```
┌──────────────────── MODULE TwoPhase ────────────────────┐

EXTENDS Sequences, Naturals, Integers

VARIABLES msgs, rmState, tmState, tmPrepared

vars ≜ ⟨msgs, rmState, tmState, tmPrepared⟩

RMs ≜ {"rm1", "rm2", "rm3", "rm4", "rm5", "rm6", "rm7", "rm8", "rm9"}

Message ≜
  [type : {"Prepared"}, theRM : RMs] ∪ [type : {"Commit", "Abort"}]


Init ≜
  ∧ msgs = {}
  ∧ rmState = [rm ∈ RMs ↦ "working"]
  ∧ tmState = "init"
  ∧ tmPrepared = {}

SndPrepare(rm) ≜
  ∧ msgs′ = msgs ∪ {[type ↦ "Prepared", theRM ↦ rm]}
  ∧ rmState[rm] = "working"
  ∧ rmState′ = [rmState EXCEPT ![rm] = "prepared"]
  ∧ UNCHANGED ⟨tmState, tmPrepared⟩

RcvPrepare(rm) ≜
  ∧ [type ↦ "Prepared", theRM ↦ rm] ∈ msgs
  ∧ tmState = "init"
  ∧ tmPrepared′ = tmPrepared ∪ {rm}
  ∧ UNCHANGED ⟨msgs, tmState, rmState⟩

SndCommit(rm) ≜
  ∧ msgs′ = msgs ∪ {[type ↦ "Commit"]}
  ∧ tmState ∈ {"init", "commmitted"}
  ∧ tmPrepared = RMs
  ∧ tmState′ = "committed"
  ∧ UNCHANGED ⟨tmPrepared, rmState⟩

RcvCommit(rm) ≜
  ∧ [type ↦ "Commit"] ∈ msgs
  ∧ rmState′ = [rmState EXCEPT ![rm] = "committed"]
  ∧ UNCHANGED ⟨msgs, tmState, tmPrepared⟩

SndAbort(rm) ≜
  ∧ msgs′ = msgs ∪ {[type ↦ "Abort"]}
  ∧ tmState ∈ {"init", "aborted"}
  ∧ tmState′ = "aborted"
  ∧ UNCHANGED ⟨tmPrepared, rmState⟩
```

```
$RcvAbort(rm) \triangleq$
   $\land [type \mapsto \text{“Abort”}] \in msgs$
   $\land rmState' = [rmState \text{ EXCEPT } ![rm] = \text{“aborted”}]$
   $\land \text{UNCHANGED } \langle msgs, tmState, tmPrepared \rangle$

$SilentAbort(rm) \triangleq$
   $\land rmState[rm] = \text{“working”}$
   $\land rmState' = [rmState \text{ EXCEPT } ![rm] = \text{“aborted”}]$
   $\land \text{UNCHANGED } \langle tmState, tmPrepared, msgs \rangle$


$Next \triangleq$
    $\exists rm \in RMs :$
        $\lor SndPrepare(rm)$
        $\lor RcvPrepare(rm)$
        $\lor SndCommit(rm)$
        $\lor RcvCommit(rm)$
        $\lor SndAbort(rm)$
        $\lor RcvAbort(rm)$
        $\lor SilentAbort(rm)$

$Spec \triangleq Init \land \Box[Next]_{vars}$

$TypeOK \triangleq$
   $\land msgs \in \text{SUBSET } Message$
   $\land rmState \in [RMs \rightarrow \{\text{“working”}, \text{“prepared”}, \text{“committed”}, \text{“aborted”}\}]$
   $\land tmState \in \{\text{“init”}, \text{“committed”}, \text{“aborted”}\}$
   $\land tmPrepared \in \text{SUBSET } RMs$

$Consistent \triangleq \forall rm1, rm2 \in RMs : \neg(rmState[rm1] = \text{“aborted”} \land rmState[rm2] = \text{“committed”})$
```