MODULE *AJupiterH*

EXTENDS *AJupiter*

VARIABLE *list*

$varsH \triangleq \langle vars, list \rangle$

$TypeOKH \triangleq TypeOK \land (list \subseteq List)$

$InitH \triangleq Init \land list = \{InitState\}$

$DoH(c) \triangleq Do(c) \land list' = list \cup \{state'[c]\}$

$RevH(c) \triangleq Rev(c) \land list' = list \cup \{state'[Server]\}$

$SRevH \triangleq SRev \land list' = list \cup \{state'[Server]\}$

$NextH \triangleq$
$\quad \lor \exists\, c \in Client : DoH(c) \lor RevH(c)$
$\quad \lor SRevH$

$FairnessH \triangleq$
$\quad \mathrm{WF}_{varsH}(SRevH \lor \exists\, c \in Client : RevH(c))$

$SpecH \triangleq InitH \land \Box[NextH]_{varsH}$ $\land FairnessH$

$WLSpec \triangleq$ The weak list specification
$\quad Comm\,!\,EmptyChannel$ no need to check *Compatible* at every state
$\qquad \Rightarrow \forall\, l1,\, l2 \in list :$
$\qquad\quad \land Injective(l1)$ no duplicate elements
$\qquad\quad \land Injective(l2)$ true due to our distinctness assumption
$\qquad\quad \land Compatible(l1,\, l2)$

THEOREM $SpecH \Rightarrow \Box WLSpec$

* Modification History
* Last modified *Wed Jan* 30 21:37:29 *CST* 2019 by anonymous
* Created *Thu Aug* 30 21:26:18 *CST* 2018 by anonymous