```
┌──────────────────── MODULE Spec ────────────────────┐
EXTENDS TLC

CONSTANTS Namespace, Commit, Device

Nothing ≜ CHOOSE c : c ∉ Commit

VARIABLES namespaces, commits, devices, running, pending, staged

├─────────────────────────────────────────────────────┤

TypeOK ≜
  ∧ namespaces ⊆ Namespace
  ∧ commits    ⊆ namespaces × Commit
  ∧ devices    ⊆ namespaces × Device
  ∧ running   ∈ [devices → commits]
  ∧ pending   ∈ [devices → commits ∪ {Nothing}]
  ∧ staged    ∈ [devices → commits ∪ {Nothing}]

Init ≜
  ∧ namespaces = {}
  ∧ commits    = {}
  ∧ devices    = {}
  ∧ running    = [d ∈ {} ↦ {}]
  ∧ pending    = [d ∈ {} ↦ {}]
  ∧ staged     = [d ∈ {} ↦ {}]

├─────────────────────────────────────────────────────┤

CreateAccount ≜ ∃ ns ∈ Namespace :
  ∧ ns ∉ namespaces
  ∧ namespaces′ = namespaces ∪ {ns}
  ∧ UNCHANGED ⟨commits, devices, running, pending, staged⟩

Bitbake(ns) ≜ ∃ c ∈ Commit :
  ∧ ns ∈ namespaces
  ∧ commits′ = commits ∪ {⟨ns, c⟩}
  ∧ UNCHANGED ⟨namespaces, devices, running, pending, staged⟩

StartDevice(ns, c) ≜ ∃ d ∈ Device :
  ∧ ns         ∈ namespaces
  ∧ ⟨ns, c⟩    ∈ commits
  ∧ ⟨ns, d⟩    ∉ devices
  ∧ devices′  = devices ∪ {⟨ns, d⟩}
  ∧ running′ = running @@ ⟨ns, d⟩ :> ⟨ns, c⟩
  ∧ pending′ = pending @@ ⟨ns, d⟩ :> Nothing
  ∧ staged′   = staged  @@ ⟨ns, d⟩  :> Nothing
  ∧ UNCHANGED ⟨namespaces, commits⟩

ScheduleUpdate(ns, c, d) ≜
  ∧ ns          ∈ namespaces
  ∧ ⟨ns, c⟩     ∈ commits
  ∧ ⟨ns, d⟩     ∈ devices
  ∧ c ≠ running[⟨ns, d⟩]
  ∧ pending[⟨ns, d⟩] = Nothing
  ∧ pending′ = [pending EXCEPT ![⟨ns, d⟩] = ⟨ns, c⟩]
  ∧ UNCHANGED ⟨namespaces, commits, devices, running, staged⟩

PullUpdate(ns, d) ≜
  ∧ ns          ∈ namespaces
  ∧ ⟨ns, d⟩     ∈ devices
  ∧ LET p ≜ pending[⟨ns, d⟩]IN
    staged′   = IF p = Nothing
                THEN staged
                ELSE [staged EXCEPT ![⟨ns, d⟩] = p]
  ∧ pending′ = IF pending[⟨ns, d⟩] = Nothing
                THEN pending
                ELSE [pending EXCEPT ![⟨ns, d⟩] = Nothing]
  ∧ UNCHANGED ⟨namespaces, commits, devices, running⟩

RebootDevice(ns, d) ≜
 LET s ≜ staged[⟨ns, d⟩]IN
  ∧ ns          ∈ namespaces
  ∧ ⟨ns, d⟩     ∈ devices
  ∧ running′ = IF s = Nothing
                THEN running
                ELSE [running EXCEPT ![⟨ns, d⟩] = s]
  ∧ staged′   = IF s = Nothing
                THEN staged
                ELSE [staged EXCEPT ![⟨ns, d⟩] = Nothing]
  ∧ UNCHANGED ⟨namespaces, commits, devices, pending⟩

OstreeAdminStatus(ns, d) ≜ ∃ c ∈ Commit, pc ∈ Commit ∪ {Nothing} :
  ∧ ns          ∈ namespaces
  ∧ ⟨ns, d⟩     ∈ devices
  ∧ running[⟨ns, d⟩] = ⟨ns, c⟩
  ∧ pending[⟨ns, d⟩] = pc
  ∧ UNCHANGED ⟨namespaces, commits, devices, pending, running, staged⟩

Next ≜
  ∨ CreateAccount
  ∨ (∃ ns ∈ Namespace                          : Bitbake(ns))
```

$$\begin{array}{ll}
\lor\ (\exists\, \mathit{ns} \in \mathit{Namespace},\ c \in \mathit{Commit} & : \mathit{StartDevice}(\mathit{ns},\ c))\\
\lor\ (\exists\, \mathit{ns} \in \mathit{Namespace},\ c \in \mathit{Commit},\ d \in \mathit{Device} & : \mathit{ScheduleUpdate}(\mathit{ns},\ c,\ d))\\
\lor\ (\exists\, \mathit{ns} \in \mathit{Namespace},\ d \in \mathit{Device} & : \mathit{PullUpdate}(\mathit{ns},\ d))\\
\lor\ (\exists\, \mathit{ns} \in \mathit{Namespace},\ d \in \mathit{Device} & : \mathit{RebootDevice}(\mathit{ns},\ d))\\
\lor\ (\exists\, \mathit{ns} \in \mathit{Namespace},\ d \in \mathit{Device} & : \mathit{OstreeAdminStatus}(\mathit{ns},\ d))
\end{array}$$

$$\begin{array}{l}
\mathit{RunningOK}\ \triangleq\\
\quad \forall\, \langle \mathit{ns},\ d\rangle \in \textsc{domain}\ \mathit{running} : \exists\, c \in \mathit{Commit} :\\
\qquad \mathit{running}[\langle \mathit{ns},\ d\rangle] = \langle \mathit{ns},\ c\rangle
\end{array}$$

$$\begin{array}{l}
\mathit{PendingOK}\ \triangleq\\
\quad \forall\, \langle \mathit{ns},\ d\rangle \in \textsc{domain}\ \mathit{pending} : \exists\, c \in \mathit{Commit} :\\
\qquad \lor\ \mathit{pending}[\langle \mathit{ns},\ d\rangle] = \langle \mathit{ns},\ c\rangle\\
\qquad \lor\ \mathit{pending}[\langle \mathit{ns},\ d\rangle] = \mathit{Nothing}
\end{array}$$

$$\begin{array}{l}
\mathit{StagedOK}\ \triangleq\\
\quad \forall\, \langle \mathit{ns},\ d\rangle \in \textsc{domain}\ \mathit{staged} : \exists\, c \in \mathit{Commit} :\\
\qquad \lor\ \mathit{staged}[\langle \mathit{ns},\ d\rangle] = \langle \mathit{ns},\ c\rangle\\
\qquad \lor\ \mathit{staged}[\langle \mathit{ns},\ d\rangle] = \mathit{Nothing}
\end{array}$$

$$\begin{array}{l}
\mathit{Inv}\ \triangleq\\
\quad \land\ \mathit{TypeOK}\\
\quad \land\ \mathit{RunningOK}\\
\quad \land\ \mathit{PendingOK}\\
\quad \land\ \mathit{StagedOK}
\end{array}$$

$$\mathit{vars}\ \triangleq\ \langle \mathit{namespaces},\ \mathit{commits},\ \mathit{devices},\ \mathit{running},\ \mathit{pending},\ \mathit{staged}\rangle$$

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