

MACHINE m0

REFINES

c0

SEES c0

VARIABLES

r

p1

p2

INVARIANTS

inv1: false<theorem> $r \in SEMAPHORE$

inv2: false<theorem> $p1 \in SEMAPHORE$

inv3: false<theorem> $p2 \in SEMAPHORE$

inv4: false<theorem> $r = locked(p1 = locked \vee p2 = locked) \wedge \neg(p1 = locked \wedge p2 = locked)$

inv5: false<theorem> $\neg(p1 = locked \wedge p2 = locked)$

EVENTS

Initialisation true<extended>

false**thenbegin**

act1: truerunlockedrunlocked

act2: truep1unlockedp1unlocked

act3: truep2unlockedp2unlocked

end

Event P1_request <ordinary>

false**extendsrefines**

false**wherewhen**

grd1: false<theorem> $truer = unlockedr = unlocked$

grd2: false<theorem> $truep1 = unlockedp1 = unlocked$

grd3: false<theorem> $truep2 = unlockedp2 = unlocked$

true**thenbegin**

act1: truerlockedrlocked

act2: truep1lockedp1locked

end

Event P1_process <ordinary>

false**extendsrefines**

false**wherewhen**

grd1: false<theorem> $truer = lockedr = locked$

grd2: false<theorem> $truep1 = lockedp1 = locked$

true**thenbegin**

act1: truerunlockedrunlocked

act2: truep1unlockedp1unlocked

end

Event P2_request <ordinary>

false**extendsrefines**

false**wherewhen**

grd1: false<theorem> $truer = unlockedr = unlocked$

grd2: false<theorem> $truep2 = unlockedp2 = unlocked$

grd3: false<theorem> $truep1 = unlockedp1 = unlocked$

true**thenbegin**

act1: truerlockedrlocked

act2: truep2lockedp2locked

end

Event P2_process <ordinary>

false**extendsrefines**

false**wherewhen**

grd1: false<theorem> $truer = lockedr = locked$

grd2: false<theorem> $truep2 = lockedp2 = locked$

true**thenbegin**

act1: truerunlockedrunlocked

```
    act2: true

p2unlockedp2unlocked

end  
END
```