MODULE *System*

EXTENDS *Naturals*, *RealTime*

CONSTANTS *Data*, *SENDTIME*
CONSTANT *BusSend*(_)
ASSUME $\forall\, m : BusSend(m) \in$ BOOLEAN
ASSUME $SENDTIME \in Nat \land SENDTIME > 0$

VARIABLES *terminals*, *bus*, *collision*, *timers*

$NoData \triangleq$ CHOOSE $d : d \notin Data$

$$
\begin{aligned}
TypeInv \triangleq\ & \land terminals \in [Nat \to [status : \{\text{“rdy”}, \text{“trying”}, \text{“fail”},\\
& \qquad\qquad \text{“transmiting”}, \text{“waiting”}, \text{“recovering”},\\
& \qquad\qquad \text{“retry”}, \text{“collision”}, \text{“restart”}\},\\
& \qquad msg : Data \cup \{NoData\}]]\\
& \land bus, collision \in \{0, 1\}\\
& \land timers = [Nat \to [t, l : Nat, r : \{\text{“no”}, \text{“yes”}\}]]
\end{aligned}
$$

$Ts \triangleq$ INSTANCE *Timers*

$$
\begin{aligned}
Init \triangleq\ & \land Ts!Init\\
& \land terminals = [n \in Nat \to [status \to \text{“rdy”}, msg \to NoData]]\\
& \land bus = 0\\
& \land collision = 0
\end{aligned}
$$

$vars \triangleq \langle terminals, bus, collision, timers\rangle$

$$
\begin{aligned}
SetSend(i) \triangleq\ & \land terminals[i].status = \text{“rdy”}\\
& \land \exists\, d \in data :\\
& \qquad \land Ts!Set(i, SENDTIME)\\
& \qquad \land terminals' = [terminals \text{ EXCEPT}\\
& \qquad\qquad ![i] = [status \to \text{“trying”}, msg \to d]]\\
& \qquad \land \text{UNCHANGED } \langle bus, collision\rangle
\end{aligned}
$$

$$
\begin{aligned}
SendOk(i) \triangleq\ & \land terminals[i].status = \text{“trying”}\\
& \land bus = 0\\
& \land BusSend(terminals[i].msg)\\
& \land Ts!Start(i)\\
& \land terminals' = [terminals \text{ EXCEPT}\\
& \qquad\qquad ![i] = [status \to \text{“transmiting”}, msg \to @.msg]]\\
& \land bus' = 1\\
& \land \text{UNCHANGED } \langle collision\rangle
\end{aligned}
$$

$$
\begin{array}{l}
SendFail(i) \triangleq \\
\quad \land\ terminals[i].status = \text{“trying”} \\
\quad \land\ bus = 1 \\
\quad \land\ \exists\, r \in Nat : \\
\qquad \land\ r > 0 \\
\qquad \land\ Ts!Set(i,\ r) \\
\qquad \land\ terminals' = [terminals\ \text{EXCEPT} \\
\qquad\qquad\qquad\qquad ![i] = [status \to \text{“fail”},\ msg \to @.msg]] \\
\qquad \land\ \text{UNCHANGED}\ \langle bus,\ collision\rangle
\end{array}
$$

$$
\begin{array}{l}
Fail(i) \triangleq \\
\quad \land\ terminals[i].status = \text{“fail”} \\
\quad \land\ Ts!Start(i) \\
\quad \land\ terminals' = [terminals\ \text{EXCEPT} \\
\qquad\qquad\qquad ![i] = [status \to \text{“waiting”},\ msg \to @.msg]] \\
\quad \land\ \text{UNCHANGED}\ \langle bus,\ collision >
\end{array}
$$

$$
\begin{array}{l}
WaitAfterFail(i) \triangleq \\
\quad \land\ terminals[i].status = \text{“waiting”} \\
\quad \land\ Ts!Timeout(i) \\
\quad \land\ terminals' = [terminals\ \text{EXCEPT} \\
\qquad\qquad\qquad\qquad ![i] = [status \to \text{“retry”},\ msg \to @.msg]] \\
\quad \land\ \text{UNCHANGED}\ \langle bus,\ collision\rangle
\end{array}
$$

$$
\begin{array}{l}
Retry(i) \triangleq \\
\quad \land\ terminals[i].status = \text{“retry”} \\
\quad \land\ Ts!Set(i,\ SENDTIME) \\
\quad \land\ terminals' = [terminals\ \text{EXCEPT} \\
\qquad\qquad\qquad ![i] = [status \to \text{“trying”},\ msg \to @.msg]] \\
\quad \land\ \text{UNCHANGED}\ \langle bus,\ collision\rangle
\end{array}
$$

$$
\begin{array}{l}
WaitAfterCollision(i) \triangleq \\
\quad \land\ terminals[i].status = \text{“recovering”} \\
\quad \land\ Ts!Timeout(i) \\
\quad \land\ terminals' = [terminals\ \text{EXCEPT} \\
\qquad\qquad\qquad\qquad ![i] = [status \to \text{“rdy”},\ msg \to @.msg]] \\
\quad \land\ \text{UNCHANGED}\ \langle bus,\ collision\rangle
\end{array}
$$

$$
\begin{array}{l}
Deliver(i) \triangleq \\
\quad \land\ terminals[i].status = \text{“transmiting”} \\
\quad \land\ Ts!Timeout(i) \\
\quad \land\ bus = 1 \\
\quad \land\ terminals' = [terminals\ \text{EXCEPT} \\
\qquad\qquad\qquad ![i] = [status \to \text{“rdy”},\ msg \to NoData]] \\
\quad \land\ bus' = 0 \\
\quad \land\ \text{UNCHANGED}\ \langle collision\rangle
\end{array}
$$

$$
\begin{array}{l}
DetectCollision \triangleq \exists\, i,\ j \in Nat \land i \neq j : \land\ terminals[i] = \text{“transmiting”} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\ terminals[j] = \text{“transmiting”} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\ collision' = 1 \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \land\ \text{UNCHANGED}\ \langle bus,\ timers,\ terminals\rangle
\end{array}
$$

$$
\begin{array}{lll}
\mathit{Collision} & \triangleq & \land\ \mathit{collision} = 1 \\
& & \land\ \mathit{terminals}' = [n \in \mathit{Nat} \to [\mathit{status} \to \text{“collision”},\ \mathit{msg} \to \mathit{NoData}]] \\
& & \land\ \mathit{timers}' = [n \in \mathit{Nat} \to [t \to 0,\ l\ \to 0,\ r \to \text{“no”}]] \\
& & \land\ \mathit{bus}' = 0 \\
& & \land\ \mathit{collision}' = 0
\end{array}
$$

$$
\begin{array}{lll}
\mathit{SetAfterCollision}(i) & \triangleq & \land\ \mathit{terminals}[i].\mathit{status} = \text{“collision”} \\
& & \land\ \exists\, r \in \mathit{Nat} \land r > 0 : \\
& & \quad \land\ \mathit{Ts}!\mathit{Set}(i,\ r) \\
& & \quad \land\ \mathit{terminals}' = [\mathit{terminals}\ \text{EXCEPT} \\
& & \qquad\qquad ![i] = [\mathit{status} \to \text{“restart”},\ \mathit{msg} \to @.\mathit{msg}]] \\
& & \quad \land\ \text{UNCHANGED}\ \langle \mathit{bus},\ \mathit{collision} \rangle
\end{array}
$$

$$
\begin{array}{lll}
\mathit{Restart}(i) & \triangleq & \land\ \mathit{terminals}[i].\mathit{status} = \text{“restart”} \\
& & \land\ \mathit{Ts}!\mathit{Start}(i) \\
& & \land\ \mathit{terminals}' = [\mathit{terminals}\ \text{EXCEPT} \\
& & \qquad\qquad ![i] = [\mathit{status} \to \text{“recovering”},\ \mathit{msg} \to @.\mathit{msg}]] \\
& & \land\ \text{UNCHANGED}\ \langle \mathit{bus},\ \mathit{collision} \rangle
\end{array}
$$

$$
\begin{array}{lll}
\mathit{Next} & \triangleq & \lor\ \mathit{Collision} \\
& & \lor\ \mathit{DetectCollision} \\
& & \lor\ (\exists\, i \in \mathit{Nat} :\ \lor\ \mathit{SetSend}(i) \lor \mathit{SendOk}(i) \lor \mathit{SendFail}(i) \\
& & \qquad\qquad \lor\ \mathit{Fail}(i) \lor \mathit{Retry}(i) \lor \mathit{Deliver}(i) \\
& & \qquad\qquad \lor\ \mathit{WaitAfterFail}(i) \lor \mathit{WaitAfterCollision}(i) \\
& & \qquad\qquad \lor\ \mathit{SetAfterCollision}(i) \lor \mathit{Restart}(i))
\end{array}
$$

$$
\begin{array}{lll}
\mathit{Fairness} & \triangleq & \land\ \mathrm{WF}_{\mathit{vars}}(\mathit{DetectCollision}) \\
& & \land\ \exists\, i \in \mathit{Nat} : \mathrm{WF}_{\mathit{vars}}(\ \lor\ \mathit{SendFail}(i) \lor \mathit{Retry}(i) \\
& & \qquad\qquad\qquad\qquad \lor\ \mathit{Fail}(i) \lor \mathit{SetAfterCollision}(i) \\
& & \qquad\qquad\qquad\qquad \lor\ \mathit{Restart}(i)) \\
& & \land\ \exists\, i \in \mathit{Nat} : \mathrm{SF}_{\mathit{vars}}(\mathit{SendOk}(i))
\end{array}
$$

$$
\begin{array}{lll}
\mathit{Spec} & \triangleq & \land\ \mathit{Init} \\
& & \land\ \Box[\mathit{Next}]_{\mathit{vars}} \\
& & \land\ \mathit{Fairness} \\
& & \land\ \mathit{RTBound}(\mathit{Collision},\ \mathit{vars},\ 0,\ 1) \\
& & \land\ \mathit{RTBound}(\mathit{DetectCollision},\ \mathit{vars},\ 0,\ 1)
\end{array}
$$

THEOREM $\mathit{Spec} \Rightarrow \mathit{TypeInv}$
