MODULE *AuthAssign*

EXTENDS *TLC*, *Naturals*

CONSTANT *User*, *nil*

VARIABLES *db_assign*,
want_assign, *want_changes*,
disk_assign,
pc, *local_wanted*, *local_user*, *num_downtime*

$max\_want\_changes \triangleq 10$

$max\_down\_times \triangleq 3$

$NullUser \triangleq User \cup \{nil\}$

$want\_vars \triangleq \langle want\_assign, want\_changes \rangle$
$job\_vars \triangleq \langle pc, local\_wanted, local\_user, num\_downtime \rangle$

$vars \triangleq \langle db\_assign, want\_vars, disk\_assign, job\_vars \rangle$

$DBStatus \triangleq \{\text{"null"}, \text{"handling"}, \text{"added"}\}$

$DiskStatus \triangleq \{\text{"active"}, \text{"null"}\}$

$TypeOK \triangleq$
- $db\_assign \in [User \to DBStatus]$
- $want\_assign \subseteq User$
- $want\_changes \in 0 \,..\, max\_want\_changes$
- $disk\_assign \in [User \to DiskStatus]$
- $pc \in \{\text{"Init"}, \text{"ReadDB"}, \text{"AssignPerm"}, \text{"RemovePerm"}, \text{"UpdateDB"}\}$
- $local\_wanted \in$ BOOLEAN
- $local\_user \in NullUser$
- $num\_downtime \in 0 \,..\, max\_down\_times$

$Init \triangleq$
- $db\_assign = [u \in User \mapsto \text{"null"}]$
- $want\_assign = \{\}$
- $want\_changes = 0$
- $disk\_assign = [u \in User \mapsto \text{"null"}]$
- $pc = \text{"Init"}$
- $local\_wanted =$ FALSE
- $local\_user = nil$
- $num\_downtime = 0$

$incWantChanges \triangleq$
- $want\_changes < max\_want\_changes$

$\land\ want\_changes' = want\_changes + 1$

$AddWanted(u) \triangleq$
$\land\ \neg(u \in want\_assign)$
$\land\ incWantChanges$
$\land\ want\_assign' = want\_assign \cup \{u\}$
$\land$ UNCHANGED $\langle db\_assign,\ disk\_assign \rangle$
$\land$ UNCHANGED job_vars

$RemoveWanted(u) \triangleq$
$\land\ u \in want\_assign$
$\land\ incWantChanges$
$\land\ want\_assign' = want\_assign \setminus \{u\}$
$\land$ UNCHANGED $\langle db\_assign,\ disk\_assign \rangle$
$\land$ UNCHANGED job_vars

$noDifferenceForUser(u) \triangleq$
IF $u \in want\_assign$
THEN $db\_assign[u] =$ "added"
ELSE $db\_assign[u] =$ "null"

$noDifferenceBetweenWantedAndDB \triangleq$
$\forall\, u \in User : noDifferenceForUser(u)$

$GetFromWanted(u) \triangleq$
$\land\ pc =$ "Init"
$\land\ \lor \neg noDifferenceForUser(u)$ enable if there is a difference
$\lor\ db\_assign[u] =$ "handling"
$\land\ pc' =$ "ReadDB"
$\land\ local\_user' = u$
$\land\ local\_wanted' = (u \in want\_assign)$
$\land$ UNCHANGED $num\_downtime$
$\land$ UNCHANGED $want\_vars$
$\land$ UNCHANGED db_assign
$\land$ UNCHANGED $disk\_assign$

$resetToInit \triangleq$
$\land\ pc' =$ "Init"
$\land\ local\_user' = nil$
$\land\ local\_wanted' =$ FALSE

$setDBHandling \triangleq$

$\land\ db\_assign' = [db\_assign \text{ EXCEPT } ![local\_user] = \text{“handling”}]$

$getFromDBHandleWanted \triangleq$
IF $db\_assign[local\_user] \in \{\text{“null”}, \text{“handling”}\}$
THEN
$\land\ pc' = \text{“AssignPerm”}$
$\land\ setDBHandling$
$\land$ UNCHANGED $\langle local\_user, local\_wanted\rangle$
ELSE
$\land\ resetToInit$
$\land$ UNCHANGED db_assign

$getFromDBHandleNotWanted \triangleq$
IF $db\_assign[local\_user] \in \{\text{“added”}, \text{“handling”}\}$
THEN
$\land\ pc' = \text{“RemovePerm”}$
$\land\ setDBHandling$
$\land$ UNCHANGED $\langle local\_user, local\_wanted\rangle$
ELSE
$\land\ resetToInit$
$\land$ UNCHANGED db_assign

$GetFromDB \triangleq$
$\land\ pc = \text{“ReadDB”}$
$\land$ IF $local\_wanted$
THEN $getFromDBHandleWanted$
ELSE $getFromDBHandleNotWanted$
$\land$ UNCHANGED $num\_downtime$
$\land$ UNCHANGED $want\_vars$
$\land$ UNCHANGED $disk\_assign$

$AssignPerm \triangleq$
$\land\ pc = \text{“AssignPerm”}$
$\land\ pc' = \text{“UpdateDB”}$
$\land\ disk\_assign' = [disk\_assign \text{ EXCEPT } ![local\_user] = \text{“active”}]$
$\land$ UNCHANGED $\langle local\_user, local\_wanted\rangle$
$\land$ UNCHANGED $num\_downtime$
$\land$ UNCHANGED $want\_vars$
$\land$ UNCHANGED db_assign

$RemovePerm \triangleq$
$\land\ pc = \text{“RemovePerm”}$
$\land\ pc' = \text{“UpdateDB”}$

$\land\ disk\_assign' = [disk\_assign \text{ EXCEPT } ![local\_user] = \text{“null”}]$ delete
$\land$ UNCHANGED $\langle local\_user, local\_wanted \rangle$
$\land$ UNCHANGED $num\_downtime$
$\land$ UNCHANGED $want\_vars$
$\land$ UNCHANGED db_assign

$UpdateDB \triangleq$
$\land\ pc = \text{“UpdateDB”}$
$\land$ IF $local\_wanted$
THEN $db\_assign' = [db\_assign \text{ EXCEPT } ![local\_user] = \text{“added”}]$
ELSE $db\_assign' = [db\_assign \text{ EXCEPT } ![local\_user] = \text{“null”}]$
$\land\ resetToInit$
$\land$ UNCHANGED $num\_downtime$
$\land$ UNCHANGED $disk\_assign$
$\land$ UNCHANGED $want\_vars$

$DownTime \triangleq$
$\land\ num\_downtime < max\_down\_times$
$\land\ num\_downtime' = num\_downtime + 1$
$\land\ pc \neq \text{“Init”}$
$\land\ resetToInit$
$\land$ UNCHANGED $\langle want\_assign, db\_assign, disk\_assign \rangle$
$\land$ UNCHANGED $want\_changes$

$TerminateCond \triangleq$
$\land\ want\_changes = max\_want\_changes$
$\land\ pc = \text{“Init”}$
$\land\ noDifferenceBetweenWantedAndDB$
$\land\ \forall\, u \in User : db\_assign[u] \neq \text{“handling”}$

$Terminated \triangleq$
$\land\ TerminateCond$
$\land$ UNCHANGED $vars$

$Next \triangleq$
$\lor\ \exists\, u \in User :$
$\lor\ AddWanted(u)$
$\lor\ RemoveWanted(u)$
$\lor\ GetFromWanted(u)$
$\lor\ GetFromDB$
$\lor\ AssignPerm$
$\lor\ RemovePerm$
$\lor\ UpdateDB$
$\lor\ DownTime$

$\lor\ Terminated$

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

$FairSpec \triangleq Spec \land \mathrm{WF}_{vars}(Next)$

$AlwaysTerminate \triangleq \Diamond TerminateCond$

$ResetFully \triangleq$
$pc = \text{“Init”} \Rightarrow$
$\land\ local\_user = nil$
$\land\ local\_wanted = \text{FALSE}$

$noDifferenceBetweenWantedAndDisk(u) \triangleq$
IF $u \in want\_assign$
THEN $disk\_assign[u] = \text{“active”}$
ELSE $disk\_assign[u] = \text{“null”}$

$Inv \triangleq$
$TerminateCond \Rightarrow$
$\land \forall\ u \in User : noDifferenceBetweenWantedAndDisk(u)$