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 $\langle proposal,\ configuration,\ mastership \rangle$

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

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

$\mathit{Order} \triangleq$
$\forall\, i \in \text{DOMAIN } \mathit{proposal} :$
$\land\ \mathit{proposal}[i].\mathit{change}.\mathit{commit} \in \{\mathit{ProposalInProgress},\ \mathit{ProposalAborted}\} \Rightarrow$
$\neg\exists\, j \in \text{DOMAIN } \mathit{proposal} :$
$\land\ j < i$
$\land\ \mathit{proposal}[j].\mathit{change}.\mathit{commit} \in \{\mathit{ProposalPending},\ \mathit{ProposalInProgress}\}$
$\land\ \mathit{proposal}[i].\mathit{change}.\mathit{commit} = \mathit{ProposalComplete} \Rightarrow$
$\neg\exists\, j \in \text{DOMAIN } \mathit{proposal} :$
$\land\ j < i$
$\land\ \mathit{proposal}[j].\mathit{change}.\mathit{commit} \in \{\mathit{ProposalPending},\ \mathit{ProposalInProgress}\}$
$\land\ \mathit{proposal}[i].\mathit{change}.\mathit{apply} \in \{\mathit{ProposalInProgress},\ \mathit{ProposalAborted}\} \Rightarrow$
$\neg\exists\, j \in \text{DOMAIN } \mathit{proposal} :$
$\land\ j < i$
$\land\ \lor\ \mathit{proposal}[j].\mathit{change}.\mathit{apply} \in \{\mathit{ProposalPending},\ \mathit{ProposalInProgress}\}$
$\lor\ \land\ \mathit{proposal}[j].\mathit{change}.\mathit{apply} = \mathit{ProposalFailed}$
$\land\ \mathit{proposal}[j].\mathit{rollback}.\mathit{apply} \notin \mathit{ProposalDone}$
$\land\ \mathit{proposal}[i].\mathit{change}.\mathit{apply} = \mathit{ProposalComplete} \Rightarrow$
$\neg\exists\, j \in \text{DOMAIN } \mathit{proposal} :$
$\land\ j < i$
$\land\ \lor\ \mathit{proposal}[j].\mathit{change}.\mathit{apply} \in \{\mathit{ProposalPending},\ \mathit{ProposalInProgress}\}$
$\lor\ \land\ \mathit{proposal}[j].\mathit{change}.\mathit{apply} = \mathit{ProposalFailed}$
$\land\ \mathit{proposal}[j].\mathit{rollback}.\mathit{apply} \notin \mathit{ProposalDone}$
$\land\ \mathit{proposal}[i].\mathit{rollback}.\mathit{commit} = \mathit{ProposalInProgress} \Rightarrow$
$\forall\, j \in \text{DOMAIN } \mathit{proposal} : j \quad > i \land \mathit{proposal}[j].\mathit{phase} = \mathit{ProposalRollback} \Rightarrow$
$\mathit{proposal}[j].\mathit{change}.\mathit{commit} \in \mathit{ProposalDone}$

$\mathit{Consistency} \triangleq$
$\land\ \mathit{target}.\mathit{running}$
$\land\ \mathit{configuration}.\mathit{state} = \mathit{ConfigurationComplete}$
$\land\ \mathit{configuration}.\mathit{apply}.\mathit{target} = \mathit{target}.\mathit{incarnation}$
$\Rightarrow \forall\, i \in \text{DOMAIN } \mathit{proposal} :$
$\land\ \mathit{proposal}[i].\mathit{change}.\mathit{apply} = \mathit{ProposalComplete}$
$\land\ \mathit{proposal}[i].\mathit{rollback}.\mathit{apply} \neq \mathit{ProposalComplete}$
$\Rightarrow \forall\, p \in \text{DOMAIN } \mathit{proposal}[i].\mathit{change}.\mathit{values} :$
$\land\ \neg\exists\, j \in \text{DOMAIN } \mathit{proposal} :$
$\land\ j > i$
$\land\ \mathit{proposal}[i].\mathit{change}.\mathit{apply} = \mathit{ProposalComplete}$
$\land\ \mathit{proposal}[i].\mathit{rollback}.\mathit{apply} \neq \mathit{ProposalComplete}$
$\Rightarrow\ \land\ p \in \text{DOMAIN } \mathit{target}.\mathit{values}$
$\land\ \mathit{target}.\mathit{values}[p].\mathit{value} = \mathit{proposal}[i].\mathit{change}.\mathit{values}[p].\mathit{value}$
$\land\ \mathit{target}.\mathit{values}[p].\mathit{index} = \mathit{proposal}[i].\mathit{change}.\mathit{values}[p].\mathit{index}$

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

THEOREM $Spec \Rightarrow Safety$

$$
\begin{array}{l}
Termination \triangleq \\
\quad \forall\, i \in 1 \,..\, NumProposals : \\
\qquad \land\, proposal[i].phase = ProposalChange \leadsto \\
\qquad\quad \land\, proposal[i].change.commit \in ProposalDone \\
\qquad\quad \land\, proposal[i].change.apply \in ProposalDone \\
\qquad \land\, proposal[i].phase = ProposalRollback \leadsto \\
\qquad\quad \land\, proposal[i].rollback.commit \in ProposalDone \\
\qquad\quad \land\, proposal[i].rollback.apply \in ProposalDone
\end{array}
$$

$Liveness \triangleq Termination$

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*