```
──────────────────── MODULE Fischer1MC ────────────────────
 Fischer1.tla modified to be model checked.
 − EXTENDS  FischerPreface: replaced by EXTENDS  FischerPrefaceMC
 − Tick: increase now by 1
 − Liveness: replace "∀ r ∈ Real : ◇(now > r)" by "SF_vars(Tick)"
EXTENDS FischerPrefaceMC
───────────────────────────────────────────────────────────
SetTimer(t, timer, tau) ≜
    timer′ = [timer EXCEPT ![t] = tau]

ResetUBTimer(t, timer) ≜
    SetTimer(t, timer, Infinity)
───────────────────────────────────────────────────────────
NCS(t) ≜
      ∧ GoFromTo(t, "ncs", "a")
      ∧ UNCHANGED ⟨x, now, lbTimer, ubTimer, counter⟩

StmtA(t) ≜
    ∧ x = NotAThread
    ∧ GoFromTo(t, "a", "b")
    ∧ SetTimer(t, ubTimer, Delta)
    ∧ UNCHANGED ⟨x, now, lbTimer, counter⟩

StmtB(t) ≜
    ∧ x′ = t
    ∧ GoFromTo(t, "b", "c")
    ∧ ResetUBTimer(t, ubTimer)
    ∧ SetTimer(t, lbTimer, Epsilon)
    ∧ UNCHANGED ⟨now, counter⟩

StmtC(t) ≜
    ∧ At(t, "c")
    ∧ TimedOut(t, lbTimer)
    ∧ IF x ≠ t THEN GoTo(t, "a") ELSE  GoTo(t, "cs")
    ∧ UNCHANGED ⟨x, now, lbTimer, ubTimer, counter⟩

CS(t) ≜
     ∧ GoFromTo(t, "cs", "d")
     ∧ counter′ = [counter EXCEPT ![t] = @ + 1]
     ∧ UNCHANGED ⟨x, now, lbTimer, ubTimer⟩

StmtD(t) ≜
    ∧ x′ = NotAThread
    ∧ GoFromTo(t, "d", "ncs")
    ∧ UNCHANGED ⟨now, lbTimer, ubTimer, counter⟩

Tick ≜
```

```
    LET $d \triangleq 1$
     IN  $\land \forall t \in Thread :$
             $ubTimer[t] \neq Infinity \Rightarrow ubTimer[t] > d$
         $\land now' = now + d$     Where is now used in the spec?
         $\land ubTimer' = [t \in Thread \mapsto$
                             IF $ubTimer[t] = Infinity$ THEN $Infinity$
                                                       ELSE $ubTimer[t] - d]$
         $\land lbTimer' = [t \in Thread \mapsto Max(0, lbTimer[t] - d)]$
         $\land$ UNCHANGED $\langle x, pc, counter \rangle$

$Next \triangleq$
    $\lor Tick$
    $\lor \exists t \in Thread :$
        $\lor NCS(t)$
        $\lor StmtA(t) \lor StmtB(t) \lor StmtC(t)$
        $\lor CS(t)$
        $\lor StmtD(t)$

$SafetySpec \triangleq Init \land \Box[Next]_{vars}$

THEOREM $SafetySpec \Rightarrow \Box MutualExclusion$

$Liveness \triangleq$
    $\land \forall t \in Thread : \mathrm{WF}_{vars}(StmtA(t) \lor StmtC(t) \lor StmtD(t))$
    $\land \mathrm{SF}_{vars}(Tick)$

$FSpec1 \triangleq SafetySpec \land Liveness$

$Progress \triangleq$
    $(\exists t \in Thread : At(t, \text{"a"}) \lor At(t, \text{"b"}) \lor At(t, \text{"c"})) \leadsto$
       $(\exists t \in Thread : At(t, \text{"cs"}))$

THEOREM $FSpec1 \Rightarrow Progress$

\* Modification History
\* Last modified Sat Aug 07 16:13:28 CST 2021 by hengxin
\* Created Sat Aug 07 15:47:31 CST 2021 by hengxin
```