$\overline{\qquad\qquad\qquad}$ MODULE $Configurations$ $\overline{\qquad\qquad\qquad}$

EXTENDS $Mastership$

INSTANCE $Naturals$

INSTANCE $FiniteSets$

LOCAL INSTANCE TLC

Status constants
CONSTANTS
 $ConfigurationInProgress$,
 $ConfigurationComplete$,
 $ConfigurationFailed$

A record of per-target configurations
VARIABLE $configuration$

LOCAL $InitState \triangleq$
 $[configurations \mapsto configuration,$
 $\ targets \qquad\quad \mapsto target,$
 $\ masterships \quad\ \mapsto mastership]$

LOCAL $NextState \triangleq$
 $[configurations \mapsto configuration',$
 $\ targets \qquad\quad \mapsto target',$
 $\ masterships \quad\ \mapsto mastership']$

LOCAL $Trace \triangleq$ INSTANCE $Trace$ WITH
 $Module \quad\ \leftarrow$ "Configurations",
 $InitState \ \leftarrow InitState,$
 $NextState \leftarrow NextState$

This section models the Configuration reconciler.

$ReconcileConfiguration(n) \triangleq$
 $\wedge \ \vee \ \wedge configuration.state = ConfigurationInProgress$
   $\wedge mastership.term = configuration.committed.term$
   $\wedge mastership.master = n$
   $\wedge target' = [target \text{ EXCEPT } !.values = configuration.applied.values]$
   $\wedge configuration' = [configuration \text{ EXCEPT } !.applied.term = mastership.term,$
                $!.state \qquad\quad = ConfigurationComplete]$
 $\wedge$ UNCHANGED $\langle mastership, \ conn \rangle$

1

Formal specification, constraints, and theorems.

$InitConfiguration \triangleq$
$\quad \wedge \; configuration = [$
$\qquad state \;\; \mapsto ConfigurationInProgress,$
$\qquad index \qquad \mapsto 0,$
$\qquad committed \mapsto [$
$\qquad\quad index \;\; \mapsto 0,$
$\qquad\quad term \;\;\; \mapsto 0,$
$\qquad\quad values \;\; \mapsto [$
$\qquad\qquad path \in \{\} \mapsto [$
$\qquad\qquad\quad path \qquad \mapsto path,$
$\qquad\qquad\quad value \;\;\; \mapsto Nil,$
$\qquad\qquad\quad index \;\;\; \mapsto 0,$
$\qquad\qquad\quad deleted \mapsto \text{FALSE}]]],$
$\qquad proposed \;\; \mapsto [index \mapsto 0],$
$\qquad applied \qquad \mapsto [$
$\qquad\quad index \;\; \mapsto 0,$
$\qquad\quad term \;\;\; \mapsto 0,$
$\qquad\quad values \mapsto [$
$\qquad\qquad path \in \{\} \mapsto [$
$\qquad\qquad\quad path \qquad \mapsto path,$
$\qquad\qquad\quad value \;\;\; \mapsto Nil,$
$\qquad\qquad\quad index \;\;\; \mapsto 0,$
$\qquad\qquad\quad deleted \mapsto \text{FALSE}]]]]$
$\quad \wedge \; Trace!Init$

$NextConfiguration \triangleq$
$\quad \vee \; \exists \, n \in Node :$
$\qquad Trace!Step(ReconcileConfiguration(n),\, [node \mapsto n])$