

MACHINE m1

REFINES m0

SEES cd

VARIABLES

- a number of cars on bridge going to island
- b number of cars on island
- c number of cars on bridge going to mainland

INVARIANTS

inv1 : $a \in \mathbb{N}$

inv2 : $b \in \mathbb{N}$

inv3 : $c \in \mathbb{N}$

inv4 : $n = a + b + c$

Gluing invariant connecting the concrete variables (a, b, c) to the abstract one (n)

inv5 : $a = 0 \vee c = 0$

EVENTS

Initialisation

begin

act2 : $a := 0$

act3 : $b := 0$

act4 : $c := 0$

end

Event $ML_out \hat{=}$

leaving mainland

refines ML_out

when

grd1 : $a + b < d$

grd2 : $c = 0$

then

act1 : $a := a + 1$

end

Event $IL_in \hat{=}$

entering island

Status convergent

when

grd1 : $a > 0$

then

act1 : $a := a - 1$

act2 : $b := b + 1$

end

Event $IL_out \hat{=}$

leaving island

Status convergent

when

grd1 : $0 < b$

grd2 : $a = 0$

then

act1 : $b := b - 1$

act2 : $c := c + 1$

end

Event $ML_in \hat{=}$
entering mainland
refines ML_in
 when
 grd1 : $c > 0$
 then
 act2 : $c := c - 1$
 end
VARIANT
 $2 * a + b$
END