

**MACHINE** m8

**REFINES** m7v2

**SEES** c2

**VARIABLES**

bal  
purse  
from  
to  
am  
startToM  
startFromM  
reqM  
valM  
ackM  
active  
idleFP  
eprP  
epaP  
aborteprP  
abortepaP  
endFP  
idleTP  
epvP  
aborteprvP  
endTP  
currentF2  
currentT2  
currentSeqNo  
Fseqno  
Tseqno

**INVARIANTS**

*inv2* :  $\forall p, n. (p \mapsto n \in \text{used} \Rightarrow n \leq \text{currentSeqNo}(p))$

**EVENTS**

**Initialisation**

**begin**

*act1* :  $\text{purse} := \emptyset$   
*act2* :  $\text{bal} := \emptyset$   
*act4* :  $\text{from} := \emptyset$   
*act5* :  $\text{to} := \emptyset$   
*act6* :  $\text{am} := \emptyset$   
*act7* :  $\text{idleFP} := \emptyset$   
*act8* :  $\text{eprP} := \emptyset$   
*act9* :  $\text{epaP} := \emptyset$   
*act10* :  $\text{aborteprP} := \emptyset$   
*act11* :  $\text{abortepaP} := \emptyset$   
*act12* :  $\text{endFP} := \emptyset$   
*act13* :  $\text{idleTP} := \emptyset$   
*act14* :  $\text{epvP} := \emptyset$

```

    act15 : abortepvP :=  $\emptyset$ 
    act16 : endTP :=  $\emptyset$ 
    act17 : startToM :=  $\emptyset$ 
    act18 : startFromM :=  $\emptyset$ 
    act19 : reqM :=  $\emptyset$ 
    act20 : valM :=  $\emptyset$ 
    act21 : ackM :=  $\emptyset$ 
    act22 : currentF2 :=  $\emptyset$ 
    act23 : currentT2 :=  $\emptyset$ 
    act24 : active :=  $\emptyset$ 
    act25 : currentSeqNo :=  $\emptyset$ 
    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 :  $idleFP := idleFP \cup \{p1\}$ 
    act5 :  $idleTP := idleTP \cup \{p2\}$ 

```

```

    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
    grd1 : p1  $\in$  idleFP
    grd2 : t  $\in$  startFromM
    grd3 : Fseqno(t) = currentSeqNo(p1)
    grd4 : p1 = from(t)
  then
    act1 : eprP := eprP  $\cup$  {p1}
    act2 : idleFP := idleFP  $\setminus$  {p1}
    act3 : currentF2(p1) := t
  end
Event StartTo  $\hat{=}$ 
refines StartTo
  any
    t
    p2
  where
    grd1 : p2  $\in$  idleTP
    grd2 : t  $\in$  startToM
    grd3 : Tseqno(t) = currentSeqNo(p2)
    grd4 : p2 = to(t)
  then
    act1 : epvP := epvP  $\cup$  {p2}
    act2 : idleTP := idleTP  $\setminus$  {p2}
    act3 : reqM := reqM  $\cup$  {t}
    act4 : currentT2(p2) := 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  $\in$  currentF2
    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*  $\in$  *currentT2*

**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*

**then**

*act1* : *abortepvP* := *abortepvP*  $\cup$  {*p2*}

*act2* : *epvP* := *epvP*  $\setminus$  {*p2*}

**end**

**Event** *Abortepa*  $\hat{=}$

**refines** *Abortepa*

**any**

*p1*

**where**

*grd1* : *p1*  $\in$  *epaP*

**then**

*act1* : *abortepaP* := *abortepaP*  $\cup$  {*p1*}

*act2* : *epaP* := *epaP*  $\setminus$  {*p1*}

**end**

**Event** *Abortepv*  $\hat{=}$

**refines** *Abortepv*

**any**

*p1*

**where**

*grd1* : *p1*  $\in$  *eprP*

**then**

*act1* : *abortepvP* := *abortepvP*  $\cup$  {*p1*}

*act2* : *eprP* := *eprP*  $\setminus$  {*p1*}

**end**

**Event** *Recover*  $\hat{=}$

**refines** *Recover*

**any**

```

    t
    p1
    p2
    a
  where
    grd1 :  $p1 \in abortepaP$ 
    grd2 :  $p2 \in abortepvP$ 
    grd7 :  $p2 \mapsto t \in currentT2$ 
    grd6 :  $p1 \mapsto t \in currentF2$ 
    grd3 :  $a \in \mathbb{N}$ 
    grd5 :  $t \mapsto p1 \in from$ 
    grd4 :  $t \mapsto a \in am$ 
  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  $Ack \triangleq$ 
refines  $Ack$ 
  any
    t
    p1
  where
    grd1 :  $p1 \in epaP$ 
    grd2 :  $t \in ackM$ 
    grd3 :  $p1 \mapsto t \in currentF2$ 
  then
    act1 :  $endFP := endFP \cup \{p1\}$ 
    act2 :  $epaP := epaP \setminus \{p1\}$ 
  end
Event  $endTrans1 \triangleq$ 
refines  $endTrans1$ 
  any
    t
    p1
    p2
  where
    grd1 :  $p1 \in aborteprP$ 
    grd2 :  $p2 \in abortepvP$ 
    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 :  $aborteprP := aborteprP \setminus \{p1\}$ 
    act2 :  $abortepvP := abortepvP \setminus \{p2\}$ 
    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 ∈ endFP
    grd2 : p2 ∈ endTP
    grd3 : p1 ↦ t ∈ currentF2
    grd4 : p2 ↦ t ∈ currentT2
    grd5 : t ↦ p1 ∈ from
    grd6 : t ↦ p2 ∈ to
  then
    act1 : endFP := endFP \ {p1}
    act2 : endTP := endTP \ {p2}
    act3 : currentF2 := {p1} ◁ currentF2
    act4 : currentT2 := {p2} ◁ currentT2
    act5 : active := (active \ {p1}) \ {p2}
  end
END

```