

MACHINE m2

REFINES m1

SEES c2

VARIABLES

bal
 purse
 trans
 from
 to
 am
 pfrom
 lfrom
 idle
 pending
 recover
 ended

INVARIANTS

inv1 : $trans \subseteq TRANS$
 inv2 : $from \in trans \rightarrow purse$
 inv3 : $to \in trans \rightarrow purse$
 inv4 : $am \in trans \rightarrow \mathbb{N}$
 inv5 : $idle \subseteq trans$
 inv6 : $pending \subseteq trans$
 inv7 : $recover \subseteq trans$
 inv8 : $ended \subseteq trans$
 inv9 : $bal \in purse \rightarrow \mathbb{N}$
 inv10 : $\forall t. t \in trans \Rightarrow from(t) \neq to(t)$
 inv11 : $finite(pending)$
 inv12 : $idle \cap pending = \emptyset$
 inv13 : $idle \cap recover = \emptyset$
 inv14 : $idle \cap ended = \emptyset$
 inv15 : $pending \cap recover = \emptyset$
 inv16 : $pending \cap ended = \emptyset$
 inv17 : $recover \cap ended = \emptyset$
 inv18 : $pfrom \in purse \leftrightarrow TRANS$
 inv19 : $ran(pfrom) = pending$
 inv27 : $finite(ran(am))$
 inv20 : $\forall p. p \in purse \Rightarrow abal(p) = bal(p) + sum(am[pfrom[\{p\}]])$
 inv21 : $pfrom^{-1} \in TRANS \leftrightarrow purse$
 inv22 : $lfrom \in purse \leftrightarrow TRANS$
 inv23 : $ran(lfrom) = recover$
 inv24 : $finite(recover)$
 inv25 : $lfrom^{-1} \in TRANS \leftrightarrow purse$
 inv26 : $\forall p. p \in purse \Rightarrow lost(p) = sum(am[lfrom[\{p\}]])$
 thm1 : $\forall p. p \in purse \Rightarrow finite(am[pfrom[\{p\}]])$
 thm2 : $\forall p. p \in purse \Rightarrow finite(am[lfrom[\{p\}]])$
 thm3 : $\forall t. t \in trans \Rightarrow finite(am[\{t\}])$

EVENTS**Initialisation****begin**

act1 : $purse := \emptyset$
 act2 : $bal := \emptyset$
 act3 : $trans := \emptyset$
 act4 : $idle := \emptyset$
 act5 : $pending := \emptyset$
 act6 : $recover := \emptyset$
 act7 : $ended := \emptyset$
 act8 : $pfrom := \emptyset$
 act9 : $lfrom := \emptyset$
 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** $Start \hat{=}$ **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** $Deduct \hat{=}$ **any**

t
 $p1$
 a

where

grd1 : $t \in idle$

```

    grd2 :  $p1 \in \text{purse}$ 
    grd4 :  $a \in \mathbb{N}$ 
    grd5 :  $a \leq \text{bal}(p1)$ 
    grd6 :  $p1 = \text{from}(t)$ 
    grd8 :  $a = \text{am}(t)$ 
  then
    act1 :  $\text{pending} := \text{pending} \cup \{t\}$ 
    act2 :  $\text{idle} := \text{idle} \setminus \{t\}$ 
    act3 :  $\text{bal}(p1) := \text{bal}(p1) - a$ 
    act4 :  $\text{pfrom} := \text{pfrom} \cup \{p1 \mapsto t\}$ 
  end
Event Increase  $\hat{=}$ 
refines TransferOk
  any
     $t$ 
     $p1$ 
     $p2$ 
     $a$ 
  where
    grd6 :  $t \in \text{pending}$ 
    grd1 :  $p1 \in \text{purse}$ 
    grd4 :  $p2 \in \text{purse}$ 
    grd5 :  $a \in \mathbb{N}$ 
    grd2 :  $\text{from}(t) = p1$ 
    grd3 :  $\text{to}(t) = p2$ 
    grd7 :  $\text{am}(t) = a$ 
    grd8 :  $p1 \mapsto t \in \text{pfrom}$ 
  then
    act1 :  $\text{bal}(p2) := \text{bal}(p2) + a$ 
    act2 :  $\text{ended} := \text{ended} \cup \{t\}$ 
    act3 :  $\text{pending} := \text{pending} \setminus \{t\}$ 
    act4 :  $\text{pfrom} := \text{pfrom} \setminus \{p1 \mapsto t\}$ 
  end
Event TransferFail  $\hat{=}$ 
refines TransferFail
  any
     $t$ 
     $p1$ 
     $a$ 
  where
    grd1 :  $t \in \text{pending}$ 
    grd2 :  $p1 \in \text{purse}$ 
    grd3 :  $a \in \mathbb{N}$ 
    grd4 :  $\text{from}(t) = p1$ 
    grd5 :  $\text{am}(t) = a$ 
    grd6 :  $p1 \mapsto t \in \text{pfrom}$ 
  then
    act1 :  $\text{recover} := \text{recover} \cup \{t\}$ 
    act2 :  $\text{pending} := \text{pending} \setminus \{t\}$ 
    act3 :  $\text{pfrom} := \text{pfrom} \setminus \{p1 \mapsto t\}$ 
    act4 :  $\text{lfrom} := \text{lfrom} \cup \{p1 \mapsto t\}$ 
  end
Event Recover  $\hat{=}$ 
refines Recover
  any
     $t$ 

```

```
    p1
    a
  where
    grd4 :  $t \in recover$ 
    grd1 :  $p1 \in purse$ 
    grd2 :  $a \in \mathbb{N}$ 
    grd5 :  $from(t) = p1$ 
    grd6 :  $p1 \mapsto t \in lfrom$ 
    grd3 :  $a = am(t)$ 
  then
    act1 :  $bal(p1) := bal(p1) + a$ 
    act3 :  $ended := ended \cup \{t\}$ 
    act4 :  $recover := recover \setminus \{t\}$ 
    act5 :  $lfrom := lfrom \setminus \{p1 \mapsto t\}$ 
  end
END
```