MODULE *Config*

EXTENDS
Northbound,
Proposals,
Configurations,
Southbound

INSTANCE *Naturals*

INSTANCE *FiniteSets*

INSTANCE *Sequences*

LOCAL INSTANCE *TLC*

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

Formal specification, constraints, and theorems.

$$
\begin{array}{l}
Init \triangleq \\
\quad \land\ InitProposal \\
\quad \land\ InitConfiguration \\
\quad \land\ InitNorthbound \\
\quad \land\ InitSouthbound
\end{array}
$$

$$
\begin{array}{l}
Next \triangleq \\
\quad \lor\ \land\ NextProposal \\
\qquad \land\ \text{UNCHANGED } \langle\rangle \\
\quad \lor\ \land\ NextConfiguration \\
\qquad \land\ \text{UNCHANGED } \langle proposal \rangle \\
\quad \lor\ \land\ NextNorthbound \\
\qquad \land\ \text{UNCHANGED } \langle configuration, target, mastership \rangle \\
\quad \lor\ \land\ NextSouthbound \\
\qquad \land\ \text{UNCHANGED } \langle proposal, configuration \rangle
\end{array}
$$

$$Spec \triangleq Init \land \Box[Next]_{vars} \land \mathrm{WF}_{vars}(Next)$$

$$
\begin{array}{l}
Order \triangleq \\
\quad \forall\, t \in \text{DOMAIN } proposal : \\
\qquad \forall\, i \in \text{DOMAIN } proposal[t] : \\
\qquad\quad \land\ \land\ proposal[t][i].phase = ProposalCommit \\
\qquad\qquad\ \land\ proposal[t][i].state\ \ = ProposalInProgress \\
\qquad\qquad\ \Rightarrow \neg\exists\, j \in \text{DOMAIN } proposal[t] : \\
\qquad\qquad\qquad\qquad \land\ j > i \\
\qquad\qquad\qquad\qquad \land\ proposal[t][j].phase = ProposalCommit \\
\qquad\qquad\qquad\qquad \land\ proposal[t][j].state\ \ = ProposalComplete
\end{array}
$$

```
        ∧ ∧ proposal[t][i].phase = ProposalApply
          ∧ proposal[t][i].state  = ProposalInProgress
          ⇒ ¬∃ j ∈ DOMAIN proposal[t] :
                ∧ j > i
                ∧ proposal[t][j].phase = ProposalApply
                ∧ proposal[t][j].state  = ProposalComplete

Consistency ≜
  ∀ t ∈ DOMAIN proposal :
    LET
        Compute the transaction indexes that have been applied to the target
      targetIndexes ≜ {i ∈ DOMAIN proposal[t] :
                          ∧ proposal[t][i].phase = ProposalApply
                          ∧ proposal[t][i].state  = ProposalComplete
                          ∧ ¬∃ j ∈ DOMAIN proposal[t] :
                                ∧ j > i
                                ∧ proposal[t][j].type = ProposalRollback
                                ∧ proposal[t][j].rollback.index = i
                                ∧ proposal[t][j].phase = ProposalApply
                                ∧ proposal[t][j].state  = ProposalComplete}
        Compute the set of paths in the target that have been updated by transactions
      appliedPaths ≜ UNION {DOMAIN proposal[t][i].change.values : i ∈ targetIndexes}
        Compute the highest index applied to the target for each path
      pathIndexes  ≜ [p ∈ appliedPaths ↦ CHOOSE i ∈ targetIndexes :
                                           ∀ j ∈ targetIndexes :
                                             ∧ i ≥ j
                                             ∧ p ∈ DOMAIN proposal[t][i].change.values]
        Compute the expected target configuration based on the last indexes applied
        to the target for each path.
      expectedConfig ≜ [p ∈ DOMAIN pathIndexes ↦ proposal[t][pathIndexes[p]].change.values[p]]
    IN
      target[t] = expectedConfig

Safety ≜ □(Order ∧ Consistency)

THEOREM Spec ⇒ Safety

Terminated(t, i) ≜
  ∧ i ∈ DOMAIN proposal[t]
  ∧ proposal[t][i].phase ∈ {ProposalApply, ProposalAbort}
  ∧ proposal[t][i].state  = ProposalComplete

Termination ≜
  ∀ t ∈ DOMAIN proposal :
    ∀ i ∈ 1 .. Len(proposal[t]) :
      Terminated(t, i)
```

$Liveness \triangleq \Diamond Termination$

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*