

MACHINE m3

REFINES m2

SEES cd, COLOR, SENSOR

VARIABLES

a as in previous abstraction
b as in previous abstraction
c as in previous abstraction
ml_tl as in previous abstraction
il_tl as in previous abstraction
il_pass as in previous abstraction
ml_pass as in previous abstraction
A Physical number of cars on bridge going to island
B Physical number of cars on island
C Physical number of cars on bridgegoing to mainland
ML_OUT_SR sensor
ML_IN_SR sensor
IL_OUT_SR sensor
IL_IN_SR sensor
ml_out_10 wire from sensor to controller
il_out_10 wire from sensor to controller
ml_in_10 wire from sensor to controller
il_in_10 wire from sensor to controller

INVARIANTS

inv24 : $A \in \mathbb{N}$
inv25 : $B \in \mathbb{N}$
inv26 : $C \in \mathbb{N}$
inv27 : $ML_OUT_SR \in Sensor$
inv28 : $ML_IN_SR \in Sensor$
inv29 : $IL_OUT_SR \in Sensor$
inv30 : $IL_IN_SR \in Sensor$
inv31 : $ml_out_10 \in BOOL$
inv32 : $il_out_10 \in BOOL$
inv33 : $ml_in_10 \in BOOL$
inv34 : $il_in_10 \in BOOL$
inv4 : $ml_out_10 = TRUE \Rightarrow ml_tl = green$
A car passed, the traffic light must have been green
inv5 : $il_out_10 = TRUE \Rightarrow il_tl = green$
A car passed, the traffic light must have been green
inv1 : $IL_IN_SR = on \Rightarrow A > 0$
car on sensor means there is a car
inv2 : $IL_OUT_SR = on \Rightarrow B > 0$
car on sensor means there is a ca
inv3 : $ML_IN_SR = on \Rightarrow C > 0$
car on sensor means there is a ca
inv6 : $IL_IN_SR = on \Rightarrow il_in_10 = FALSE$
inv7 : $IL_OUT_SR = on \Rightarrow il_out_10 = FALSE$
inv8 : $ML_IN_SR = on \Rightarrow ml_in_10 = FALSE$

$\text{inv9} : ML_OUT_SR = on \Rightarrow ml_out_10 = FALSE$
 $\text{inv10} : il_in_10 = TRUE \wedge ml_out_10 = TRUE \Rightarrow A = a$
 Connection between physical and logical numbers
 $\text{inv11} : il_in_10 = FALSE \wedge ml_out_10 = TRUE \Rightarrow A = a + 1$
 $\text{inv12} : il_in_10 = TRUE \wedge ml_out_10 = FALSE \Rightarrow A = a - 1$
 $\text{inv13} : il_in_10 = FALSE \wedge ml_out_10 = FALSE \Rightarrow A = a$
 $\text{inv14} : il_in_10 = TRUE \wedge il_out_10 = TRUE \Rightarrow B = b$
 $\text{inv15} : il_in_10 = TRUE \wedge il_out_10 = FALSE \Rightarrow B = b + 1$
 $\text{inv16} : il_in_10 = FALSE \wedge il_out_10 = TRUE \Rightarrow B = b - 1$
 $\text{inv17} : il_in_10 = FALSE \wedge il_out_10 = FALSE \Rightarrow B = b$
 $\text{inv18} : il_out_10 = TRUE \wedge ml_in_10 = TRUE \Rightarrow C = c$
 $\text{inv19} : il_out_10 = TRUE \wedge ml_in_10 = FALSE \Rightarrow C = c + 1$
 $\text{inv20} : il_out_10 = FALSE \wedge ml_in_10 = TRUE \Rightarrow C = c - 1$
 $\text{inv21} : il_out_10 = FALSE \wedge ml_in_10 = FALSE \Rightarrow C = c$
 $\text{inv22} : A = 0 \vee C = 0$
 Law of physical variables
 $\text{inv23} : A + B + C \leq d$
 Law of physical variables

EVENTS

Initialisation

begin
 $\text{act2} : a := 0$
 $\text{act3} : b := 0$
 $\text{act4} : c := 0$
 $\text{act1} : ml_tl := red$
 $\text{act5} : il_tl := red$
 $\text{act6} : ml_pass := 1$
 $\text{act7} : il_pass := 1$
 $\text{act15} : ml_out_10 := FALSE$
 $\text{qct16} : il_out_10 := FALSE$
 $\text{act17} : ml_in_10 := FALSE$
 $\text{act18} : il_in_10 := FALSE$
 $\text{act8} : A := 0$
 $\text{act9} : B := 0$
 $\text{act10} : C := 0$
 $\text{act11} : ML_IN_SR := off$
 $\text{act12} : ML_OUT_SR := off$
 $\text{act13} : IL_OUT_SR := off$
 $\text{act14} : IL_IN_SR := off$
end

Event $ML_out1 \hat{=}$

refines ML_out1

when
 $\text{grd1} : ml_out_10 = TRUE$
 $\text{grd2} : a + b + 1 < d$
then
 $\text{act1} : a := a + 1$
 $\text{act2} : ml_pass := 1$
 $\text{act3} : ml_out_10 := FALSE$
end

Event $ML_out2 \hat{=}$

refines ML_out2

when
 $\text{grd1} : ml_out_10 = TRUE$

```

    grd2:  $a + b + 1 = d$ 
  then
    act1:  $a := a + 1$ 
    act2:  $ml\_tl := red$ 
    act3:  $ml\_pass := 1$ 
    act4:  $ml\_out\_10 := FALSE$ 
  end
Event  $IL\_out1 \hat{=}$ 
refines  $IL\_out1$ 
  when
    grd1:  $il\_out\_10 = TRUE$ 
    grd2:  $b > 1$ 
  then
    act1:  $b := b - 1$ 
    act2:  $c := c + 1$ 
    act3:  $il\_pass := 1$ 
    act4:  $il\_out\_10 := FALSE$ 
  end
Event  $IL\_out2 \hat{=}$ 
refines  $IL\_out2$ 
  when
    grd1:  $il\_out\_10 = TRUE$ 
    grd2:  $b = 1$ 
  then
    act1:  $b := b - 1$ 
    act2:  $il\_tl := red$ 
    act3:  $c := c + 1$ 
    act4:  $il\_pass := 1$ 
    act5:  $il\_out\_10 := FALSE$ 
  end
Event  $ML\_tl\_green \hat{=}$ 
Status convergent
refines  $ML\_tl\_green$ 
  when
    grd1:  $ml\_tl = red$ 
    grd2:  $a + b < d$ 
    grd3:  $c = 0$ 
    grd4:  $il\_pass = 1$ 
    grd5:  $il\_out\_10 = FALSE$ 
    grd6:  $ML\_OUT\_SR = on$ 
  then
    act1:  $ml\_tl := green$ 
    act2:  $il\_tl := red$ 
    act3:  $ml\_pass := 0$ 
  end
Event  $IL\_tl\_green \hat{=}$ 
Status convergent
refines  $IL\_tl\_green$ 
  when
    grd1:  $il\_tl = red$ 
    grd2:  $0 < b$ 
    grd3:  $a = 0$ 
    grd4:  $ml\_pass = 1$ 
    grd5:  $ml\_out\_10 = FALSE$ 
    grd6:  $IL\_OUT\_SR = on$ 

```

```

    then
      act1 : il_tl := green
      act2 : ml_tl := red
      act3 : il_pass := 0
    end
Event ML_in  $\hat{=}$ 
refines ML_in
  when
    grd1 : ml_in_10 = TRUE
    grd2 : c > 0
  then
    act1 : c := c - 1
    act2 : ml_in_10 := FALSE
  end
Event IL_in  $\hat{=}$ 
refines IL_in
  when
    grd1 : il_in_10 = TRUE
    grd2 : 0 < a
  then
    act1 : a := a - 1
    act2 : b := b + 1
    act3 : il_in_10 := FALSE
  end
Event ML_OUT_ARR  $\hat{=}$ 
Physical Events
  when
    grd1 : ML_OUT_SR = off
    grd2 : ml_out_10 = FALSE
  then
    act1 : ML_OUT_SR := on
  end
Event ML_IN_ARR  $\hat{=}$ 
  when
    grd1 : ML_IN_SR = off
    grd2 : ml_in_10 = FALSE
    grd3 : C > 0
  then
    act1 : ML_IN_SR := on
  end
Event IL_IN_ARR  $\hat{=}$ 
  when
    grd1 : IL_IN_SR = off
    grd2 : il_in_10 = FALSE
    grd3 : A > 0
  then
    act1 : IL_IN_SR := on
  end
Event IL_OUT_AR  $\hat{=}$ 
  when
    grd1 : IL_OUT_SR = off
    grd2 : il_out_10 = FALSE
    grd3 : B > 0
  then
    act1 : IL_OUT_SR := on

```

```

    end
Event ML_OUT_DEP  $\hat{=}$ 
    when
        grd1 : ML_OUT_SR = on
        grd2 : ml_tl = green
    then
        act1 : ML_OUT_SR := off
        act2 : ml_out_10 := TRUE
        act3 : A := A + 1
    end
Event ML_IN_DEP  $\hat{=}$ 
    when
        grd1 : ML_IN_SR = on
    then
        act1 : ML_IN_SR := off
        act2 : ml_in_10 := TRUE
        act3 : C := C - 1
    end
Event IL_IN_DEP  $\hat{=}$ 
    when
        grd1 : IL_IN_SR = on
    then
        act1 : IL_IN_SR := off
        act2 : il_in_10 := TRUE
        act3 : A := A - 1
        act4 : B := B + 1
    end
Event IL_OUT_DEP  $\hat{=}$ 
    when
        grd1 : IL_OUT_SR = on
        grd2 : il_tl = green
    then
        act1 : IL_OUT_SR := off
        act2 : il_out_10 := TRUE
        act3 : B := B - 1
        act4 : C := C + 1
    end
END

```