

```

1 MACHINE
2   Autobrake
3   REFINES
4     Generic
5   SEES
6     AutobrakeCtx
7   VARIABLES  $t, x_s, v, x$ 
8   INVARIANTS
9      $inv1: v \in RReal \leftrightarrow RReal$ 
10     $inv2: Closed2Closed(Rzero, t) \subseteq dom(v)$ 
11     $inv3: x \in RReal \leftrightarrow RReal$ 
12     $inv4: Closed2Closed(Rzero, t) \subseteq dom(x)$ 
13     $inv5: x_p = bind(v, x)$ 
14     $inv6: boundedBy(Closed2Closed(Rzero, t), v, Rzero, Vmax)$ 
15     $inv7: \forall t \cdot t \in Closed2Closed(Rzero, t) \wedge x(t) \mapsto SP \in geq \Rightarrow x_s = stopped$ 
16  EVENTS
17  INITIALISATION
18  WITH
19     $x_{p'}: x_{p'} = bind(v', x')$ 
20  THEN
21     $act1: t := Rzero$ 
22     $act2: v, x :| v' = \{Rzero \mapsto v0\} \wedge x' = \{Rzero \mapsto x0\}$ 
23     $act4: x_s := stabilizing$ 
24  END
25
26  Behave
27  REFINES Behave
28  ANY  $tp, e$ 
29  WHERE
30     $grd0: tp \in RRealPlus \wedge t \mapsto tp \in lt$ 
31     $grd1: e \in DE(S)$ 
32     $grd2: Solvable(Closed2Closed(t, tp), e)$ 
33  WITH
34     $x_{p'}: x_{p'} = bind(v', x')$ 
35     $Inv: Inv = S$ 
36  THEN
37     $act1:$ 
38       $t, x, v :|$ 
39         $t' = tp \wedge$ 
40         $x' \in RRealPlus \rightarrow RReal \wedge v' \in RRealPlus \rightarrow RReal \wedge$ 
41         $CBAPSolutionOf(t, t', bind(v, x), bind(v', x'), e, S)$ 
42  END
43
44  ctrl_transition_accelerate
45  REFINES Transition
46  WHERE
47     $grd1: plus(x(t) \mapsto divide(times(v(t) \mapsto v(t)) \mapsto times(Rtwo \mapsto b))) \mapsto SP \in lt$ 
48  WITH
49     $s: s = \{accelerating\}$ 
50  THEN
51     $act1: x_s := accelerating$ 
52  END
53
54  ctrl_transition_stabilize
55  REFINES Transition
56  WHERE
57     $grd1: plus(x(t) \mapsto divide(times(v(t) \mapsto v(t)) \mapsto times(Rtwo \mapsto b))) \mapsto SP \in lt$ 
58  WITH
59     $s: s = \{stabilizing\}$ 
60  THEN
61     $act1: x_s := stabilizing$ 
62  END
63
64  ctrl_transition_brake
65  REFINES Transition
66  WHERE
67     $grd1: plus(x(t) \mapsto divide(times(v(t) \mapsto v(t)) \mapsto times(Rtwo \mapsto b))) \mapsto SP \in lt$ 
68  WITH
69     $s: s = \{braking\}$ 
70  THEN
71     $act1: x_s := braking$ 
72  END
73

```

```

74 ctrl_sense_near_stop
75 REFINES Sense
76 WHERE
77   grd1:  $plus(x(t) \mapsto divide(times(v(t) \mapsto v(t)) \mapsto times(Rtwo \mapsto b))) \mapsto SP \in geq$ 
78   grd2:  $v(t) \mapsto Rzero \in gt$ 
79 WITH
80   s:  $s = \{nearing\_stop\}$ 
81   p:  $p = STATES \times RReal \times \{v\_ \mapsto x\_ \mid plus(x\_ \mapsto divide(times(v\_ \mapsto v\_)) \mapsto times(Rtwo \mapsto b))) \mapsto SP \in geq \wedge v\_ \mapsto Rzero \in gt\}$ 
82 THEN
83   act1:  $x\_s := nearing\_stop$ 
84 END
85
86 ctrl_sense_stopping
87 REFINES Sense
88 WHERE
89   grd1:  $v(t) = Rzero$ 
90 WITH
91   s:  $s = \{stabilizing, stopped\}$ 
92   p:  $p = STATES \times RReal \times \{v\_ \mapsto x\_ \mid v\_ = Rzero \wedge x\_ \in RReal\}$ 
93 THEN
94   act1:
95      $x\_s :|$ 
96      $(x\_s = nearing\_stop \Rightarrow x\_s' = stopped) \wedge$ 
97      $(x\_s \neq nearing\_stop \Rightarrow x\_s' = stabilizing)$ 
98 END
99
100 ctrl_actuate_brake
101 REFINES Actuate
102 ANY tp
103 WHERE
104   grd0:  $tp \in RRealPlus \wedge t \mapsto tp \in lt$ 
105   grd1:  $x\_s \in \{braking, nearing\_stop\}$ 
106 WITH
107   e:  $e = ode(f\_deceleration(t \mapsto v(t)), v(t) \mapsto x(t), t)$ 
108   s:  $s = \{braking, nearing\_stop\}$ 
109    $x\_p'$ :  $x\_p' = bind(v', x')$ 
110   Inv:  $Inv = \{(v\_ \mapsto x\_ \mid x\_ \in RReal \wedge Rzero \mapsto v\_ \in leq)\}$ 
111 THEN
112   act1:
113      $t, v, x :|$ 
114      $t' = tp \wedge$ 
115      $v' \in RReal \mapsto RReal \wedge Closed2Closed(Rzero, t') \subseteq dom(v') \wedge$ 
116      $x' \in RReal \mapsto RReal \wedge Closed2Closed(Rzero, t') \subseteq dom(x') \wedge$ 
117      $CBAPsolutionOf($ 
118        $t, t', bind(v, x), bind(v', x'),$ 
119        $ode(f\_deceleration(t \mapsto v(t)), v(t) \mapsto x(t), t),$ 
120        $\{(v\_ \mapsto x\_ \mid x\_ \in RReal \wedge Rzero \mapsto v\_ \in leq)\}$ 
121      $)$ 
122 END
123
124 ctrl_actuate_stabilize
125 REFINES Actuate
126 ANY tp
127 WHERE
128   grd0:  $tp \in RRealPlus \wedge t \mapsto tp \in lt$ 
129   grd1:  $x\_s \in \{stabilizing, stopped\}$ 
130 WITH
131   e:  $e = ode(f\_stable, v(t) \mapsto x(t), t)$ 
132   s:  $s = \{stabilizing, stopped\}$ 
133    $x\_p'$ :  $x\_p' = bind(v', x')$ 
134   Inv:
135      $Inv = \{(v\_ \mapsto x\_ \mid v\_ \in RReal \wedge x\_ \in RReal \wedge$ 
136        $plus(x\_ \mapsto divide(times(v\_ \mapsto v\_)) \mapsto times(Rtwo \mapsto b))) \mapsto SP \in lt\}$ 
137 THEN
138   act1:
139      $t, v, x :|$ 
140      $t' = tp \wedge$ 
141      $v' \in RReal \mapsto RReal \wedge Closed2Closed(Rzero, t') \subseteq dom(v') \wedge$ 
142      $x' \in RReal \mapsto RReal \wedge Closed2Closed(Rzero, t') \subseteq dom(x') \wedge$ 
143      $CBAPsolutionOf($ 
144        $t, t', bind(v, x), bind(v', x'),$ 
145        $ode(f\_stable, v(t) \mapsto x(t), t),$ 
146        $\{(v\_ \mapsto x\_ \mid v\_ \in RReal \wedge x\_ \in RReal \wedge$ 
147          $plus(x\_ \mapsto divide(times(v\_ \mapsto v\_)) \mapsto times(Rtwo \mapsto b))) \mapsto SP \in lt\}$ 

```

```

148 )
149 END
150
151 ctrl_actuate_accelerate
152 REFINES Actuate
153 ANY tp
154 WHERE
155   grd0:  $tp \in RRealPlus \wedge t \mapsto tp \in lt$ 
156   grd1:  $x\_s = accelerating$ 
157 WITH
158   e:  $e = ode(f\_acceleration, v(t) \mapsto x(t), t)$ 
159   s:  $s = \{accelerating\}$ 
160   x_p':  $x\_p' = bind(v', x')$ 
161   Inv:
162      $Inv = \{(v\_ \mapsto x\_ ) \mid v\_ \in RReal \wedge x\_ \in RReal \wedge$ 
163        $plus(x\_ \mapsto divide(times(v\_ \mapsto v\_ ) \mapsto times(Rtwo \mapsto b))) \mapsto SP \in lt \wedge$ 
164        $v\_ \mapsto Vmax \in leq\}$ 
165 THEN
166   act1:
167     t, v, x :|
168      $t' = tp \wedge$ 
169      $v' \in RReal \leftrightarrow RReal \wedge Closed2Closed(Rzero, t') \subseteq dom(v') \wedge$ 
170      $x' \in RReal \leftrightarrow RReal \wedge Closed2Closed(Rzero, t') \subseteq dom(x') \wedge$ 
171     CBASolutionOf(
172       t, t', bind(v, x), bind(v', x'),
173       ode(f_acceleration, v(t) \mapsto x(t), t),
174        $\{(v\_ \mapsto x\_ ) \mid v\_ \in RReal \wedge x\_ \in RReal \wedge$ 
175          $plus(x\_ \mapsto divide(times(v\_ \mapsto v\_ ) \mapsto times(Rtwo \mapsto b))) \mapsto SP \in lt \wedge$ 
176          $v\_ \mapsto Vmax \in leq\}$ 
177     )
178 END
179
180 END

```