MODULE *TreinProtocol*

EXTENDS *Naturals*
VARIABLES *system*

$$
\begin{aligned}
&\mathit{trein\_waarden} \triangleq \{\text{“perron”}, \text{“vertrokken”}\}\\
&\mathit{deur\_waarden} \triangleq \{\text{“open”}, \text{“dicht”}\}\\
&\mathit{begeleider\_waarden} \triangleq \{\text{“perron”}, \text{“trein”}\}\\
&\mathit{AC\_waarden} \triangleq \{\text{“aan”}, \text{“uit”}\}\\
&\mathit{licht\_waarden} \triangleq \{\text{“uit”}, \text{“rood”}, \text{“wit”}\}\\
&\mathit{bestuurder\_waarden} \triangleq \{\text{“wacht”}, \text{“wil\_vertrekken”}\}\\
&\mathit{startuur\_waarden} \triangleq \{\text{“aangebroken”}, \text{“n\_aangebroken”}\}\\
&\mathit{spoor\_waarden} \triangleq \{\text{“vrij”}, \text{“n\_vrij”}\}
\end{aligned}
$$

$$
\begin{aligned}
&\mathit{TypeInvariant} \triangleq \mathit{system} \in [\mathit{trein} : \mathit{trein\_waarden}, \mathit{deur\_beg} : \mathit{deur\_waarden},\\
&\quad \mathit{deur\_rest} : \mathit{deur\_waarden}, \mathit{begeleider} : \mathit{begeleider\_waarden}, \mathit{AC} : \mathit{AC\_waarden},\\
&\quad \mathit{licht} : \mathit{licht\_waarden}, \mathit{bestuurder} : \mathit{bestuurder\_waarden}, \mathit{startuur} : \mathit{startuur\_waarden},\\
&\quad \mathit{spoor} : \mathit{spoor\_waarden}]
\end{aligned}
$$

$$
\begin{aligned}
\mathit{Init} \triangleq\ &\land \mathit{TypeInvariant}\\
&\land \mathit{system.trein} = \text{“perron”}\\
&\land \mathit{system.deur\_beg} = \text{“open”}\\
&\land \mathit{system.deur\_rest} = \text{“open”}\\
&\land \mathit{system.begeleider} = \text{“perron”}\\
&\land \mathit{system.bestuurder} = \text{“wacht”}\\
&\land \mathit{system.AC} = \text{“uit”}\\
&\land \mathit{system.licht} = \text{“uit”}\\
&\land \mathit{system.spoor} = \text{“vrij”}\\
&\land \mathit{system.startuur} = \text{“n\_aangebroken”}
\end{aligned}
$$

$$
\begin{aligned}
\mathit{uur\_aangebroken} \triangleq\ &\land \mathit{system.startuur} = \text{“n\_aangebroken”}\\
&\land \mathit{system}' = [\mathit{system}\ \text{EXCEPT}\ !.\mathit{startuur} = \text{“aangebroken”}]
\end{aligned}
$$

$$
\begin{aligned}
\mathit{beg\_sluit\_andere\_deuren} \triangleq\ &\land \mathit{system.deur\_rest} = \text{“open”}\\
&\land \mathit{system.begeleider} = \text{“trein”}\\
&\land \mathit{system}' = [\mathit{system}\ \text{EXCEPT}\ !.\mathit{deur\_rest} = \text{“dicht”}]
\end{aligned}
$$

$$
\begin{aligned}
\mathit{beg\_sluit\_eigen\_deur} \triangleq\ &\land \mathit{system.deur\_beg} = \text{“open”}\\
&\land \mathit{system.trein} = \text{“vertrokken”}\\
&\land \mathit{system.begeleider} = \text{“trein”}\\
&\land \mathit{system}' = [\mathit{system}\ \text{EXCEPT}\ !.\mathit{deur\_beg} = \text{“dicht”}]
\end{aligned}
$$

$$
\begin{aligned}
\mathit{beg\_stapt\_af} \triangleq\ &\land (\mathit{system.deur\_beg} = \text{“open”} \lor \mathit{system.deur\_rest} = \text{“open”})\\
&\land \mathit{system.begeleider} = \text{“trein”}\\
&\land \mathit{system.trein} = \text{“perron”}\\
&\land \mathit{system}' = [\mathit{system}\ \text{EXCEPT}\ !.\mathit{begeleider} = \text{“perron”}]
\end{aligned}
$$

$$
\begin{array}{lcl}
\mathit{beg\_stapt\_op} & \triangleq & \land\ (\mathit{system.deur\_beg} = \text{“}\textsf{open}\text{”} \lor \mathit{system.deur\_rest} = \text{“}\textsf{open}\text{”})\\
 & & \land\ \mathit{system.trein} = \text{“}\textsf{perron}\text{”}\\
 & & \land\ \mathit{system.begeleider} = \text{“}\textsf{perron}\text{”}\\
 & & \land\ \mathit{system}' = [\mathit{system}\ \textsc{except}\ !.\mathit{begeleider} = \text{“}\textsf{trein}\text{”}]
\end{array}
$$

$$
\begin{array}{lcl}
\mathit{activeren\_AC} & \triangleq & \land\ \mathit{system.startuur} = \text{“}\textsf{aangebroken}\text{”}\\
 & & \land\ \mathit{system.deur\_rest} = \text{“}\textsf{dicht}\text{”}\\
 & & \land\ \mathit{system.begeleider} = \text{“}\textsf{perron}\text{”}\\
 & & \land\ \mathit{system.AC} = \text{“}\textsf{uit}\text{”}\\
 & & \land\ \mathit{system}' = [\mathit{system}\ \textsc{except}\ !.\mathit{AC} = \text{“}\textsf{aan}\text{”},\ !.\mathit{licht} = \text{“}\textsf{rood}\text{”}]
\end{array}
$$

$$
\begin{array}{lcl}
\mathit{licht\_op\_wit} & \triangleq & \land\ \mathit{system.licht} = \text{“}\textsf{rood}\text{”}\\
 & & \land\ \mathit{system}' = [\mathit{system}\ \textsc{except}\ !.\mathit{licht} = \text{“}\textsf{wit}\text{”}]
\end{array}
$$

$$
\begin{array}{lcl}
\mathit{best\_wil\_vertrekken} & \triangleq & \land\ \mathit{system.spoor} = \text{“}\textsf{vrij}\text{”}\\
 & & \land\ \mathit{system.licht}\ \ = \text{“}\textsf{wit}\text{”}\\
 & & \land\ \mathit{system.bestuurder} = \text{“}\textsf{wacht}\text{”}\\
 & & \land\ \mathit{system}' = [\mathit{system}\ \textsc{except}\ !.\mathit{bestuurder} = \text{“}\textsf{wil\_vertrekken}\text{”}]
\end{array}
$$

$$
\begin{array}{lcl}
\mathit{trein\_vertrekt} & \triangleq & \land\ \mathit{system.bestuurder} = \text{“}\textsf{wil\_vertrekken}\text{”}\\
 & & \land\ \mathit{system}' = [\mathit{system}\ \textsc{except}\ !.\mathit{trein} = \text{“}\textsf{vertrokken}\text{”}]
\end{array}
$$

$$
\begin{array}{lcl}
\mathit{Next} & \triangleq & \lor\ \mathit{uur\_aangebroken}\\
 & & \lor\ \mathit{beg\_sluit\_andere\_deuren}\\
 & & \lor\ \mathit{beg\_sluit\_eigen\_deur}\\
 & & \lor\ \mathit{beg\_stapt\_af}\\
 & & \lor\ \mathit{beg\_stapt\_op}\\
 & & \lor\ \mathit{activeren\_AC}\\
 & & \lor\ \mathit{licht\_op\_wit}\\
 & & \lor\ \mathit{best\_wil\_vertrekken}\\
 & & \lor\ \mathit{trein\_vertrekt}
\end{array}
$$

$$
\begin{array}{lcl}
\mathit{Liveness} & \triangleq & \land\ \mathrm{SF}_{\mathit{system}}(\mathit{uur\_aangebroken})\\
 & & \land\ \mathrm{SF}_{\mathit{system}}(\mathit{beg\_sluit\_andere\_deuren})\\
 & & \land\ \mathrm{SF}_{\mathit{system}}(\mathit{beg\_stapt\_af})\\
 & & \land\ \mathrm{SF}_{\mathit{system}}(\mathit{activeren\_AC})\\
 & & \land\ \mathrm{SF}_{\mathit{system}}(\mathit{beg\_stapt\_op})\\
 & & \land\ \mathrm{SF}_{\mathit{system}}(\mathit{licht\_op\_wit})\\
 & & \land\ \mathrm{SF}_{\mathit{system}}(\mathit{best\_wil\_vertrekken})\\
 & & \land\ \mathrm{SF}_{\mathit{system}}(\mathit{trein\_vertrekt})\\
 & & \land\ \mathrm{SF}_{\mathit{system}}(\mathit{beg\_sluit\_eigen\_deur})
\end{array}
$$

$$
\mathit{Spec} \triangleq \mathit{Init} \land \Box[\mathit{Next}]_{\mathit{system}} \land \mathit{Liveness}
$$

$$
\begin{array}{lcl}
\mathit{veiligheidseis}1 & \triangleq & \mathit{system.trein} = \text{“}\textsf{vertrokken}\text{”} \Rightarrow \mathit{system.begeleider} = \text{“}\textsf{trein}\text{”}\\
\mathit{veiligheidseis}2 & \triangleq & \mathit{system.trein} = \text{“}\textsf{vertrokken}\text{”} \Rightarrow \mathit{system.deur\_rest} = \text{“}\textsf{dicht}\text{”}
\end{array}
$$

$$veiligheidseis3 \triangleq system.trein = \text{“vertrokken”} \leadsto system.deur\_beg = \text{“dicht”}$$

$$liveness\_eis \triangleq (system.startuur = \text{“aangebroken”} \land system.spoor = \text{“vrij”}) \leadsto (system.trein = \text{“vertrokken”})$$