Contents

CONTEXT C0
END

CONTEXT Sensor

SETS

SENSOR

CONSTANTS

on

off

AXIOMS

axm1: $SENSOR = \{on, off\}$

axm2: $on \neq off$

END

CONTEXT Colors

SETS

COLORS

CONSTANTS

red

green

AXIOMS

axm1: $COLORS = \{green, red\}$

axm2: $green \neq red$

END

MACHINE M0

First iteration of the model. Basic behaviour.

SEES C0

VARIABLES

a Room occupied

INVARIANTS

inv1: $a \in BOOL$

EVENTS

Initialisation ⟨extended⟩

begin

act1: $a := FALSE$

end

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

when

grd1: $a = FALSE$

then

act1: $a := TRUE$

end

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

when

grd1: $a = TRUE$

then

act1: $a := FALSE$

end

END

MACHINE M1
REFINES M0
SEES C0,Colors
VARIABLES

  a Room occupied
  tl Color of the traffic light

INVARIANTS

  inv1: $tl \in COLORS$
  inv2: $tl = green \Rightarrow a = FALSE$

EVENTS

Initialisation ⟨extended⟩

```
    begin
        act1: $a := FALSE$
        act2: $tl := red$
    end
```

Event PERSON_IN ⟨ordinary⟩ $\widehat{=}$
extends PERSON_IN

```
    when
        grd1: $a = FALSE$
        grd2: $tl = green$
    then
        act1: $a := TRUE$
        act2: $tl := red$
    end
```

Event PERSON_OUT ⟨ordinary⟩ $\widehat{=}$
extends PERSON_OUT

```
    when
        grd1: $a = TRUE$
    then
        act1: $a := FALSE$
    end
```

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

```
    when
        grd1: $tl = red$
        grd2: $a = FALSE$
    then
        act1: $tl := green$
    end
```

END

MACHINE M2
REFINES M1
SEES C0,Colors,Sensor
VARIABLES

a Room occupied

tl Color of the traffic light

A Room physically occupied

SR Sensor

wire_01 wire from sensor to controller

INVARIANTS

inv1: $A \in BOOL$

inv2: $SR \in SENSOR$

inv3: $wire\_01 \in BOOL$

inv4: $wire\_01 = TRUE \Rightarrow tl = green$

The wire did change => the traffic light was green (as someone left the sensor)

inv5: $SR = on \Rightarrow wire\_01 = FALSE$

The sensor is on => the wire didn't just change

inv8: $tl = green \Rightarrow (a = FALSE \land SR = on) \lor wire\_01 = TRUE$

The light is green => the wire just changed or there is someone standing and the controller knows the room is empty

inv9: $wire\_01 = FALSE \Leftrightarrow A = a$

The wire didn't change <=> the reality and the controller coincide

inv6: $wire\_01 = TRUE \Rightarrow A = TRUE \land a = FALSE$

The wire just changed => the reality and the controlled disagree, specifically in reality A = TRUE

inv10: $SR = off \land wire\_01 = FALSE \Rightarrow tl = red$

No one is standing and the wire didn't just change => the light is red

inv11: $A = FALSE \Rightarrow a = FALSE$

Whenever the room is empty in reality, the controller knows (magic event)

inv13: $a = TRUE \Rightarrow A = TRUE$

If the controller thinks the room is full, in reality it will be

inv12: $a = TRUE \Rightarrow tl = red$

If the controller thinks the room is full, the light will always be red

inv7:

$(a = FALSE \land wire\_01 = TRUE) \lor$
$(a = TRUE \land A = TRUE) \lor$
$(SR = on \land tl = red \land a = FALSE) \lor$
$(SR = off \land wire\_01 = FALSE) \lor$
$(SR = on \land tl = green)$

EVENTS

Initialisation ⟨extended⟩

begin

act1: $a := FALSE$
act2: $tl := red$
act4: $A := FALSE$
act5: $SR := off$
act6: $wire\_01 := FALSE$

end

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

Person walks in as seen by the controller. Changes the state and the light

refines PERSON_IN

when

grd1: $a = FALSE$
grd2: $wire\_01 = TRUE$

then

```
        act1: $a := TRUE$
        act3: $tl := red$
        act2: $wire\_01 := FALSE$
    end
Event PERSON_OUT ⟨ordinary⟩ $\widehat{=}$
    Magic event.
extends PERSON_OUT
    when
        grd1: $a = TRUE$
        grd2: $A = TRUE$
    then
        act1: $a := FALSE$
        act2: $A := FALSE$
    end
Event TL_GREEN ⟨ordinary⟩ $\widehat{=}$
    Change the light to green when the room seems empty and there is someone in the sensor
extends TL_GREEN
    when
        grd1: $tl = red$
        grd2: $a = FALSE$
        grd5: $SR = on$
    then
        act1: $tl := green$
    end
Event SR_ARRIVE ⟨ordinary⟩ $\widehat{=}$
    Activate the sensor when there is no-one standing and the last change was processed
    when
        grd1: $SR = off$
        grd2: $wire\_01 = FALSE$
    then
        act1: $SR := on$
    end
Event SR_DEPARTURE ⟨ordinary⟩ $\widehat{=}$
    Deactivate the sensor when someone leaves (tl must be green!)
    when
        grd1: $SR = on$
        grd2: $tl = green$
    then
        act1: $SR := off$
        act2: $wire\_01 := TRUE$
        act3: $A := TRUE$
    end
END
```