MODULE *InternalMemory*

EXTENDS *MemoryInterface*

VARIABLES *mem*, *ctl*, *buf*

$vars \triangleq \langle memInt, mem, ctl, buf \rangle$

$$
\begin{aligned}
IInit \triangleq\ & \land mem \in [Adr \to Val] \\
& \land ctl\ \ = [p \in Proc \mapsto \text{“rdy”}] \\
& \land buf\ \ = [p \in Proc \mapsto NoVal] \\
& \land memInt \in InitMemInt
\end{aligned}
$$

$$
\begin{aligned}
TypeInvariant \triangleq\ & \\
& \land mem \in [Adr \to Val] \\
& \land ctl\ \ \in [Proc \to \{\text{“rdy”}, \text{“busy”}, \text{“done”}\}] \\
& \land buf\ \ \in [Proc \to MReq \cup Val \cup \{NoVal\}]
\end{aligned}
$$

$$
\begin{aligned}
Req(p) \triangleq\ & \land ctl[p] = \text{“rdy”} \\
& \land \exists\, req \in MReq : \\
& \qquad \land Send(p, req, memInt, memInt') \\
& \qquad \land buf' = [buf \text{ EXCEPT } ![p] = req] \\
& \qquad \land ctl' = [ctl \text{ EXCEPT } ![p] = \text{“busy”}] \\
& \land \text{UNCHANGED } mem
\end{aligned}
$$

$$
\begin{aligned}
Do(p) \triangleq\ & \\
& \land ctl[p] = \text{“busy”} \\
& \land mem' = \text{IF } buf[p].op = \text{“Wr”} \\
& \qquad \text{THEN } [mem \text{ EXCEPT } ![buf[p].adr] = buf[p].val] \\
& \qquad \text{ELSE } mem \\
& \land buf' = [buf \text{ EXCEPT } ![p] = \text{IF } buf[p].op = \text{“Wr”} \\
& \qquad\qquad\qquad\qquad \text{THEN } NoVal \\
& \qquad\qquad\qquad\qquad \text{ELSE } mem[buf[p].adr]] \\
& \land ctl' = [ctl \text{ EXCEPT } ![p] = \text{“done”}] \\
& \land \text{UNCHANGED } memInt
\end{aligned}
$$

$$
\begin{aligned}
Rsp(p) \triangleq\ & \land ctl[p] = \text{“done”} \\
& \land Reply(p, buf[p], memInt, memInt') \\
& \land ctl' = [ctl \text{ EXCEPT } ![p] = \text{“rdy”}] \\
& \land \text{UNCHANGED } \langle mem, buf \rangle
\end{aligned}
$$

$$INext \triangleq \exists\, p \in Proc : Req(p) \lor Do(p) \lor Rsp(p)$$

Liveness: Every request must receive a response.

$$Liveness \triangleq \forall\, p \in Proc : \mathrm{WF}_{vars}(Do(p)) \land \mathrm{WF}_{vars}(Rsp(p))$$

$$ISpec \triangleq IInit \ \land\ \Box[INext]_{vars}$$

THEOREM $ISpec \Rightarrow \Box\, TypeInvariant$