MODULE *Timer*

EXTENDS *Naturals*, *DK_RealTime*, *RealTime*

VARIABLES *timers*

$$TTypeInv \triangleq timers \in [Nat \to [t, l : Nat, r : \{\text{“no”}, \text{“yes”}\}]]$$

$$TInit \triangleq timers = [n \in Nat \to [t \to now, l \to 0, r \to \text{“no”}]]$$

$$\begin{aligned} Set(i, lim) \triangleq\ & \land lim > 0 \\ & \land timers[i].r = \text{“no”} \\ & \land timers' = [timers \text{ EXCEPT } ![i] = [t \to @.t, l \to lim, r \to @.r]] \\ & \land \text{UNCHANGED } \langle now \rangle \end{aligned}$$

$$\begin{aligned} Start(i) \triangleq\ & \land timers[i].r = \text{“no”} \\ & \land timers[i].l > 0 \\ & \land timers' = [timers \text{ EXCEPT } ![i] = [t \to now, l \to @.l, r \to \text{“yes”}]] \\ & \land \text{UNCHANGED } \langle now \rangle \end{aligned}$$

$$\begin{aligned} Timeout(i) \triangleq\ & \land timers[i].r = \text{“yes”} \\ & \land now - timers[i].t \geq timers[i].l \\ & \land timers' = [timers \text{ EXCEPT } ![i] = [t \to @.t, l \to @.l, r \to \text{“no”}]] \\ & \land \text{UNCHANGED } \langle now \rangle \end{aligned}$$

$$\begin{aligned} Stop(i) \triangleq\ & \land timers[i].r = \text{“yes”} \\ & \land timers' = [timers \text{ EXCEPT } ![i] = [t \to @.t, l \to @.l, r \to \text{“no”}]] \\ & \land \text{UNCHANGED } \langle now \rangle \end{aligned}$$

$$TNext \triangleq \exists\, i \in Nat : Start(i) \lor Stop(i) \lor Timeout(i) \lor (\exists\, t \in Nat : Set(i, t))$$

$$TSpec \triangleq TInit \land \Box[TNext]_{timers} \land (\forall\, i \in Nat : RTBound(Timeout(i), \langle timers, now \rangle, 0, 1))$$

THEOREM $TSpec \Rightarrow \Box\, TTypeInv$