$\overline{\qquad\qquad}$ MODULE $Config$ $\overline{\qquad\qquad}$

EXTENDS
    $Northbound$,
    $Transactions$,
    $Proposals$,
    $Configurations$,
    $Southbound$

INSTANCE $Naturals$

INSTANCE $FiniteSets$

INSTANCE $Sequences$

LOCAL INSTANCE TLC

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

Formal specification, constraints, and theorems.

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

$Next \triangleq$
    $\lor\ \land\ NextTransaction$
       $\land$ UNCHANGED $\langle configuration,\ target,\ mastership \rangle$
    $\lor\ \land\ NextProposal$
       $\land$ UNCHANGED $\langle transaction \rangle$
    $\lor\ \land\ NextConfiguration$
       $\land$ UNCHANGED $\langle transaction,\ proposal \rangle$
    $\lor\ \land\ NextNorthbound$
       $\land$ UNCHANGED $\langle proposal,\ configuration,\ target,\ mastership \rangle$
    $\lor\ \land\ NextSouthbound$
       $\land$ UNCHANGED $\langle transaction,\ proposal,\ configuration \rangle$

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

$Order \triangleq$
    $\forall\ t \in$ DOMAIN $proposal :$
      $\forall\ i \in$ DOMAIN $proposal[t] :$
        $\land\ \land\ proposal[t][i].phase = ProposalCommit$
          $\land\ proposal[t][i].state\ \ = ProposalInProgress$

1

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

$Consistency \triangleq$
  $\forall\, t \in \text{DOMAIN } proposal :$
    LET

Compute the transaction indexes that have been applied to the target

$$targetIndexes \triangleq \{i \in \text{DOMAIN } transaction :$$
$$\land\, i \in \text{DOMAIN } proposal[t]$$
$$\land\, proposal[t][i].phase = ProposalApply$$
$$\land\, proposal[t][i].state\ = ProposalComplete$$
$$\land\, t \in \text{DOMAIN } transaction[i].targets$$
$$\land\, \neg\exists\, j \in \text{DOMAIN } transaction :$$
$$\land\, j > i$$
$$\land\, transaction[j].type = TransactionRollback$$
$$\land\, transaction[j].rollback = i$$
$$\land\, transaction[j].phase = TransactionApply$$
$$\land\, transaction[j].state\ = TransactionComplete\}$$

Compute the set of paths in the target that have been updated by transactions

$$appliedPaths \quad \triangleq \text{UNION } \{\text{DOMAIN } proposal[t][i].change.values : i \in targetIndexes\}$$

Compute the highest index applied to the target for each path

$$pathIndexes \quad \triangleq [p \in appliedPaths \mapsto \text{CHOOSE } i \in targetIndexes :$$
$$\forall\, j \in targetIndexes :$$
$$\land\, i \geq j$$
$$\land\, p \in \text{DOMAIN } proposal[t][i].change.values]$$

Compute the expected target configuration based on the last indexes applied to the target for each path.

$$expectedConfig \triangleq [p \in \text{DOMAIN } pathIndexes \mapsto proposal[t][pathIndexes[p]].change.values[p]]$$

    IN

      $target[t] = expectedConfig$

$Isolation \triangleq$
  $\forall\, i \in \text{DOMAIN } transaction :$
    $\land\ \land\, transaction[i].phase = TransactionCommit$
      $\land\, transaction[i].state\ = TransactionInProgress$
      $\land\, transaction[i].isolation = Serializable$
      $\Rightarrow \neg\exists\, j \in \text{DOMAIN } transaction :$

$$\land\ j > i$$
$$\land\ \text{DOMAIN } transaction[j].targets \cap \text{DOMAIN } transaction[i].targets \neq \{\}$$
$$\land\ transaction[j].phase = TransactionCommit$$
$$\land\ \land\ transaction[i].phase = TransactionApply$$
$$\quad\ \land\ transaction[i].state\ = TransactionInProgress$$
$$\quad\ \land\ transaction[i].isolation = Serializable$$
$$\quad\ \Rightarrow \neg\exists\, j \in \text{DOMAIN } transaction :$$
$$\qquad\ \land\ j > i$$
$$\qquad\ \land\ \text{DOMAIN } transaction[j].targets \cap \text{DOMAIN } transaction[i].targets \neq \{\}$$
$$\qquad\ \land\ transaction[j].phase = TransactionApply$$

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

THEOREM $Spec \Rightarrow Safety$

$Terminated(i)\ \triangleq$
$\quad \land\ i \in \text{DOMAIN } transaction$
$\quad \land\ transaction[i].phase \in \{TransactionApply,\ TransactionAbort\}$
$\quad \land\ transaction[i].state\ = TransactionComplete$

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

$Liveness\ \triangleq\ \Diamond Termination$

THEOREM $Spec \Rightarrow Liveness$

\ * Modification History
\ * Last modified *Mon Feb* 21 01:32:07 *PST* 2022 by *jordanhalterman*
\ * Created *Wed Sep* 22 13:22:32 *PDT* 2021 by *jordanhalterman*