Contents

CONTEXT c0
SETS
CLOCKS
CONSTANTS
Infinity
AXIOMS
axm1: $Infinity > 0$
axm2: $Infinity \geq 100$
for animb
END

CONTEXT belt_c0_clks
EXTENDS c0
CONSTANTS
bclks
b1
b2
tb
tp
AXIOMS
axm2: $bclks \subseteq CLOCKS$
axm1: $partition(bclks, \{b1\}, \{b2\})$
axm4: $tb > 0$
axm5: $tp > 0$
axm6: $tb \geq 5$
for aminb
axm7: $tp \geq 2$
for aminb
END

CONTEXT belt_press_c
EXTENDS belt_c0_clks,press_c1_clks
AXIOMS
axm5: $pclks \cap bclks = \varnothing$
new added one
END

CONTEXT press_c0

CONSTANTS

bottom

middle

top

AXIOMS

axm3: $bottom \in \mathbb{R}$

axm4: $middle \in \mathbb{R}$

axm5: $top \in \mathbb{R}$

axm6: $top > middle$

axm7: $middle > bottom$

axm8: ⟨theorem⟩ $top > bottom$

END

MACHINE press0
SEES press_c0
VARIABLES
position
work1
work3
work2
INVARIANTS
inv1: $position \in \{bottom, middle, top\}$
inv4: $work1 = TRUE \Rightarrow position = middle$
inv5: $work2 = TRUE \Rightarrow position = top$
inv6: $work3 = TRUE \Rightarrow position = bottom$
EVENTS
Initialisation
begin
act2: $position := middle$
act5: $work1 := FALSE$
act6: $work3 := FALSE$
act7: $work2 := FALSE$
end
Event Loading_start ⟨ordinary⟩ $\widehat{=}$
when
grd1: $position = middle$
grd3: $work1 = FALSE$
then
act2: $work1 := TRUE$
end
Event Loading ⟨ordinary⟩ $\widehat{=}$
when
grd2: $work1 = TRUE$
then
act1: $position := top$
act2: $work1 := FALSE$
end
Event Pressing_start ⟨ordinary⟩ $\widehat{=}$
when
grd1: $position = top$
grd2: $work2 = FALSE$
then
act1: $work2 := TRUE$
end
Event Pressing ⟨ordinary⟩ $\widehat{=}$
when
grd1: $work2 = TRUE$
then
act2: $position := bottom$
act3: $work2 := FALSE$
end
Event Unloading_start ⟨ordinary⟩ $\widehat{=}$
when
grd1: $position = bottom$
grd3: $work3 = FALSE$
then
act2: $work3 := TRUE$
end
Event Unloading ⟨ordinary⟩ $\widehat{=}$

when

grd2: $work3 = TRUE$

then

act2: $position := middle$

act3: $work3 := FALSE$

end

END

MACHINE press1

Using time and Click

REFINES press0

SEES press_c1_clks

VARIABLES

position

work1

work2

work3

lbTimer2

now

ubTimer2

INVARIANTS

inv12: $lbTimer2 \in \{p1, p2, p3\} \to \mathbb{R}$

inv13: $now \in \mathbb{R}$

inv9: $work1 = FALSE \Rightarrow lbTimer2(p1) = 0$

inv10: $work2 = FALSE \Rightarrow lbTimer2(p2) = 0$

inv11: $work3 = FALSE \Rightarrow lbTimer2(p3) = 0$

inv14: $ubTimer2 \in \{p1, p2, p3\} \to \mathbb{R}$

EVENTS

Initialisation ⟨extended⟩

begin

act2: $position := middle$

act5: $work1 := FALSE$

act6: $work3 := FALSE$

act7: $work2 := FALSE$

act15: $lbTimer2 := \{p1 \mapsto 0, p2 \mapsto 0, p3 \mapsto 0\}$

act16: $now := 0$

act17: $ubTimer2 := \{p1 \mapsto ubTa, p2 \mapsto Infinity, p3 \mapsto Infinity\}$

end

Event Loading_start ⟨ordinary⟩ $\widehat{=}$

extends Loading_start

when

grd1: $position = middle$

grd3: $work1 = FALSE$

then

act2: $work1 := TRUE$

act7: $lbTimer2(p1) := lbTa$

act8: $ubTimer2(p1) := ubTa$

end

Event Loading ⟨ordinary⟩ $\widehat{=}$

extends Loading

when

grd2: $work1 = TRUE$

grd5: $lbTimer2(p1) = 0$

then

act1: $position := top$

act2: $work1 := FALSE$

act3: $ubTimer2(p1) := Infinity$

end

Event Pressing_start ⟨ordinary⟩ $\widehat{=}$

extends Pressing_start

when

grd1: $position = top$

grd2: $work2 = FALSE$

then
act1: $work2 := TRUE$
act4: $lbTimer2(p2) := lbTb$
act5: $ubTimer2(p2) := ubTb$
end
Event Pressing ⟨ordinary⟩ $\widehat{=}$
extends Pressing
when
grd1: $work2 = TRUE$
grd4: $lbTimer2(p2) = 0$
then
act2: $position := bottom$
act3: $work2 := FALSE$
act4: $ubTimer2(p2) := Infinity$
end
Event Unloading_start ⟨ordinary⟩ $\widehat{=}$
extends Unloading_start
when
grd1: $position = bottom$
grd3: $work3 = FALSE$
then
act2: $work3 := TRUE$
act6: $lbTimer2(p3) := lbTc$
act7: $ubTimer2(p3) := ubTc$
end
Event Unloading ⟨ordinary⟩ $\widehat{=}$
extends Unloading
when
grd2: $work3 = TRUE$
grd5: $lbTimer2(p3) = 0$
then
act2: $position := middle$
act3: $work3 := FALSE$
act4: $ubTimer2(p3) := Infinity$
end
Event Click ⟨ordinary⟩ $\widehat{=}$
any
w
where
grd1: $w > 0$
grd2: $w \leq min(ran(ubTimer2))$
then
act1: $now := now + w$
act2: $lbTimer2 := \{c \mapsto v | c \in dom(lbTimer2) \land v = max(\{0, lbTimer2(c) - w\})\}$
act3: $ubTimer2 := ubTimer2 \lhd\!\!\!\!- \{c \mapsto v | c \in dom(ubTimer2 \rhd\!\!\!\!- \{Infinity\}) \land v = ubTimer2(c) - w\}$
end
END

MACHINE belt0
SEES belt_c0_clks
VARIABLES
sensor1
lbTimer0
now
ubTimer0
INVARIANTS
inv2: $sensor1 \in BOOL$
inv4: $lbTimer0 \in \{b1\} \rightarrow \mathbb{R}$
inv5: $now \in \mathbb{R}$
inv6: $ubTimer0 \in \{b1\} \rightarrow \mathbb{R}$
DLF:
$(((sensor1 = FALSE) \land (lbTimer0(b1) = 0)) \lor (sensor1 = TRUE) \lor (\exists w \cdot ((w > 0) \land (w \leq min(ran(ubTimer0)))))$
inv7: ⟨theorem⟩ $min(ran(ubTimer0)) = 0 \Rightarrow ubTimer0(b1) = 0$
inv8: $ubTimer0(b1) = 0 \Rightarrow sensor1 = TRUE$
inv9: $sensor1 = FALSE \Rightarrow ubTimer0(b1) = Infinity$
EVENTS
Initialisation
begin
act1: $sensor1 := TRUE$
act3: $lbTimer0 := \{b1 \mapsto 0\}$
act4: $now := 0$
act5: $ubTimer0 := \{b1 \mapsto Infinity\}$
end
Event Belt_1 ⟨ordinary⟩ $\widehat{=}$
when
grd1: $sensor1 = FALSE$
grd2: $lbTimer0(b1) = 0$
then
act1: $sensor1 := TRUE$
act2: $lbTimer0(b1) := tb$
act3: $ubTimer0(b1) := tp$
end
Event loading_start ⟨ordinary⟩ $\widehat{=}$
when
grd1: $sensor1 = TRUE$
then
act1: $sensor1 := FALSE$
act2: $ubTimer0(b1) := Infinity$
end
Event Click ⟨ordinary⟩ $\widehat{=}$
any
w
where
grd5: $w > 0$
grd6: $w \leq min(ran(ubTimer0))$
then
act1: $lbTimer0 := \{c \mapsto v | c \in dom(lbTimer0) \land v = max(\{0, lbTimer0(c) - w\})\}$
act3: $ubTimer0 := ubTimer0 \lhd\!\!\!\!- \{c \mapsto v | c \in dom(ubTimer0 \rhd\!\!\!\!> \{Infinity\}) \land v = ubTimer0(c) - w\}$
act2: $now := now + w$
end
END

MACHINE belt1
REFINES belt0
SEES belt_c0_clks
VARIABLES
sensor1
sensor2
lbTimer1
now
ubTimer1
lbTimer0
ubTimer0
INVARIANTS
inv3: $lbTimer1 \in \{b1, b2\} \to \mathbb{R}$
inv4: $ubTimer1 \in \{b1, b2\} \to \mathbb{R}$
inv5: $sensor2 \in BOOL$
inv1: $lbTimer0 \subseteq lbTimer1$
inv2: $ubTimer0 \subseteq ubTimer1$
EVENTS
Initialisation ⟨extended⟩
begin
act1: $sensor1 := TRUE$
act3: $lbTimer0 := \{b1 \mapsto 0\}$
act4: $now := 0$
act5: $ubTimer0 := \{b1 \mapsto Infinity\}$
act6: $sensor2 := FALSE$
act7: $lbTimer1 := \{b1 \mapsto 0, b2 \mapsto 0\}$
act8: $ubTimer1 := \{b1 \mapsto Infinity, b2 \mapsto Infinity\}$
end
Event Belt_1 ⟨ordinary⟩ $\widehat{=}$
extends Belt_1
when
grd1: $sensor1 = FALSE$
grd2: $lbTimer0(b1) = 0$
grd3: $lbTimer1(b1) = 0$
then
act1: $sensor1 := TRUE$
act2: $lbTimer0(b1) := tb$
act3: $ubTimer0(b1) := tp$
act4: $lbTimer1(b1) := tb$
act5: $ubTimer1(b1) := tp$
end
Event loading_start ⟨ordinary⟩ $\widehat{=}$
extends loading_start
when
grd1: $sensor1 = TRUE$
then
act1: $sensor1 := FALSE$
act2: $ubTimer0(b1) := Infinity$
act3: $ubTimer1(b1) := Infinity$
end
Event Belt_2 ⟨ordinary⟩ $\widehat{=}$
when
grd1: $sensor2 = TRUE$
grd2: $lbTimer1(b2) = 0$
then

act1: $sensor2 := FALSE$
act2: $lbTimer1(b2) := tb$
act3: $ubTimer1(b2) := tp$

end

Event unloading_start ⟨ordinary⟩ $\widehat{=}$

when

grd1: $sensor2 = FALSE$

then

act1: $sensor2 := TRUE$
act2: $ubTimer1(b2) := Infinity$

end

Event Click ⟨ordinary⟩ $\widehat{=}$

refines Click

any

w

where

grd5: $w > 0$
grd7: $w \leq min(ran(ubTimer1))$
grd6: ⟨theorem⟩ $w \leq min(ran(ubTimer0))$

then

act1: $lbTimer0 := \{c \mapsto v | c \in dom(lbTimer0) \land v = max(\{0, lbTimer0(c) - w\})\}$
act3: $ubTimer0 := ubTimer0 \lhd\!\!\!\!- \{c \mapsto v | c \in dom(ubTimer0 \rhd \{Infinity\}) \land v = ubTimer0(c) - w\}$
act2: $now := now + w$
act4: $lbTimer1 := \{c \mapsto v | c \in dom(lbTimer1) \land v = max(\{0, lbTimer1(c) - w\})\}$
act5: $ubTimer1 := ubTimer1 \lhd\!\!\!\!- \{c \mapsto v | c \in dom(ubTimer1 \rhd \{Infinity\}) \land v = ubTimer1(c) - w\}$

end

END

MACHINE belt2
REFINES belt1
SEES belt_c0_clks
VARIABLES
sensor1
sensor2
lbTimer1
now
ubTimer1
EVENTS
Initialisation
begin
act1: $sensor1 := TRUE$
act4: $now := 0$
act6: $sensor2 := FALSE$
act7: $lbTimer1 := \{b1 \mapsto 0, b2 \mapsto 0\}$
act8: $ubTimer1 := \{b1 \mapsto Infinity, b2 \mapsto Infinity\}$
end
Event Belt_1 ⟨ordinary⟩ $\widehat{=}$
refines Belt_1
when
grd1: $sensor1 = FALSE$
grd3: $lbTimer1(b1) = 0$
then
act1: $sensor1 := TRUE$
act4: $lbTimer1(b1) := tb$
act5: $ubTimer1(b1) := tp$
end
Event loading_start ⟨ordinary⟩ $\widehat{=}$
refines loading_start
when
grd1: $sensor1 = TRUE$
then
act1: $sensor1 := FALSE$
act3: $ubTimer1(b1) := Infinity$
end
Event Belt_2 ⟨ordinary⟩ $\widehat{=}$
extends Belt_2
when
grd1: $sensor2 = TRUE$
grd2: $lbTimer1(b2) = 0$
then
act1: $sensor2 := FALSE$
act2: $lbTimer1(b2) := tb$
act3: $ubTimer1(b2) := tp$
end
Event unloading_start ⟨ordinary⟩ $\widehat{=}$
extends unloading_start
when
grd1: $sensor2 = FALSE$
then
act1: $sensor2 := TRUE$
act2: $ubTimer1(b2) := Infinity$
end
Event Click ⟨ordinary⟩ $\widehat{=}$
refines Click

any

w

where

grd5: $w > 0$

grd7: $w \leq min(ran(ubTimer1))$

then

act2: $now := now + w$

act4: $lbTimer1 := \{c \mapsto v | c \in dom(lbTimer1) \land v = max(\{0, lbTimer1(c) - w\})\}$

act5: $ubTimer1 := ubTimer1 \lhd\!\!\!\!- \{c \mapsto v | c \in dom(ubTimer1 \rhd\!\!\!\!- \{Infinity\}) \land v = ubTimer1(c) - w\}$

end

END

MACHINE belt2_press1
REFINES belt2
SEES belt_press_c
VARIABLES

sensor1
position
work1
work2
work3
lbTimer2
now
ubTimer2
sensor2
lbTimer1
ubTimer1

INVARIANTS

inv0: $work2 \in BOOL$
inv1: $now \in \mathbb{Z}$
inv2: $position \in \mathbb{Z}$
inv3: $sensor2 \in BOOL$
inv4: $ubTimer2 \in \mathbb{P}(CLOCKS \times \mathbb{Z})$
inv5: $sensor1 \in BOOL$
inv6: $lbTimer1 \in \mathbb{P}(CLOCKS \times \mathbb{Z})$
inv7: $work1 \in BOOL$
inv8: $work3 \in BOOL$
inv9: $lbTimer2 \in \mathbb{P}(CLOCKS \times \mathbb{Z})$
inv12: $lbTimer2 \in pclks \rightarrow \mathbb{R}$
inv14: $ubTimer2 \in pclks \rightarrow \mathbb{R}$
inv10: $ubTimer1 \in bclks \rightarrow \mathbb{R}$

EVENTS
Initialisation
begin

belt2·act1: $sensor1 := TRUE$
press1.act2: $position := middle$
press1.act5: $work1 := FALSE$
press1.act6: $work3 := FALSE$
press1.act7: $work2 := FALSE$
press1.act15: $lbTimer2 := \{p1 \mapsto 0, p2 \mapsto 0, p3 \mapsto 0\}$
press1.act16: $now := 0$
press1.act17: $ubTimer2 := \{p1 \mapsto ubTa, p2 \mapsto Infinity, p3 \mapsto Infinity\}$
belt2·act2: $sensor2 := FALSE$
belt2·act3: $lbTimer1 := \{b1 \mapsto 0, b2 \mapsto 0\}$
belt2.act5: $ubTimer1 := \{b1 \mapsto Infinity, b2 \mapsto Infinity\}$

end
Event belt2·Belt_1 ⟨ordinary⟩ $\widehat{=}$
refines Belt_1
when

belt2·grd1: $sensor1 = FALSE$
belt2·grd2: $lbTimer1(b1) = 0$

then

belt2·act1: $sensor1 := TRUE$
belt2·act2: $lbTimer1(b1) := tb$
act3: $ubTimer1(b1) := tp$

end

Event belt2·Belt_2 ⟨ordinary⟩ $\widehat{=}$
refines Belt_2
when
belt2·grd1: $sensor2 = TRUE$
belt2·grd2: $lbTimer1(b2) = 0$
then
belt2·act1: $sensor2 := FALSE$
belt2·act2: $lbTimer1(b2) := tb$
belt2.act3: $ubTimer1(b2) := tp$
end
Event belt2·loading_start_press1·Loading_start ⟨ordinary⟩ $\widehat{=}$
refines loading_start
when
belt2·grd1: $sensor1 = TRUE$
press1.grd1: $position = middle$
press1.grd3: $work1 = FALSE$
then
press1.act2: $work1 := TRUE$
press1.act7: $lbTimer2(p1) := lbTa$
belt2·act1: $sensor1 := FALSE$
press1.act8: $ubTimer2(p1) := ubTa$
belt2.act2: $ubTimer1(b1) := Infinity$
end
Event belt2·unloading_start_press1·Unloading_start ⟨ordinary⟩ $\widehat{=}$
refines unloading_start
when
press1.grd1: $position = bottom$
belt2·grd1: $sensor2 = FALSE$
press1.grd3: $work3 = FALSE$
then
press1.act2: $work3 := TRUE$
press1.act6: $lbTimer2(p3) := lbTc$
belt2·act1: $sensor2 := TRUE$
press1.act7: $ubTimer2(p3) := ubTc$
belt2.act2: $ubTimer1(b2) := Infinity$
end
Event press1.Loading ⟨ordinary⟩ $\widehat{=}$
when
press1.grd2: $work1 = TRUE$
press1.grd5: $lbTimer2(p1) = 0$
then
press1.act1: $position := top$
press1.act2: $work1 := FALSE$
press1.act3: $ubTimer2(p1) := Infinity$
end
Event press1.Pressing_start ⟨ordinary⟩ $\widehat{=}$
when
press1.grd1: $position = top$
press1.grd2: $work2 = FALSE$
then
press1.act1: $work2 := TRUE$
press1.act4: $lbTimer2(p2) := lbTb$
press1.act5: $ubTimer2(p2) := ubTb$
end
Event press1.Pressing ⟨ordinary⟩ $\widehat{=}$
when
press1.grd1: $work2 = TRUE$
press1.grd4: $lbTimer2(p2) = 0$

then

press1.act2: $position := bottom$

press1.act3: $work2 := FALSE$

press1.act4: $ubTimer2(p2) := Infinity$

end

Event press1.Unloading ⟨ordinary⟩ $\widehat{=}$

when

press1.grd2: $work3 = TRUE$

press1.grd5: $lbTimer2(p3) = 0$

then

press1.act2: $position := middle$

press1.act3: $work3 := FALSE$

press1.act4: $ubTimer2(p3) := Infinity$

end

Event belt2·Click_press1·Click ⟨ordinary⟩ $\widehat{=}$

refines Click

any

w

where

belt2·grd5: $w > 0$

press1·grd2: $w \leq min(ran(ubTimer2))$

grd6: $w \leq min(ran(ubTimer1))$

then

belt2·act2: $now := now + w$

belt2·act1: $lbTimer1 := lbTimer1 \lhd\!\!\!\cdot \{c \mapsto v | c \in bclks \wedge v = max(\{0, lbTimer1(c) - w\})\}$

press1·act2: $lbTimer2 := \{c \mapsto v | c \in dom(lbTimer2) \wedge v = max(\{0, lbTimer2(c) - w\})\}$

press1·act3: $ubTimer2 := ubTimer2 \lhd\!\!\!\cdot \{c \mapsto v | c \in dom(ubTimer2 \rhd \{Infinity\}) \wedge v = ubTimer2(c) - w\}$

belt2.act3: $ubTimer1 := ubTimer1 \lhd\!\!\!\cdot \{c \mapsto v | c \in dom(ubTimer1 \rhd \{Infinity\}) \wedge v = ubTimer1(c) - w\}$

end

END