Specification of an Elevator in Z

Safety-Critical Systems 3, WiSe'07/08

Jan Peleska (jp@tzi.de)
Christof Efkemann (chref@tzi.de)

2nd version, Oct 23, 2007

Safety Requirements

Declaration of Constants

The number of the ground floor and of the highest floor, and the maximum weight of the elevator together with its passengers:

$$
\begin{array}{|l}
topFloor : \mathbb{N} \\
groundFloor : \mathbb{N} \\
maxWeight : \mathbb{N} \\
\hline
groundFloor < topFloor
\end{array}
$$

Declaration of Types

The set of all admissible floor numbers:

$$FLOORS == groundFloor \,..\, topFloor$$

Possible states of a door:

$$DOOR ::= open \mid closed$$

Possible motion states for the elevator:

$$DIRECTION ::= up \mid down \mid stopped$$

Specification of the State Space

The elevator state space, as far as it is safety-relevant:

ElevatorState

$$
\begin{aligned}
&weight : \mathbb{N} \\
&move : DIRECTION \\
&door : DOOR \\
&thisFloor : FLOORS \\
\hline
&weight \leq maxWeight \\
&thisFloor = topFloor \Rightarrow move \in \{stopped, down\} \\
&thisFloor = groundFloor \Rightarrow move \in \{stopped, up\} \\
&door \neq closed \Rightarrow move = stopped
\end{aligned}
$$

Specification of the Operations

MoveUp

$$
\begin{aligned}
&\Delta ElevatorState \\
\hline
&move = up \\
&thisFloor' = thisFloor + 1
\end{aligned}
$$

MoveDown

$$
\begin{aligned}
&\Delta ElevatorState \\
\hline
&move = down \\
&thisFloor' = thisFloor - 1
\end{aligned}
$$

StableState

$$
\begin{aligned}
&\Delta ElevatorState \\
\hline
&move = stopped \\
&thisFloor' = thisFloor
\end{aligned}
$$

User Requirements

Specification of the State Space

UserState

$$
\begin{array}{l}
ElevatorState \\
upQ : \operatorname{seq} FLOORS \\
downQ : \operatorname{seq} FLOORS \\
\hline
\forall\, i : 1 \mathinner{..} (\#upQ - 1) \bullet upQ(i) < upQ(i+1) \\
\forall\, i : 1 \mathinner{..} (\#downQ - 1) \bullet downQ(i) > downQ(i+1) \\
\#upQ \geq 1 \Rightarrow thisFloor < head(upQ) \\
\#downQ \geq 1 \Rightarrow thisFloor > head(downQ)
\end{array}
$$

Specification of the Operations

. . . to be continued . . .