MODULE *Config*

EXTENDS
Northbound,
Proposal,
Configuration,
Mastership,
Southbound

INSTANCE *Naturals*

INSTANCE *FiniteSets*

INSTANCE *Sequences*

LOCAL INSTANCE *TLC*

$vars \triangleq \langle proposal,\ configuration,\ mastership,\ node,\ target \rangle$

Formal specification, constraints, and theorems.

$Init \triangleq$
$\land\ InitNorthbound$
$\land\ InitProposal$
$\land\ InitConfiguration$
$\land\ InitMastership$
$\land\ InitSouthbound$

$Next \triangleq$
$\lor\ \land\ NextNorthbound$
$\quad\land$ UNCHANGED $\langle\rangle$
$\lor\ \land\ NextProposal$
$\quad\land$ UNCHANGED $\langle\rangle$
$\lor\ \land\ NextConfiguration$
$\quad\land$ UNCHANGED $\langle proposal \rangle$
$\lor\ \land\ NextMastership$
$\quad\land$ UNCHANGED $\langle proposal,\ configuration \rangle$
$\lor\ \land\ NextSouthbound$
$\quad\land$ UNCHANGED $\langle proposal,\ configuration,\ mastership \rangle$

$Spec \triangleq$
$\land\ Init$
$\land\ \Box[Next]_{vars}$
$\land\ \forall\, i\ \in 1\,..\,NumProposals : \mathrm{WF}_{vars}(Change(i) \lor Rollback(i))$
$\land\ \forall\, n \in Nodes,\ i \in 1\,..\,NumProposals : \mathrm{WF}_{vars}(ReconcileProposal(n,\ i))$
$\land\ \forall\, n \in Nodes : \mathrm{WF}_{\langle configuration,\ mastership,\ node,\ target \rangle}(ReconcileConfiguration(n))$
$\land\ \forall\, n \in Nodes : \mathrm{WF}_{\langle mastership,\ node,\ target \rangle}(ReconcileMastership(n))$

$\land \forall\, n \in \mathit{Nodes} : \mathrm{WF}_{\langle \mathit{node},\, \mathit{target} \rangle}(\mathit{Connect}(n) \lor \mathit{Disconnect}(n))$
$\land \mathrm{WF}_{\langle \mathit{target} \rangle}(\mathit{Start})$
$\land \mathrm{WF}_{\langle \mathit{target} \rangle}(\mathit{Stop})$

$\mathit{IsCommittedChange}(i) \triangleq$
$\land\ \mathit{proposal}[i].\mathit{state} = \mathit{ProposalChange}$
$\land\ \lor\ \land\ \mathit{proposal}[i].\mathit{change}.\mathit{phase} = \mathit{ProposalCommit}$
$\qquad\ \land\ \mathit{proposal}[i].\mathit{change}.\mathit{status} = \mathit{ProposalFailed}$
$\qquad \lor\ \mathit{proposal}[i].\mathit{change}.\mathit{phase} = \mathit{ProposalApply}$

$\mathit{IsAppliedChange}(i) \triangleq$
$\land\ \mathit{proposal}[i].\mathit{state} = \mathit{ProposalChange}$
$\land\ \mathit{proposal}[i].\mathit{change}.\mathit{phase} = \mathit{ProposalApply}$
$\land\ \mathit{proposal}[i].\mathit{change}.\mathit{status} = \mathit{ProposalComplete}$

$\mathit{IsCommittedRollback}(i) \triangleq$
$\land\ \mathit{proposal}[i].\mathit{state} = \mathit{ProposalRollback}$
$\land\ \lor\ \land\ \mathit{proposal}[i].\mathit{change}.\mathit{phase} = \mathit{ProposalCommit}$
$\qquad\ \land\ \mathit{proposal}[i].\mathit{change}.\mathit{status} = \mathit{ProposalFailed}$
$\qquad \lor\ \mathit{proposal}[i].\mathit{change}.\mathit{phase} = \mathit{ProposalApply}$

$\mathit{IsAppliedRollback}(i) \triangleq$
$\land\ \mathit{proposal}[i].\mathit{state} = \mathit{ProposalRollback}$
$\land\ \lor\ \mathit{proposal}[i].\mathit{rollback}.\mathit{phase} = \mathit{ProposalCommit}$
$\qquad \lor\ \land\ \mathit{proposal}[i].\mathit{rollback}.\mathit{phase} = \mathit{ProposalApply}$
$\qquad\ \land\ \mathit{proposal}[i].\mathit{rollback}.\mathit{status} \in \{\mathit{ProposalPending},\ \mathit{ProposalComplete}\}$

$\mathit{Order} \triangleq$
$\forall\, i \in \text{DOMAIN}\ \mathit{proposal} :$
$\land\ \mathit{IsCommittedChange}(i) \Rightarrow$
$\qquad \forall\, j \in \text{DOMAIN}\ \mathit{proposal} : j < i \Rightarrow$
$\qquad\ \land\ \mathit{proposal}[j].\mathit{state} = \mathit{ProposalChange} \Rightarrow \mathit{IsCommittedChange}(j)$
$\qquad\ \land\ \mathit{proposal}[j].\mathit{state} = \mathit{ProposalRollback} \Rightarrow \mathit{IsCommittedRollback}(j)$
$\land\ \mathit{IsAppliedChange}(i) \Rightarrow$
$\qquad \forall\, j \in \text{DOMAIN}\ \mathit{proposal} : j < i \Rightarrow$
$\qquad\ \land\ \mathit{proposal}[j].\mathit{state} = \mathit{ProposalChange} \Rightarrow \mathit{IsAppliedChange}(j)$
$\qquad\ \land\ \mathit{proposal}[j].\mathit{state} = \mathit{ProposalRollback} \Rightarrow \mathit{IsAppliedRollback}(j)$

$\mathit{Consistency} \triangleq$
$\land\ \mathit{target}.\mathit{running}$
$\land\ \mathit{configuration}.\mathit{state} = \mathit{ConfigurationComplete}$
$\land\ \mathit{configuration}.\mathit{apply}.\mathit{incarnation} = \mathit{target}.\mathit{incarnation}$
$\Rightarrow \forall\, i \in \text{DOMAIN}\ \mathit{proposal} :$
$\qquad \mathit{IsAppliedChange}(i) \Rightarrow$
$\qquad\ \forall\, p \in \text{DOMAIN}\ \mathit{proposal}[i].\mathit{change}.\mathit{values} :$
$\qquad\ \land \neg\exists\, j \in \text{DOMAIN}\ \mathit{proposal} :$

$$
\begin{array}{l}
\quad \land\, j > i \\
\quad \land\, proposal[j].change.phase = ProposalApply \\
\quad \land\, proposal[j].change.status = ProposalComplete \\
\quad \land\, proposal[j].rollback.phase = ProposalApply \\
\qquad \Rightarrow proposal[j].rollback.status \neq ProposalComplete \\
\quad \land\, p \in \text{DOMAIN } proposal[j].change.values \\
\Rightarrow\ \land\, p \in \text{DOMAIN } target.values \\
\quad \land\, target.values[p].value = proposal[i].change.values[p].value \\
\quad \land\, target.values[p].index = proposal[i].change.values[p].index
\end{array}
$$

$Safety \triangleq \Box(Order \land Consistency)$

THEOREM $Spec \Rightarrow Safety$

$$
\begin{array}{l}
ChangeCommitting(i) \triangleq \\
\quad \land\, proposal[i].state = ProposalChange \\
\quad \land\, proposal[i].change.phase = ProposalCommit \\
\quad \land\, proposal[i].change.status = ProposalInProgress
\end{array}
$$

$$
\begin{array}{l}
ChangeApplied(i) \triangleq \\
\quad \land\, proposal[i].change.phase = ProposalApply \\
\quad \land\, proposal[i].change.status = ProposalComplete
\end{array}
$$

$$
\begin{array}{l}
RollbackCommitting(i) \triangleq \\
\quad \land\, proposal[i].state = ProposalRollback \\
\quad \land\, proposal[i].rollback.phase = ProposalCommit \\
\quad \land\, proposal[i].rollback.status = ProposalInProgress
\end{array}
$$

$$
\begin{array}{l}
RollbackApplied(i) \triangleq \\
\quad \land\, proposal[i].rollback.phase = ProposalApply \\
\quad \land\, proposal[i].rollback.status = ProposalComplete
\end{array}
$$

$$
\begin{array}{l}
Terminates(i) \triangleq \\
\quad \land\, ChangeCommitting(i) \leadsto ChangeApplied(i) \\
\quad \land\, RollbackCommitting(i) \leadsto RollbackApplied(i)
\end{array}
$$

$$
\begin{array}{l}
Termination \triangleq \\
\quad \forall\, i \in 1 \,..\, NumProposals : Terminates(i)
\end{array}
$$

$Liveness \triangleq Termination$

THEOREM $Spec \Rightarrow Liveness$

* Modification History
* Last modified *Fri Apr* 21 18:30:03 *PDT* 2023 by *jhalterm*
* Last modified *Mon Feb* 21 01:32:07 *PST* 2022 by *jordanhalterman*
* Created *Wed Sep* 22 13:22:32 *PDT* 2021 by *jordanhalterman*