

MACHINE m6

REFINES m5

SEES c2

VARIABLES

bal
purse
trans
from
to
am
startToM
startFromM
reqM
valM
ackM
idleFP
eprP
epaP
abortepP
abortepaP
endFP
idleTP
epvP
abortepvP
endTP
currentF
currentT
active

INVARIANTS

inv1 : $currentF \in \text{purse} \leftrightarrow \text{trans}$
inv2 : $currentT \in \text{purse} \leftrightarrow \text{trans}$
inv3 : $active \subseteq \text{purse}$
inv4 : $idleFP \subseteq \text{purse}$
inv5 : $eprP \subseteq \text{purse}$
inv6 : $epaP \subseteq \text{purse}$
inv7 : $abortepP \subseteq \text{purse}$
inv8 : $abortepaP \subseteq \text{purse}$
inv9 : $endFP \subseteq \text{purse}$
inv10 : $idleTP \subseteq \text{purse}$
inv11 : $epvP \subseteq \text{purse}$
inv12 : $abortepvP \subseteq \text{purse}$
inv13 : $endTP \subseteq \text{purse}$
inv14 : $currentF[idleFP] \subseteq idleF$
inv15 : $currentF[eprP] \subseteq epr$
inv16 : $currentF[epaP] \subseteq epa$
inv17 : $currentF[abortepP] \subseteq abortep$
inv18 : $currentF[abortepaP] \subseteq abortepa$

$\text{inv19} : \text{currentF}[\text{endFP}] \subseteq \text{endF}$
 $\text{inv20} : \text{currentT}[\text{idleTP}] \subseteq \text{idleT}$
 $\text{inv21} : \text{currentT}[\text{epvP}] \subseteq \text{epv}$
 $\text{inv22} : \text{currentT}[\text{abortepvP}] \subseteq \text{abortepv}$
 $\text{inv23} : \text{currentT}[\text{endTP}] \subseteq \text{endT}$
 $\text{inv73} : (\text{idleFP} \cup \text{epvP} \cup \text{epaP} \cup \text{abortepvP} \cup \text{abortepaP} \cup \text{endFP} \cup \text{idleTP} \cup \text{epvP} \cup \text{abortepvP} \cup \text{endTP}) \subseteq \text{active}$

EVENTS

Initialisation

begin

$\text{act1} : \text{purse} := \emptyset$
 $\text{act2} : \text{bal} := \emptyset$
 $\text{act3} : \text{trans} := \emptyset$
 $\text{act4} : \text{from} := \emptyset$
 $\text{act5} : \text{to} := \emptyset$
 $\text{act6} : \text{am} := \emptyset$
 $\text{act7} : \text{idleFP} := \emptyset$
 $\text{act8} : \text{epvP} := \emptyset$
 $\text{act9} : \text{epaP} := \emptyset$
 $\text{act10} : \text{abortepvP} := \emptyset$
 $\text{act11} : \text{abortepaP} := \emptyset$
 $\text{act12} : \text{endFP} := \emptyset$
 $\text{act13} : \text{idleTP} := \emptyset$
 $\text{act14} : \text{epvP} := \emptyset$
 $\text{act15} : \text{abortepvP} := \emptyset$
 $\text{act16} : \text{endTP} := \emptyset$
 $\text{act17} : \text{startToM} := \emptyset$
 $\text{act18} : \text{startFromM} := \emptyset$
 $\text{act19} : \text{reqM} := \emptyset$
 $\text{act20} : \text{valM} := \emptyset$
 $\text{act21} : \text{ackM} := \emptyset$
 $\text{act22} : \text{currentF} := \emptyset$
 $\text{act23} : \text{currentT} := \emptyset$
 $\text{act24} : \text{active} := \emptyset$

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
  grd1 :  $t \in TRANS \setminus trans$ 
  grd2 :  $p1 \in purse \setminus active$ 
  grd3 :  $p2 \in purse \setminus active$ 
  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 :  $idleFP := idleFP \cup \{p1\}$ 
  act6 :  $idleTP := idleTP \cup \{p2\}$ 
  act7 :  $startFromM := startFromM \cup \{t\}$ 
  act8 :  $startToM := startToM \cup \{t\}$ 
  act9 :  $active := active \cup \{p1\} \cup \{p2\}$ 
  act10 :  $currentF(p1) := t$ 
  act11 :  $currentT(p2) := t$ 
end
Event  $StartFrom \hat{=}$ 
refines  $StartFrom$ 
any
   $t$ 
   $p1$ 
where
  grd1 :  $p1 \in idleFP$ 
  grd2 :  $t \in startFromM$ 
  grd3 :  $p1 \mapsto t \in currentF$ 
  grd4 :  $p1 = from(t)$ 
then
  act1 :  $eprP := eprP \cup \{p1\}$ 
  act2 :  $idleFP := idleFP \setminus \{p1\}$ 
end
Event  $StartTo \hat{=}$ 
refines  $StartTo$ 
any
   $t$ 
   $p2$ 
where
  grd1 :  $p2 \in idleTP$ 
  grd2 :  $t \in startToM$ 
  grd3 :  $p2 \mapsto t \in currentT$ 
  grd4 :  $p2 = to(t)$ 
then
  act1 :  $epvP := epvP \cup \{p2\}$ 
  act2 :  $idleTP := idleTP \setminus \{p2\}$ 
  act3 :  $reqM := reqM \cup \{t\}$ 
end
Event  $Deduct \hat{=}$ 
refines  $Deduct$ 
any
   $t$ 
   $p1$ 
   $a$ 
where

```

```

    grd1 :  $p1 \in eprP$ 
    grd3 :  $t \in reqM$ 
    grd4 :  $p1 = from(t)$ 
    grd5 :  $p1 \mapsto t \in currentF$ 
    grd6 :  $a \in \mathbb{N}$ 
    grd7 :  $a = am(t)$ 
    grd8 :  $a \leq bal(p1)$ 
  then
    act1 :  $epaP := epaP \cup \{p1\}$ 
    act2 :  $eprP := eprP \setminus \{p1\}$ 
    act3 :  $bal(p1) := bal(p1) - a$ 
    act4 :  $valM := valM \cup \{t\}$ 
  end
Event Increase  $\hat{=}$ 
refines Increase
  any
     $t$ 
     $p1$ 
     $p2$ 
     $a$ 
  where
    grd1 :  $p1 \in purse$ 
    grd2 :  $p2 \in epvP$ 
    grd3 :  $t \in valM$ 
    grd4 :  $a \in \mathbb{N}$ 
    grd5 :  $am(t) = a$ 
    grd6 :  $from(t) = p1$ 
    grd7 :  $to(t) = p2$ 
    grd8 :  $p2 \mapsto t \in currentT$ 
  then
    act1 :  $bal(p2) := bal(p2) + a$ 
    act2 :  $endTP := endTP \cup \{p2\}$ 
    act3 :  $epvP := epvP \setminus \{p2\}$ 
    act4 :  $ackM := ackM \cup \{t\}$ 
  end
Event Abortepv  $\hat{=}$ 
refines Abortepv
  any
     $p2$ 
  where
    grd1 :  $p2 \in epvP$ 
  with
     $t : t = currentT(p2) \wedge p2 \in dom(currentT)$ 
  then
    act1 :  $abortepvP := abortepvP \cup \{p2\}$ 
    act2 :  $epvP := epvP \setminus \{p2\}$ 
  end
Event Abortepa  $\hat{=}$ 
refines Abortepa
  any
     $p1$ 
  where
    grd1 :  $p1 \in epaP$ 
  with
     $t : t = currentF(p1) \wedge p1 \in dom(currentF)$ 
  then

```

```

    act1: abortepaP := abortepaP  $\cup$  {p1}
    act2: epaP := epaP  $\setminus$  {p1}
end
Event Abortepr  $\hat{=}$ 
refines Abortepr
  any
    p1
  where
    grd1: p1  $\in$  eprP
  with
    t: t = currentF(p1)  $\wedge$  p1  $\in$  dom(currentF)
  then
    act1: aborteprP := aborteprP  $\cup$  {p1}
    act2: eprP := eprP  $\setminus$  {p1}
  end
Event Recover  $\hat{=}$ 
refines Recover
  any
    t
    p1
    p2
    a
  where
    grd1: p1  $\in$  abortepaP
    grd2: p2  $\in$  abortepvP
    grd6: p1  $\mapsto$  t  $\in$  currentF
    grd7: p2  $\mapsto$  t  $\in$  currentT
    grd3: a  $\in$   $\mathbb{N}$ 
    grd4: a = am(t)
    grd5: from(t) = p1
  then
    act1: bal(p1) := bal(p1) + a
    act2: endFP := endFP  $\cup$  {p1}
    act3: endTP := endTP  $\cup$  {p2}
    act4: abortepaP := abortepaP  $\setminus$  {p1}
    act5: abortepvP := abortepvP  $\setminus$  {p2}
  end
Event Ack  $\hat{=}$ 
refines Ack
  any
    t
    p1
  where
    grd1: p1  $\in$  epaP
    grd2: t  $\in$  ackM
    grd3: p1  $\mapsto$  t  $\in$  currentF
  then
    act1: endFP := endFP  $\cup$  {p1}
    act2: epaP := epaP  $\setminus$  {p1}
  end
Event endTrans1  $\hat{=}$ 
  any
    t
    p1
    p2
  where

```

```

    grd1 :  $p1 \in abortepvP$ 
    grd2 :  $p2 \in abortepvP$ 
    grd3 :  $p1 \mapsto t \in currentF$ 
    grd4 :  $p2 \mapsto t \in currentT$ 
    grd5 :  $from(t) = p1$ 
    grd6 :  $to(t) = p2$ 
  then
    act1 :  $abortepvP := abortepvP \setminus \{p1\}$ 
    act2 :  $abortepvP := abortepvP \setminus \{p2\}$ 
    act3 :  $currentF := \{p1\} \triangleleft currentF$ 
    act4 :  $currentT := \{p2\} \triangleleft currentT$ 
    act5 :  $active := (active \setminus \{p1\}) \setminus \{p2\}$ 
  end
Event  $endTrans2 \triangleq$ 
  any
     $t$ 
     $p1$ 
     $p2$ 
  where
    grd1 :  $p1 \in endFP$ 
    grd2 :  $p2 \in endTP$ 
    grd3 :  $p1 \mapsto t \in currentF$ 
    grd4 :  $p2 \mapsto t \in currentT$ 
    grd5 :  $from(t) = p1$ 
    grd6 :  $to(t) = p2$ 
  then
    act1 :  $endFP := endFP \setminus \{p1\}$ 
    act2 :  $endTP := endTP \setminus \{p2\}$ 
    act3 :  $currentF := \{p1\} \triangleleft currentF$ 
    act4 :  $currentT := \{p2\} \triangleleft currentT$ 
    act5 :  $active := (active \setminus \{p1\}) \setminus \{p2\}$ 
  end
END

```