

MACHINE m1

SEES c1

VARIABLES

purse

abal

lost

INVARIANTS

inv1 : $\text{purse} \subseteq \text{PURSE}$

inv2 : $\text{abal} \in \text{purse} \rightarrow \mathbb{N}$

inv3 : $\text{lost} \in \text{purse} \rightarrow \mathbb{N}$

EVENTS

Initialisation

begin

act1 : $\text{purse} := \emptyset$

act2 : $\text{abal} := \emptyset$

act3 : $\text{lost} := \emptyset$

end

Event createPurse $\hat{=}$

any

p

a

where

grd1 : $p \in \text{PURSE} \setminus \text{purse}$

grd2 : $a \in \mathbb{N}$

grd3 : $a > 0$

then

act1 : $\text{purse} := \text{purse} \cup \{p\}$

act2 : $\text{abal}(p) := a$

act3 : $\text{lost}(p) := 0$

end

Event TransferOk $\hat{=}$

any

$p1$

$p2$

a

where

grd1 : $p1 \in \text{purse}$

grd2 : $p2 \in \text{purse}$

grd3 : $p1 \neq p2$

grd4 : $a \in \mathbb{N}$

grd6 : $\text{abal}(p1) \geq a$

then

act1 : $\text{abal} := (\text{abal} \triangleleft \{p1 \mapsto \text{abal}(p1) - a\}) \triangleleft \{p2 \mapsto \text{abal}(p2) + a\}$

end

Event TransferFail $\hat{=}$

any

$p1$

a

where

grd1 : $p1 \in \text{purse}$

grd2 : $a \in \mathbb{N}$

```
    grd4 :  $abal(p1) \geq a$ 
  then
    act1 :  $abal(p1) := abal(p1) - a$ 
    act2 :  $lost(p1) := lost(p1) + a$ 
  end
Event Recover  $\hat{=}$ 
  any
     $p1$ 
     $a$ 
  where
    grd1 :  $p1 \in purse$ 
    grd2 :  $a \in \mathbb{N}$ 
    grd4 :  $lost(p1) \geq a$ 
  then
    act2 :  $lost(p1) := lost(p1) - a$ 
    act1 :  $abal(p1) := abal(p1) + a$ 
  end
END
```