

<div> <div>MODULE <i>Timer</i></div> <div>EXTENDS <i>Naturals</i>, <i>DK_RealTime</i>, <i>RealTime</i></div> <div>VARIABLES <i>time</i>, <i>running</i>, <i>limit</i></div> <div> <math display="block">TTypeInv \triangleq time, limit \in Nat \wedge running \in \{ "no", "yes" \}</math> <math display="block">sv \triangleq \langle limit, running, time \rangle</math> <math display="block">av \triangleq \langle limit, running, time, now \rangle</math> </div> <div> <math display="block">TInit \triangleq limit = 0 \wedge running = "no"</math> <math display="block">Set(l) \triangleq \wedge l &gt; 0</math> <math display="block">\wedge running = "no"</math> <math display="block">\wedge limit' = l</math> <math display="block">\wedge UNCHANGED \langle time, now, running \rangle</math> <math display="block">Start \triangleq \wedge running = "yes"</math> <math display="block">\wedge limit &gt; 0</math> <math display="block">\wedge time' = now</math> <math display="block">\wedge running' = "yes"</math> <math display="block">\wedge UNCHANGED \langle now, limit \rangle</math> <math display="block">Timeout \triangleq \wedge running = "yes"</math> <math display="block">\wedge now - time \geq limit</math> <math display="block">\wedge running' = "no"</math> <math display="block">\wedge UNCHANGED \langle time, now, limit \rangle</math> <math display="block">Stop \triangleq \wedge running = "yes"</math> <math display="block">\wedge running' = "no"</math> <math display="block">\wedge UNCHANGED \langle time, now, limit \rangle</math> <math display="block">TNext \triangleq Start \vee Stop \vee Timeout \vee (\exists t \in Nat : Set(t))</math> <math display="block">TSpec \triangleq TInit \wedge \Box [TNext]_{sv} \wedge RTBound(Timeout, av, 0, 1)</math> <div>THEOREM <math>TSpec \Rightarrow \Box TTypeInv</math></div> </div> </div>
--