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 tries / requests must be processable in parallel

EXTENDS $\mathit{Integers}$, $\mathit{FiniteSets}$

CONSTANTS

$\quad \_\mathit{ReqIDs},$ the request IDs sent by the user (an Id is the idempotent key)

$\quad \_\mathit{MaxTries},$

$\quad \mathit{NULL}$

ASSUME $\_\mathit{MaxTries} < 10$

VARIABLES

$\quad \mathit{reqTriesCount},$ the different tries of specific $\_\mathit{Requests}$

$\quad \mathit{hits},$ the number of hits of the "protected" backend per requests

$\quad \mathit{tries},$ a specific real

$\quad \mathit{responses}$ the responses received by the client for each try

$\mathit{vars} \triangleq \langle \mathit{tries}, \mathit{reqTriesCount}, \mathit{hits}, \mathit{responses} \rangle$

Initial State

$\mathit{Init} \triangleq$

$\quad \land \mathit{reqTriesCount} = [r \in \_\mathit{ReqIDs} \mapsto 0]$

$\quad \land \mathit{tries} = [r \in \_\mathit{ReqIDs} \mapsto [\mathit{id} \mapsto 0, \mathit{status} \mapsto \text{"not submitted"}]]$

$\quad \land \mathit{hits} = [r \in \_\mathit{ReqIDs} \mapsto 0]$

$\quad \land \mathit{responses} = \langle \rangle$

$\mathit{TypeInvariants} \triangleq$

$\quad \land$ TRUE todo

Actions

$\mathit{Submit}(r) \triangleq$

$\quad \land \mathit{reqTriesCount}[r] < \_\mathit{MaxTries}$

$\quad \land \mathit{reqTriesCount}' = [\mathit{reqTriesCount} \text{ EXCEPT } ![r] = \mathit{reqTriesCount}[r] + 1]$

$\quad \land \mathit{tries}' = [\mathit{tries} \text{ EXCEPT } ![r].\mathit{id} = \mathit{reqTriesCount}[r] + 1, ![r].\mathit{status} = \text{"submitted"}]$

$\quad \land \text{UNCHANGED } \langle \mathit{hits}, \mathit{responses} \rangle$

Spec

$\mathit{Next} \triangleq$

$\quad \lor \exists\, r \in \_\mathit{ReqIDs} :$

$\qquad \lor \mathit{Submit}(r)$

$\mathit{Spec} \triangleq$

$\land \; \mathit{Init}$
$\land \; \Box[\mathit{Next}]_{\mathit{vars}}$