

MACHINE m3

REFINES m2

SEES c2

VARIABLES

bal
 purse
 trans
 from
 to
 am
 idle
 pending
 recover
 ended

INVARIANTS

inv1 : $pfrom^{-1} = (pending \triangleleft from)$
 better than $pfrom = (pending \triangleleft from)^{-1}$
inv2 : $lfrom^{-1} = (recover \triangleleft from)$

EVENTS

Initialisation

begin
 act1 : $purse := \emptyset$
 act2 : $bal := \emptyset$
 act3 : $trans := \emptyset$
 act4 : $idle := \emptyset$
 act5 : $pending := \emptyset$
 act6 : $recover := \emptyset$
 act7 : $ended := \emptyset$
 act10 : $from := \emptyset$
 act11 : $to := \emptyset$
 act12 : $am := \emptyset$
end

Event *createPurse* $\hat{=}$

refines *createPurse*

any
 p
 a
where
 grd1 : $p \in PURSE \setminus purse$
 grd2 : $a \in \mathbb{N}$
 grd3 : $a > 0$
then
 act1 : $purse := purse \cup \{p\}$
 act2 : $bal(p) := a$
end

Event *Start* $\hat{=}$

refines *Start*

any
 t
 p1

```

    p2
    a
  where
    grd1 :  $t \in TRANS \setminus trans$ 
    grd2 :  $p1 \in purse$ 
    grd3 :  $p2 \in purse$ 
    grd4 :  $a \in \mathbb{N}$ 
    grd5 :  $a > 0$ 
    grd6 :  $p1 \neq p2$ 
  then
    act1 :  $trans := trans \cup \{t\}$ 
    act2 :  $from(t) := p1$ 
    act3 :  $to(t) := p2$ 
    act4 :  $am(t) := a$ 
    act5 :  $idle := idle \cup \{t\}$ 
  end
Event Deduct  $\hat{=}$ 
refines Deduct
  any
    t
    p1
    a
  where
    grd1 :  $t \in idle$ 
    grd2 :  $p1 \in purse$ 
    grd4 :  $a \in \mathbb{N}$ 
    grd5 :  $a \leq bal(p1)$ 
    grd6 :  $p1 = from(t)$ 
    grd8 :  $a = am(t)$ 
  then
    act1 :  $pending := pending \cup \{t\}$ 
    act2 :  $idle := idle \setminus \{t\}$ 
    act3 :  $bal(p1) := bal(p1) - a$ 
  end
Event Increase  $\hat{=}$ 
refines Increase
  any
    t
    p1
    p2
    a
  where
    grd6 :  $t \in pending$ 
    grd1 :  $p1 \in purse$ 
    grd4 :  $p2 \in purse$ 
    grd5 :  $a \in \mathbb{N}$ 
    grd2 :  $from(t) = p1$ 
    grd3 :  $to(t) = p2$ 
    grd7 :  $am(t) = a$ 
  then
    act1 :  $bal(p2) := bal(p2) + a$ 
    act2 :  $ended := ended \cup \{t\}$ 
    act3 :  $pending := pending \setminus \{t\}$ 
  end
Event TransferFail  $\hat{=}$ 
refines TransferFail

```

```

any
  t
where
  grd1 :  $t \in \text{pending}$ 
with
  p1 :  $p1 = \text{from}(t)$ 
  a :  $a = \text{am}(t)$ 
then
  act2 :  $\text{recover} := \text{recover} \cup \{t\}$ 
  act3 :  $\text{pending} := \text{pending} \setminus \{t\}$ 
end
Event Recover  $\hat{=}$ 
refines Recover
any
  t
  p1
  a
where
  grd4 :  $t \in \text{recover}$ 
  grd1 :  $p1 \in \text{purse}$ 
  grd2 :  $a \in \mathbb{N}$ 
  grd5 :  $\text{from}(t) = p1$ 
  grd3 :  $a = \text{am}(t)$ 
then
  act1 :  $\text{bal}(p1) := \text{bal}(p1) + a$ 
  act3 :  $\text{ended} := \text{ended} \cup \{t\}$ 
  act4 :  $\text{recover} := \text{recover} \setminus \{t\}$ 
end
END

```