovingDown, 4

startMovingUp, 4