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.

| | NTEXT HouseContext |
|-----|-------------------------------|
| | DIR |
| 1.5 | down max_floor up |
| | CHINE Elevator |
| | curr dest dir |
| 2.5 | moveUp |
| | moveDown |
| 2.4 | $\operatorname{enterDest}(d)$ |
| 2.5 | startMovingUp |
| 2.6 | startMovingDown |

1 CONTEXT HouseContext SETS 1.1 DIR The direction of travel 1.2 CONSTANTS Moving up up down Moving down max_floor The house has no more than these number of floors. AXIOMS $\begin{array}{ll} \verb"axm_01: & \verb"partition(DIR, \{up\}, \{down\}) \\ \verb"axm_02: & \verb"max_floor \in \mathbb{N} & The maximum floor is a number. \end{array}$ $\max_{\text{floor}} = 10$ axm_03:

END

```
MACHINE Elevator 15 a 2
```

SEES HouseContext

```
2.1
VARIABLES
 curr Current floor
 dest Destination floor, stop when curr == dest
        Direction of movement
INVARIANTS
 inv_1:
          curr \in \mathbb{N}
 inv_2: curr > 0
 inv_3: curr \leq \max_{\text{floor}}
 inv_4: dest \in \mathbb{N}
 inv_5: dest > 0
 inv_6: dest \leq \max_{s} 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_{\text{floor}}
          curr \neq dest
 grd_3:
THEN
 act_01: curr := curr + 1
END
EVENT moveDown
                                                                                                  2.3
WHERE
 grd_1:
          dir = down
 grd_2:
          curr > 1
          curr \neq dest
 grd_3:
THEN
 act 01: curr := curr - 1
END
                                                                                                  2.4
EVENT enterDest
ANY
 d
WHERE
 \operatorname{grd}_1: d \in \mathbb{N}
 grd_2: d>0
```

```
grd_3: d \le \max_{l} 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
                                                                                            2.6
{\tt EVENT} \  \, {\tt startMovingDown}
WHERE
 grd_1:
          dest < curr
          dir = up
 gtd_2:
THEN
 act_1: dir := down
END
```

curr, 3

dest, 3

dir, 3

Elevator, 3 enterDest, 3

HouseContext, 2, 3

INITIALISATION, 3

 $\begin{array}{c} \text{moveDown, 3} \\ \text{moveUp, 3} \end{array}$

 $\begin{array}{c} {\rm startMovingDown}, \ 4 \\ {\rm startMovingUp}, \ 4 \end{array}$