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.

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: $curr \in \mathbb{N}$
  inv_2: $curr > 0$
  inv_3: $curr \leq max\_floor$
  inv_4: $dest \in \mathbb{N}$
  inv_5: $dest > 0$
  inv_6: $dest \leq max\_floor$
  inv_7: $dir \in DIR$

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: $curr \neq dest$

THEN

  act_01: $curr := curr + 1$

END

EVENT moveDown   2.3
WHERE

  grd_1: $dir = down$
  grd_2: $curr > 1$
  grd_3: $curr \neq dest$

THEN

  act_01: $curr := curr - 1$

END

EVENT enterDest   2.4
ANY

  d

WHERE

  grd_1: $d \in \mathbb{N}$
  grd_2: $d > 0$
  grd_3: $d \leq max\_floor$

```
THEN
  act_1:    dest := d
END
```

```
EVENT  startMovingUp
WHERE
  grd_1:    dest > curr
  gtd_2:    dir = down
THEN
  act_1:    dir := up
END
```

```
EVENT  startMovingDown
WHERE
  grd_1:    dest < curr
  gtd_2:    dir = up
THEN
  act_1:    dir := down
END
```