MODULE *IdemProxy*

Expectations :
- Every request must be hit the server exactly once
- For each try of a request, the response must be the same
- 2 requests must be processable in parallel

EXTENDS *Integers*, *FiniteSets*, *Sequences*

CONSTANTS
_ReqIDs, the request *IDs* sent by the user (an *Id* is the idempotent key)
_MaxTries how many times a request is retried

ASSUME $\_MaxTries < 10$

VARIABLES
requests the state of all requests and their corresponding tries

$vars \triangleq \langle requests \rangle$

tryKeys is a simple helper providing the set of try keys
$tryKeys \triangleq 1 \,..\, \_MaxTries$

Initial State

$Init \triangleq$
requests is a struct with *_ReqIDs* as keys associated with structs with *tryKeys* as keys associatied with the given try current status
$\land\ requests = [req \in \_ReqIDs \mapsto [st \in tryKeys \mapsto \text{“pending”}]]$

$TypeInvariants \triangleq$
$\land$ TRUE todo

Actions

$HitProxy(r,\ i) \triangleq$
$\land\ requests[r][i] = \text{“pending”}$
$\land\ requests' = [requests \text{ EXCEPT } ![r][i] = \text{“submitted”}]$

$HitServer(r,\ i) \triangleq$
$\land\ requests[r][i] = \text{“submitted”}$
$\land\ Cardinality(\{x \in \text{DOMAIN } requests[r] : requests[r][x] = \text{“processed”}\}) = 0$ add a blocking thread
$\land\ requests' = [requests \text{ EXCEPT } ![r][i] = \text{“processed”}]$

Spec

$Next \triangleq$

$\lor \exists\, r \in \_ReqIDs,\, i \in tryKeys :$
$\quad \lor HitProxy(r,\, i)$
$\quad \lor HitServer(r,\, i)$

$Fairness \triangleq \forall\, r \in \_ReqIDs,\, i \in tryKeys :$
$\qquad \land \mathrm{SF}_{vars}(HitServer(r,\, i))$
$\qquad \land \mathrm{SF}_{vars}(HitProxy(r,\, i))$

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

$RequestIsProcessedOnlyOnce \triangleq$
$\quad \Box(\forall\, req \in \text{DOMAIN } requests :$
$\qquad Cardinality(\{x \in \text{DOMAIN } requests[req] : requests[req][x] = \text{“processed”}\}) < 2)$

THEOREM $Spec \Rightarrow RequestIsProcessedOnlyOnce$