

MACHINE m4

REFINES m3

SEES c2

VARIABLES

bal
purse
trans
from
to
am
idleF
epr
epa
abortepv
abortepa
endF
idleT
epv
abortepv
endT

INVARIANTS

inv1 : $idleF \subseteq trans$
inv2 : $epr \subseteq trans$
inv3 : $epa \subseteq trans$
inv4 : $abortepv \subseteq trans$
inv5 : $abortepa \subseteq trans$
inv6 : $endF \subseteq trans$
inv7 : $idleT \subseteq trans$
inv8 : $epv \subseteq trans$
inv9 : $abortepv \subseteq trans$
inv10 : $endT \subseteq trans$

Invariants I

inv11 : $epr \subseteq idle$
inv12 : $epv \cap (epa \cup abortepa) \subseteq pending$
inv13 : $epa \cap (epv \cup abortepv) \subseteq pending$
inv14 : $epa \cap abortepa = \emptyset$
inv15 : $epv \cap abortepv = \emptyset$
inv16 : $abortepa \cap abortepv = recover$

Invariants II

inv17 : $idleF \subseteq idle$
inv18 : $idleT \cap (epa \cup abortepa) = \emptyset$
inv19 : $idleT \cap (epv \cup abortepv) = \emptyset$
inv20 : $pending \subseteq (epa \cup abortepa)$
inv21 : $endT \cap pending = \emptyset$
inv22 : $(epv \cup abortepv) \cap endT = \emptyset$

Invariants III

inv23 : $epr \cap idleF = \emptyset$

$\text{inv24} : \text{idleT} \cap \text{endT} = \emptyset$
 $\text{inv25} : \text{endT} \subseteq \text{ended}$
 $\text{inv26} : \text{abortepa} \cap \text{epv} = \emptyset$
 $\text{inv27} : \text{epa} \cap \text{epv} = \emptyset$
 $\text{inv28} : \text{idleF} \cap \text{epa} = \emptyset$
 $\text{inv29} : \text{idleF} \cap \text{abortepa} = \emptyset$

EVENTS

Initialisation

begin
 $\text{act1} : \text{purse} := \emptyset$
 $\text{act2} : \text{bal} := \emptyset$
 $\text{act3} : \text{trans} := \emptyset$
 $\text{act4} : \text{from} := \emptyset$
 $\text{act5} : \text{to} := \emptyset$
 $\text{act6} : \text{am} := \emptyset$
 $\text{act7} : \text{idleF} := \emptyset$
 $\text{act8} : \text{epv} := \emptyset$
 $\text{act9} : \text{epa} := \emptyset$
 $\text{act10} : \text{abortepv} := \emptyset$
 $\text{act11} : \text{abortepa} := \emptyset$
 $\text{act12} : \text{endF} := \emptyset$
 $\text{act13} : \text{idleT} := \emptyset$
 $\text{act14} : \text{epv} := \emptyset$
 $\text{act15} : \text{abortepv} := \emptyset$
 $\text{act16} : \text{endT} := \emptyset$

end

Event $\text{createPurse} \hat{=}$

refines createPurse

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

Event $\text{Start} \hat{=}$

refines Start

any
 t
 $p1$
 $p2$
 a
where
 $\text{grd1} : t \in \text{TRANS} \setminus \text{trans}$
 $\text{grd2} : p1 \in \text{purse}$
 $\text{grd3} : p2 \in \text{purse}$
 $\text{grd4} : a \in \mathbb{N}$
 $\text{grd5} : a > 0$
 $\text{grd6} : p1 \neq p2$
then
 $\text{act1} : \text{trans} := \text{trans} \cup \{t\}$

```

    act2 :  $from(t) := p1$ 
    act3 :  $to(t) := p2$ 
    act4 :  $am(t) := a$ 
    act5 :  $idleF := idleF \cup \{t\}$ 
    act6 :  $idleT := idleT \cup \{t\}$ 
  end
Event StartFrom  $\hat{=}$ 
  any
     $t$ 
     $p1$ 
  where
    grd1 :  $p1 \in purse$ 
    grd2 :  $t \in idleF$ 
    grd3 :  $p1 = from(t)$ 
  then
    act1 :  $epr := epr \cup \{t\}$ 
    act2 :  $idleF := idleF \setminus \{t\}$ 
  end
Event StartTo  $\hat{=}$ 
  any
     $t$ 
     $p2$ 
  where
    grd1 :  $p2 \in purse$ 
    grd2 :  $t \in idleT$ 
    grd3 :  $p2 = to(t)$ 
  then
    act1 :  $epv := epv \cup \{t\}$ 
    act2 :  $idleT := idleT \setminus \{t\}$ 
  end
Event Deduct  $\hat{=}$ 
refines Deduct
  any
     $t$ 
     $p1$ 
     $a$ 
  where
    grd1 :  $p1 \in purse$ 
    grd2 :  $t \in epr$ 
    grd3 :  $t \in (epv \cup abortepv)$ 
    grd4 :  $p1 = from(t)$ 
    grd5 :  $a \in \mathbb{N}$ 
    grd6 :  $a = am(t)$ 
    grd7 :  $a \leq bal(p1)$ 
  then
    act1 :  $epa := epa \cup \{t\}$ 
    act2 :  $epr := epr \setminus \{t\}$ 
    act3 :  $bal(p1) := bal(p1) - a$ 
  end
Event Increase  $\hat{=}$ 
refines Increase
  any
     $t$ 
     $p1$ 
     $p2$ 
     $a$ 

```

```

where
  grd1 :  $p1 \in \text{purse}$ 
  grd2 :  $p2 \in \text{purse}$ 
  grd3 :  $t \in \text{epv}$ 
  grd4 :  $t \in (\text{epa} \cup \text{abortepa})$ 
  grd5 :  $a \in \mathbb{N}$ 
  grd6 :  $\text{am}(t) = a$ 
  grd7 :  $\text{from}(t) = p1$ 
  grd8 :  $\text{to}(t) = p2$ 
then
  act1 :  $\text{bal}(p2) := \text{bal}(p2) + a$ 
  act2 :  $\text{endT} := \text{endT} \cup \{t\}$ 
  act3 :  $\text{epv} := \text{epv} \setminus \{t\}$ 
end
Event Abortepv1  $\hat{=}$ 
refines TransferFail
any
   $t$ 
where
  grd1 :  $t \in \text{epv}$ 
  grd2 :  $t \in \text{abortepa}$ 
then
  act1 :  $\text{abortepv} := \text{abortepv} \cup \{t\}$ 
  act2 :  $\text{epv} := \text{epv} \setminus \{t\}$ 
end
Event Abortepv2  $\hat{=}$ 
any
   $t$ 
where
  grd1 :  $t \in \text{epv}$ 
  grd2 :  $t \notin \text{abortepa}$ 
then
  act1 :  $\text{abortepv} := \text{abortepv} \cup \{t\}$ 
  act2 :  $\text{epv} := \text{epv} \setminus \{t\}$ 
end
Event Abortepa1  $\hat{=}$ 
refines TransferFail
any
   $t$ 
where
  grd1 :  $t \in \text{epa}$ 
  grd2 :  $t \in \text{abortepv}$ 
then
  act1 :  $\text{abortepa} := \text{abortepa} \cup \{t\}$ 
  act2 :  $\text{epa} := \text{epa} \setminus \{t\}$ 
end
Event Abortepa2  $\hat{=}$ 
any
   $t$ 
where
  grd1 :  $t \in \text{epa}$ 
  grd2 :  $t \notin \text{abortepv}$ 
then
  act1 :  $\text{abortepa} := \text{abortepa} \cup \{t\}$ 
  act2 :  $\text{epa} := \text{epa} \setminus \{t\}$ 
end

```

```

Event Abortepr  $\hat{=}$ 
  any
    t
  where
    grd1 :  $t \in epr$ 
  then
    act1 :  $abortepr := abortepr \cup \{t\}$ 
    act2 :  $epr := epr \setminus \{t\}$ 
  end
Event Recover  $\hat{=}$ 
refines Recover
  any
    t
    p1
    a
  where
    grd1 :  $p1 \in purse$ 
    grd2 :  $t \in abortepa$ 
    grd3 :  $t \in abortepv$ 
    grd4 :  $a \in \mathbb{N}$ 
    grd5 :  $a = am(t)$ 
    grd6 :  $from(t) = p1$ 
  then
    act1 :  $bal(p1) := bal(p1) + a$ 
    act2 :  $endF := endF \cup \{t\}$ 
    act3 :  $endT := endT \cup \{t\}$ 
    act4 :  $abortepa := abortepa \setminus \{t\}$ 
    act5 :  $abortepv := abortepv \setminus \{t\}$ 
  end
Event Ack  $\hat{=}$ 
  any
    t
  where
    grd1 :  $t \in epa$ 
    grd2 :  $t \in endT$ 
  then
    act1 :  $endF := endF \cup \{t\}$ 
    act2 :  $epa := epa \setminus \{t\}$ 
  end
END

```