

EXTENDS

Northbound,
Proposal,
Configuration,
Mastership,
Southbound

INSTANCE *Naturals*

INSTANCE *FiniteSets*

INSTANCE *Sequences*

LOCAL INSTANCE *TLC*

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

Formal specification, constraints, and theorems.

Init \triangleq

\wedge *InitNorthbound*
 \wedge *InitProposal*
 \wedge *InitConfiguration*
 \wedge *InitMastership*
 \wedge *InitSouthbound*

Next \triangleq

$\vee \wedge$ *NextNorthbound*
 \wedge UNCHANGED $\langle \rangle$
 $\vee \wedge$ *NextProposal*
 \wedge UNCHANGED $\langle \rangle$
 $\vee \wedge$ *NextConfiguration*
 \wedge UNCHANGED $\langle \text{proposal} \rangle$
 $\vee \wedge$ *NextMastership*
 \wedge UNCHANGED $\langle \text{proposal}, \text{configuration} \rangle$
 $\vee \wedge$ *NextSouthbound*
 \wedge UNCHANGED $\langle \text{proposal}, \text{configuration}, \text{mastership} \rangle$

Spec \triangleq

\wedge *Init*
 $\wedge \Box[Next]_{vars}$
 $\wedge \forall i \in 1 \dots NumProposals : WF_{vars}(Change(i) \vee Rollback(i))$
 $\wedge \forall n \in Nodes, i \in 1 \dots NumProposals : WF_{vars}(ReconcileProposal(n, i))$
 $\wedge \forall n \in Nodes : WF_{\langle \text{configuration}, \text{mastership}, \text{node}, \text{target} \rangle}(ReconcileConfiguration(n))$
 $\wedge \forall n \in Nodes : WF_{\langle \text{mastership}, \text{node}, \text{target} \rangle}(ReconcileMastership(n))$

$$\begin{aligned}
& \wedge \forall n \in \text{Nodes} : \text{WF}_{\langle \text{node}, \text{target} \rangle}(\text{Connect}(n) \vee \text{Disconnect}(n)) \\
& \wedge \text{WF}_{\langle \text{target} \rangle}(\text{Start}) \\
& \wedge \text{WF}_{\langle \text{target} \rangle}(\text{Stop})
\end{aligned}$$

$\text{Order} \triangleq$

$$\begin{aligned}
& \forall i \in \text{DOMAIN } \text{proposal} : \\
& \quad \wedge \text{proposal}[i].\text{change.commit} \in \{\text{ProposalInProgress}, \text{ProposalAborted}\} \Rightarrow \\
& \quad \quad \neg \exists j \in \text{DOMAIN } \text{proposal} : \\
& \quad \quad \quad \wedge j < i \\
& \quad \quad \quad \wedge \text{proposal}[j].\text{change.commit} \in \{\text{ProposalPending}, \text{ProposalInProgress}\} \\
& \quad \wedge \text{proposal}[i].\text{change.commit} = \text{ProposalComplete} \Rightarrow \\
& \quad \quad \neg \exists j \in \text{DOMAIN } \text{proposal} : \\
& \quad \quad \quad \wedge j < i \\
& \quad \quad \quad \wedge \text{proposal}[j].\text{change.commit} \in \{\text{ProposalPending}, \text{ProposalInProgress}\} \\
& \quad \wedge \text{proposal}[i].\text{change.apply} \in \{\text{ProposalInProgress}, \text{ProposalAborted}\} \Rightarrow \\
& \quad \quad \neg \exists j \in \text{DOMAIN } \text{proposal} : \\
& \quad \quad \quad \wedge j < i \\
& \quad \quad \quad \wedge \vee \text{proposal}[j].\text{change.apply} \in \{\text{ProposalPending}, \text{ProposalInProgress}\} \\
& \quad \quad \quad \quad \vee \wedge \text{proposal}[j].\text{change.apply} = \text{ProposalFailed} \\
& \quad \quad \quad \quad \wedge \text{proposal}[j].\text{rollback.apply} \notin \text{ProposalDone} \\
& \quad \wedge \text{proposal}[i].\text{change.apply} = \text{ProposalComplete} \Rightarrow \\
& \quad \quad \neg \exists j \in \text{DOMAIN } \text{proposal} : \\
& \quad \quad \quad \wedge j < i \\
& \quad \quad \quad \wedge \vee \text{proposal}[j].\text{change.apply} \in \{\text{ProposalPending}, \text{ProposalInProgress}\} \\
& \quad \quad \quad \quad \vee \wedge \text{proposal}[j].\text{change.apply} = \text{ProposalFailed} \\
& \quad \quad \quad \quad \wedge \text{proposal}[j].\text{rollback.apply} \notin \text{ProposalDone} \\
& \quad \wedge \text{proposal}[i].\text{rollback.commit} = \text{ProposalInProgress} \Rightarrow \\
& \quad \quad \forall j \in \text{DOMAIN } \text{proposal} : j > i \wedge \text{proposal}[j].\text{phase} = \text{ProposalRollback} \Rightarrow \\
& \quad \quad \quad \text{proposal}[j].\text{change.commit} \in \text{ProposalDone}
\end{aligned}$$

$\text{Consistency} \triangleq$

$$\begin{aligned}
& \wedge \text{target.running} \\
& \wedge \text{configuration.status} = \text{ConfigurationComplete} \\
& \wedge \text{configuration.apply.target} = \text{target.incarnation} \\
& \Rightarrow \forall i \in \text{DOMAIN } \text{proposal} : \\
& \quad \wedge \text{proposal}[i].\text{change.apply} = \text{ProposalComplete} \\
& \quad \wedge \text{proposal}[i].\text{rollback.apply} \neq \text{ProposalComplete} \\
& \quad \Rightarrow \forall p \in \text{DOMAIN } \text{proposal}[i].\text{change.values} : \\
& \quad \quad \wedge \neg \exists j \in \text{DOMAIN } \text{proposal} : \\
& \quad \quad \quad \wedge j > i \\
& \quad \quad \quad \wedge \text{proposal}[i].\text{change.apply} = \text{ProposalComplete} \\
& \quad \quad \quad \wedge \text{proposal}[i].\text{rollback.apply} \neq \text{ProposalComplete} \\
& \quad \Rightarrow \wedge p \in \text{DOMAIN } \text{target.values} \\
& \quad \quad \wedge \text{target.values}[p].\text{value} = \text{proposal}[i].\text{change.values}[p].\text{value} \\
& \quad \quad \wedge \text{target.values}[p].\text{index} = \text{proposal}[i].\text{change.values}[p].\text{index}
\end{aligned}$$

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

THEOREM $Spec \Rightarrow Safety$

$Termination \triangleq$

$\forall i \in 1 \dots NumProposals :$
 $\wedge proposal[i].phase = ProposalChange \leadsto$
 $\wedge proposal[i].change.commit \in ProposalDone$
 $\wedge proposal[i].change.apply \in ProposalDone$
 $\wedge proposal[i].phase = ProposalRollback \leadsto$
 $\wedge proposal[i].rollback.commit \in ProposalDone$
 $\wedge proposal[i].rollback.apply \in ProposalDone$

$Liveness \triangleq Termination$

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*