MODULE *Config*

EXTENDS
Northbound,
Proposals,
Configurations,
Mastership,
Southbound,
Target

INSTANCE *Naturals*

INSTANCE *FiniteSets*

INSTANCE *Sequences*

LOCAL INSTANCE *TLC*

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

Formal specification, constraints, and theorems.

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

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

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

$Order \triangleq$

$\forall\, i \in \text{DOMAIN } proposal :$
$\land\ \land\ proposal[i].phase = ProposalCommit$
$\land\ proposal[i].state\ = ProposalInProgress$
$\Rightarrow \neg\exists\, j \in \text{DOMAIN } proposal :$
$\land\ j > i$
$\land\ proposal[j].phase = ProposalCommit$
$\land\ proposal[j].state\ = ProposalComplete$
$\land\ \land\ proposal[i].phase = ProposalApply$
$\land\ proposal[i].state\ = ProposalInProgress$
$\Rightarrow \neg\exists\, j \in \text{DOMAIN } proposal :$
$\land\ j > i$
$\land\ proposal[j].phase = ProposalApply$
$\land\ proposal[j].state\ = ProposalComplete$

$Consistency \triangleq$
LET
Compute the transaction indexes that have been applied to the target
$targetIndexes \triangleq \{i \in \text{DOMAIN } proposal :$
$\land\ proposal[i].phase = ProposalApply$
$\land\ proposal[i].state\ = ProposalComplete$
$\land\ \neg\exists\, j \in \text{DOMAIN } proposal :$
$\land\ j > i$
$\land\ proposal[j].type = ProposalRollback$
$\land\ proposal[j].rollback.index = i$
$\land\ proposal[j].phase = ProposalApply$
$\land\ proposal[j].state\ = ProposalComplete\}$
Compute the set of paths in the target that have been updated by transactions
$appliedPaths \triangleq \text{UNION } \{\text{DOMAIN } proposal[i].change.values : i \in targetIndexes\}$
Compute the highest index applied to the target for each path
$pathIndexes \triangleq [p \in appliedPaths \mapsto \text{CHOOSE } i \in targetIndexes :$
$\forall\, j \in targetIndexes :$
$\land\ i \geq j$
$\land\ p \in \text{DOMAIN } proposal[i].change.values]$
Compute the expected target configuration based on the last indexes applied
to the target for each path.
$expectedConfig \triangleq [p \in \text{DOMAIN } pathIndexes \mapsto proposal[pathIndexes[p]].change.values[p]]$
IN
$target = expectedConfig$

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

THEOREM $Spec \Rightarrow Safety$

$Terminated(i) \triangleq$
$\land\ i \in \text{DOMAIN } proposal$
$\land\ proposal[i].phase \in \{ProposalApply,\ ProposalAbort\}$

$\land\ proposal[i].state\ = ProposalComplete$

$Termination \triangleq$
$\forall\, i \in 1\,..\,Len(proposal) :$
$Terminated(i)$

$Liveness \triangleq \Diamond Termination$

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*