

MACHINE m5

REFINES m4

SEES c2

VARIABLES

bal
purse
trans
from
to
am
idleF
epr
epa
abortepv
abortepa
endF
idleT
epv
abortepv
endT
startToM
startFromM
reqM
valM
ackM

INVARIANTS

inv1 : $startToM \subseteq trans$
inv2 : $startFromM \subseteq trans$
inv3 : $reqM \subseteq trans$
inv4 : $valM \subseteq trans$
inv5 : $ackM \subseteq trans$
inv8 : $epa \cap ackM \subseteq endT$
HR first iteration
inv6 : $epr \cap reqM \subseteq epv \cup abortepv$
inv7 : $epv \cap valM \subseteq epa \cup abortepa$
hrInv8 : $valM \cap idleF = \emptyset$
hrInv7 : $epr \cap valM = \emptyset$
hrInv4 : $valM \cap idleT = \emptyset$
hrInv9 : $abortepa \cap idleF = \emptyset$
hrInv3 : $reqM \cap idleF \subseteq epv \cup abortepv$
hrInv2 : $endT = endF \cup ackM$
HR second iteration
hrInv6 : $epr \cap abortepa = \emptyset$
HR third iteration

EVENTS

Initialisation

begin

```

    act1 :  $purse := \emptyset$ 
    act2 :  $bal := \emptyset$ 
    act3 :  $trans := \emptyset$ 
    act4 :  $from := \emptyset$ 
    act5 :  $to := \emptyset$ 
    act6 :  $am := \emptyset$ 
    act7 :  $idleF := \emptyset$ 
    act8 :  $epr := \emptyset$ 
    act9 :  $epa := \emptyset$ 
    act10 :  $abortepr := \emptyset$ 
    act11 :  $abortepa := \emptyset$ 
    act12 :  $endF := \emptyset$ 
    act13 :  $idleT := \emptyset$ 
    act14 :  $epv := \emptyset$ 
    act15 :  $abortepv := \emptyset$ 
    act16 :  $endT := \emptyset$ 
    act17 :  $startToM := \emptyset$ 
    act18 :  $startFromM := \emptyset$ 
    act19 :  $reqM := \emptyset$ 
    act20 :  $valM := \emptyset$ 
    act21 :  $ackM := \emptyset$ 
  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 :  $idleF := idleF \cup \{t\}$ 
    act6 :  $idleT := idleT \cup \{t\}$ 
  
```

```

    act7 : startFromM := startFromM  $\cup$  {t}
    act8 : startToM := startToM  $\cup$  {t}
  end
Event StartFrom  $\hat{=}$ 
refines StartFrom
  any
    t
    p1
  where
    grd1 : p1  $\in$  purse
    grd2 : t  $\in$  idleF
    grd3 : p1 = from(t)
    grd4 : t  $\in$  startFromM
  then
    act1 : epr := epr  $\cup$  {t}
    act2 : idleF := idleF  $\setminus$  {t}
  end
Event StartTo  $\hat{=}$ 
refines StartTo
  any
    t
    p2
  where
    grd1 : p2  $\in$  purse
    grd2 : t  $\in$  idleT
    grd3 : p2 = to(t)
    grd4 : t  $\in$  startToM
  then
    act1 : epv := epv  $\cup$  {t}
    act2 : idleT := idleT  $\setminus$  {t}
    act3 : reqM := reqM  $\cup$  {t}
  end
Event Deduct  $\hat{=}$ 
refines Deduct
  any
    t
    p1
    a
  where
    grd1 : p1  $\in$  purse
    grd2 : t  $\in$  epr
    grd3 : t  $\in$  reqM
    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
    act4 : valM := valM  $\cup$  {t}
  end
Event Increase  $\hat{=}$ 
refines Increase
  any
    t

```

```

    p1
    p2
    a
  where
    grd1 : p1 ∈ purse
    grd2 : p2 ∈ purse
    grd3 : t ∈ epv
    grd4 : t ∈ valM
    grd5 : a ∈ ℕ
    grd6 : am(t) = a
    grd7 : from(t) = p1
    grd8 : to(t) = p2
  then
    act1 : bal(p2) := bal(p2) + a
    act2 : endT := endT ∪ {t}
    act3 : epv := epv \ {t}
    act4 : ackM := ackM ∪ {t}
  end
Event Abortepv ≐
refines Abortepv1, Abortepv2
  any
    t
  where
    grd1 : t ∈ epv
  then
    act1 : abortepv := abortepv ∪ {t}
    act2 : epv := epv \ {t}
  end
Event Abortepa ≐
refines Abortepa1, Abortepa2
  any
    t
  where
    grd1 : t ∈ epa
  then
    act1 : abortepa := abortepa ∪ {t}
    act2 : epa := epa \ {t}
  end
Event Abortepv ≐
refines Abortepv
  any
    t
  where
    grd1 : t ∈ epr
  then
    act1 : abortepv := abortepv ∪ {t}
    act2 : epr := epr \ {t}
  end
Event Recover ≐
refines Recover
  any
    t
    p1
    a
  where
    grd1 : p1 ∈ 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  $Ack \hat{=}$ 
refines  $Ack$ 
  any
     $t$ 
  where
    grd1 :  $t \in epa$ 
    grd2 :  $t \in ackM$ 
  then
    act1 :  $endF := endF \cup \{t\}$ 
    act2 :  $epa := epa \setminus \{t\}$ 
  end
END

```