

```

1  ┌────────────────────────── MODULE RaceConditionLock ───────────────────────────┐
2  EXTENDS Naturals
3  CONSTANT N

6  --algorithm RaceConditionLock
7  variables total = 0, lock_free = TRUE ;

9  process Proc ∈ 1 .. N
10 variable x
11 begin
12   lock: await lock_free = TRUE ;
13       lock_free := FALSE ;
14   read: x := total ;
15   inc: x := x + 1 ;
16   save: total := x ;
17   unlock: lock_free := TRUE ;
18 end process ;

20 end algorithm ;
22 BEGIN TRANSLATION
23 CONSTANT defaultInitValue
24 VARIABLES total, lock_free, pc, x
26 vars ≜ ⟨total, lock_free, pc, x⟩
28 ProcSet ≜ (1 .. N)
30 Init ≜ Global variables
31   ∧ total = 0
32   ∧ lock_free = TRUE
33   Process Proc
34   ∧ x = [self ∈ 1 .. N ↦ defaultInitValue]
35   ∧ pc = [self ∈ ProcSet ↦ "lock"]

37 lock(self) ≜ ∧ pc[self] = "lock"
38                ∧ lock_free = TRUE
39                ∧ lock_free' = FALSE
40                ∧ pc' = [pc EXCEPT ![self] = "read"]
41                ∧ UNCHANGED ⟨total, x⟩

43 read(self) ≜ ∧ pc[self] = "read"
44                ∧ x' = [x EXCEPT ![self] = total]
45                ∧ pc' = [pc EXCEPT ![self] = "inc"]
46                ∧ UNCHANGED ⟨total, lock_free⟩

48 inc(self) ≜ ∧ pc[self] = "inc"
49                ∧ x' = [x EXCEPT ![self] = x[self] + 1]
50                ∧ pc' = [pc EXCEPT ![self] = "save"]

```

```

51           $\wedge$  UNCHANGED  $\langle total, lock\_free \rangle$ 
53   $save(self) \triangleq$   $\wedge pc[self] = \text{"save"}$ 
54           $\wedge total' = x[self]$ 
55           $\wedge pc' = [pc \text{ EXCEPT } ![self] = \text{"unlock"}]$ 
56           $\wedge$  UNCHANGED  $\langle lock\_free, x \rangle$ 
58   $unlock(self) \triangleq$   $\wedge pc[self] = \text{"unlock"}$ 
59           $\wedge lock\_free' = \text{TRUE}$ 
60           $\wedge pc' = [pc \text{ EXCEPT } ![self] = \text{"Done"}]$ 
61           $\wedge$  UNCHANGED  $\langle total, x \rangle$ 
63   $Proc(self) \triangleq$   $lock(self) \vee read(self) \vee inc(self) \vee save(self)$ 
64           $\vee unlock(self)$ 
66   $Next \triangleq$   $(\exists self \in 1 \dots N : Proc(self))$ 
67           $\vee$  Disjunct to prevent deadlock on termination
68           $((\forall self \in ProcSet : pc[self] = \text{"Done"}) \wedge \text{UNCHANGED } vars)$ 
70   $Spec \triangleq$   $Init \wedge \square [Next]_{vars}$ 
72   $Termination \triangleq$   $\diamond (\forall self \in ProcSet : pc[self] = \text{"Done"})$ 
74  END TRANSLATION
76   $AlgoOK \triangleq$   $(\forall self \in ProcSet : pc[self] = \text{"Done"}) \Rightarrow total = N$ 
78  |-----|
    \ * Modification History
    \ * Last modified Thu Nov 30 18:49:37 PST 2017 by satya
    \ * Created Thu Nov 30 18:44:41 PST 2017 by satya

```