MODULE *timer*

EXTENDS *Naturals*, *RealTime*
VARIABLES *time*, *running*, *limit*

$$\begin{aligned} TTypeInv \triangleq\ & \land time \in Nat \\ & \land limit \in Nat \\ & \land running \in \{\text{“yes”}, \text{“no”}\} \end{aligned}$$

$$av \triangleq \langle limit, time, running\rangle$$
$$sv \triangleq \langle limit, time, running, now\rangle$$

$$TInit \triangleq limit = 0 \land running = \text{“no”}$$

$$\begin{aligned} Set(l) \triangleq\ & \land l > 0 \\ & \land running = \text{“no”} \\ & \land limit' = l \\ & \land \text{UNCHANGED } \langle time, now, running\rangle \end{aligned}$$

$$\begin{aligned} Start \triangleq\ & \land running = \text{“no”} \\ & \land limit > 0 \\ & \land time' = now \\ & \land running' = \text{“yes”} \\ & \land \text{UNCHANGED } \langle now, limit\rangle \end{aligned}$$

$$\begin{aligned} Timeout \triangleq\ & \land running = \text{“yes”} \\ & \land now - time \geq limit \\ & \land running' = \text{“no”} \\ & \land \text{UNCHANGED } \langle now, time, limit\rangle \end{aligned}$$

$$\begin{aligned} Stop \triangleq\ & \land running = \text{“yes”} \\ & \land running' = \text{“no”} \\ & \land \text{UNCHANGED } \langle now, time, limit\rangle \end{aligned}$$

$$TNext \triangleq Start \lor Stop \lor Timeout \lor (\exists\, t \in Nat : Set(t))$$
$$TSpec \triangleq TInit \land \Box[TNext]_{sv} \land RTBound(Timeout, av, 0, 1)$$

THEOREM $TSpec \Rightarrow \Box\, TTypeInv$

MODULE *RealTime*

EXTENDS Reals, *Naturals* VARIABLES now

(**)
(* *Estas* definiciones son de *DK_RealTime*. Se agregaron a este modulo porque *)
(* extenderlo desde aquel era un quilombo. *)
(**)

$$RTTypeInv \triangleq now \in Nat$$

$RTInit \triangleq now = 0$
Tick $\triangleq now' = now + 1$
$RTSpec \triangleq RTInit \land \text{WF\_}now(Tick)$

$RTBound(A, v, D, E) \triangleq$
LET $TNext(t) \triangleq t' = \text{IF } \langle A\rangle\_v \lor \neg(\text{ENABLED } \langle A\rangle\_v)'$
THEN 0
ELSE $t + (now' - now)$
$Timer(t) \triangleq (t = 0) \land \Box[TNext(t)]\_\langle t, v, now\rangle$
$MaxTime(t) \triangleq \Box(t \leq E)$
$MinTime(t) \triangleq \Box[A \Rightarrow t \geq D]\_v$
IN $\exists\, t : Timer(t) \land MaxTime(t) \land MinTime(t)$

$RTnow(v) \triangleq$ LET $NowNext \triangleq \land now' \in \{r \in Real : r > now\}$
$\land$ UNCHANGED v
IN $\land now \in Real$
$\land \Box[NowNext]\_now$
$\land \forall\, r \in Real : \text{WF\_}now(NowNext \land (now' > r))$

THEOREM $RTSpec \Rightarrow \Box RTTypeInv$

\ * *Modification History*
\ * *Last modified Sun Feb* 27 21 : 28 : 57 *ART* 2022 *by sebapc*
\ * *Created Sun Feb* 27 20 : 21 : 57 *ART* 2022 *by sebapc*