

MACHINE m9

REFINES m8

SEES c4

VARIABLES

bal
purse
from
to
am
startToM
startFromM
reqM
valM
ackM
active
currentF2
currentT2
currentSeqNo
statusF
statusT
Fseqno
Tseqno

INVARIANTS

inv1 : $statusF \in \text{purse} \leftrightarrow status$
inv2 : $statusT \in \text{purse} \leftrightarrow status$
inv3 : $idleFP = statusF^{-1}[\{IDLEF\}]$
inv4 : $eprP = statusF^{-1}[\{EPR\}]$
inv5 : $epaP = statusF^{-1}[\{EPA\}]$
inv6 : $abortepP = statusF^{-1}[\{ABORTEPR\}]$
inv7 : $abortepaP = statusF^{-1}[\{ABORTEPA\}]$
inv8 : $endFP = statusF^{-1}[\{ENDF\}]$
inv9 : $idleTP = statusT^{-1}[\{IDLET\}]$
inv10 : $epvP = statusT^{-1}[\{EPV\}]$
inv11 : $abortepvP = statusT^{-1}[\{ABORTEPV\}]$
inv12 : $endTP = statusT^{-1}[\{ENDT\}]$

EVENTS

Initialisation

begin

act1 : $\text{purse} := \emptyset$
act2 : $\text{bal} := \emptyset$
act4 : $\text{from} := \emptyset$
act5 : $\text{to} := \emptyset$
act6 : $\text{am} := \emptyset$
act7 : $\text{startToM} := \emptyset$
act8 : $\text{startFromM} := \emptyset$
act9 : $\text{reqM} := \emptyset$
act10 : $\text{valM} := \emptyset$
act11 : $\text{ackM} := \emptyset$

```

    act12: currentF2 :=  $\emptyset$ 
    act13: currentT2 :=  $\emptyset$ 
    act14: active :=  $\emptyset$ 
    act15: currentSeqNo :=  $\emptyset$ 
    act17: statusF :=  $\emptyset$ 
    act18: statusT :=  $\emptyset$ 
    act29: Fseqno :=  $TRANS \times \{0\}$ 
    act30: Tseqno :=  $TRANS \times \{0\}$ 
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:  $bal(p) := a$ 
    act3:  $currentSeqNo(p) := 0$ 
  end
Event Start  $\hat{=}$ 
refines Start
  any
    t
    p1
    p2
    a
    n1
    n2
  where
    grd1:  $t \in TRANS$ 
    grd2:  $p1 \in purse \setminus active$ 
    grd3:  $p2 \in purse \setminus active$ 
    grd4:  $a \in \mathbb{N}$ 
    grd5:  $a > 0$ 
    grd6:  $p1 \neq p2$ 
    grd7:  $n1 \in \mathbb{N}$ 
    grd8:  $n2 \in \mathbb{N}$ 
    grd9:  $n1 = Fseqno(t)$ 
    grd10:  $n2 = Tseqno(t)$ 
    grd11:  $n1 > currentSeqNo(p1)$ 
    grd12:  $n2 > currentSeqNo(p2)$ 
  then
    act1:  $from(t) := p1$ 
    act2:  $to(t) := p2$ 
    act3:  $am(t) := a$ 
    act4:  $statusF(p1) := IDLEF$ 
    act5:  $statusT(p2) := IDLET$ 
    act6:  $startFromM := startFromM \cup \{t\}$ 
    act7:  $startToM := startToM \cup \{t\}$ 
    act8:  $active := active \cup \{p1\} \cup \{p2\}$ 
    act9:  $currentSeqNo := \{p1 \mapsto n1\} \cup \{p2 \mapsto n2\} \cup (\{p1, p2\} \triangleleft currentSeqNo)$ 
  end

```

Event *StartFrom* $\hat{=}$

refines *StartFrom*

any

t

p1

where

grd2 : $t \in startFromM$

grd4 : $t \mapsto p1 \in from$

grd3 : $Fseqno(t) = currentSeqNo(p1)$

grd1 : $p1 \mapsto IDLEF \in statusF$

then

act1 : $statusF(p1) := EPR$

act2 : $currentF2(p1) := t$

end

Event *StartTo* $\hat{=}$

refines *StartTo*

any

t

p2

where

grd2 : $t \in startToM$

grd4 : $t \mapsto p2 \in to$

grd3 : $Tseqno(t) = currentSeqNo(p2)$

grd1 : $p2 \mapsto IDLET \in statusT$

then

act1 : $statusT(p2) := EPV$

act2 : $reqM := reqM \cup \{t\}$

act3 : $currentT2(p2) := t$

end

Event *Deduct* $\hat{=}$

refines *Deduct*

any

t

p1

a

where

grd3 : $t \in reqM$

grd4 : $t \mapsto p1 \in from$

grd5 : $p1 \mapsto t \in currentF2$

grd6 : $a \in \mathbb{N}$

grd7 : $t \mapsto a \in am$

grd8 : $a \leq bal(p1)$

grd1 : $p1 \mapsto EPR \in statusF$

then

act1 : $statusF(p1) := EPA$

act2 : $bal(p1) := bal(p1) - a$

act3 : $valM := valM \cup \{t\}$

end

Event *Increase* $\hat{=}$

refines *Increase*

any

t

p1

p2

a

where

```

    grd1 :  $p1 \in \text{purse}$ 
    grd3 :  $t \in \text{val}M$ 
    grd4 :  $a \in \mathbb{N}$ 
    grd5 :  $t \mapsto a \in \text{am}$ 
    grd6 :  $t \mapsto p1 \in \text{from}$ 
    grd7 :  $t \mapsto p2 \in \text{to}$ 
    grd8 :  $p2 \mapsto t \in \text{current}T2$ 
    grd2 :  $p2 \mapsto \text{EPV} \in \text{status}T$ 
  then
    act1 :  $\text{bal}(p2) := \text{bal}(p2) + a$ 
    act2 :  $\text{status}T(p2) := \text{ENDT}$ 
    act3 :  $\text{ack}M := \text{ack}M \cup \{t\}$ 
  end
Event Abortepv  $\hat{=}$ 
refines Abortepv
  any
     $p2$ 
  where
    grd1 :  $p2 \in \text{ran}(\text{to})$ 
    grd2 :  $p2 \mapsto \text{EPV} \in \text{status}T$ 
  then
    act1 :  $\text{status}T(p2) := \text{ABORTEPV}$ 
  end
Event Abortepa  $\hat{=}$ 
refines Abortepa
  any
     $p1$ 
  where
    grd1 :  $p1 \in \text{ran}(\text{from})$ 
    grd2 :  $p1 \mapsto \text{EPA} \in \text{status}F$ 
  then
    act1 :  $\text{status}F(p1) := \text{ABORTEPA}$ 
  end
Event Abortepv  $\hat{=}$ 
refines Abortepv
  any
     $p1$ 
  where
    grd1 :  $p1 \in \text{ran}(\text{from})$ 
    grd2 :  $p1 \mapsto \text{EPR} \in \text{status}F$ 
  then
    act1 :  $\text{status}F(p1) := \text{ABORTEPR}$ 
  end
Event Recover  $\hat{=}$ 
refines Recover
  any
     $t$ 
     $p1$ 
     $p2$ 
     $a$ 
  where
    grd7 :  $p2 \mapsto t \in \text{current}T2$ 
    grd6 :  $p1 \mapsto t \in \text{current}F2$ 
    grd3 :  $a \in \mathbb{N}$ 
    grd4 :  $t \mapsto a \in \text{am}$ 
    grd5 :  $t \mapsto p1 \in \text{from}$ 

```

```

    grd8 :  $t \mapsto p2 \in to$ 
    grd1 :  $p1 \mapsto ABORTEPA \in statusF$ 
    grd2 :  $p2 \mapsto ABORTEPV \in statusT$ 
  then
    act1 :  $bal(p1) := bal(p1) + a$ 
    act2 :  $statusF(p1) := ENDF$ 
    act3 :  $statusT(p2) := ENDT$ 
  end
Event Ack  $\triangleq$ 
refines Ack
  any
     $t$ 
     $p1$ 
  where
    grd2 :  $t \in ackM$ 
    grd3 :  $p1 \mapsto t \in currentF2$ 
    grd4 :  $p1 \in ran(from)$ 
    grd1 :  $p1 \mapsto EPA \in statusF$ 
  then
    act1 :  $statusF(p1) := ENDF$ 
  end
Event endTrans1  $\triangleq$ 
refines endTrans1
  any
     $t$ 
     $p1$ 
     $p2$ 
  where
    grd1 :  $p1 \mapsto ABORTEPR \in statusF$ 
    grd2 :  $p2 \mapsto ABORTEPV \in statusT$ 
    grd3 :  $p1 \mapsto t \in currentF2$ 
    grd4 :  $p2 \mapsto t \in currentT2$ 
    grd5 :  $t \mapsto p1 \in from$ 
    grd6 :  $t \mapsto p2 \in to$ 
  then
    act1 :  $statusF := statusF \setminus \{p1 \mapsto ABORTEPR\}$ 
    act2 :  $statusT := statusT \setminus \{p2 \mapsto ABORTEPV\}$ 
    act3 :  $currentF2 := \{p1\} \triangleleft currentF2$ 
    act4 :  $currentT2 := \{p2\} \triangleleft currentT2$ 
    act5 :  $active := (active \setminus \{p1\}) \setminus \{p2\}$ 
  end
Event endTrans2  $\triangleq$ 
refines endTrans2
  any
     $t$ 
     $p1$ 
     $p2$ 
  where
    grd1 :  $p1 \mapsto ENDF \in statusF$ 
    grd2 :  $p2 \mapsto ENDT \in statusT$ 
    grd3 :  $p1 \mapsto t \in currentF2$ 
    grd4 :  $p2 \mapsto t \in currentT2$ 
    grd5 :  $t \mapsto p1 \in from$ 
    grd6 :  $t \mapsto p2 \in to$ 
  then
    act1 :  $statusF := statusF \setminus \{p1 \mapsto ENDF\}$ 

```

```
act2:  $statusT := statusT \setminus \{p2 \mapsto ENDT\}$ 
act3:  $currentF2 := \{p1\} \triangleleft currentF2$ 
act4:  $currentT2 := \{p2\} \triangleleft currentT2$ 
act5:  $active := (active \setminus \{p1\}) \setminus \{p2\}$ 
end
END
```