MODULE *ORSet*

EXTENDS *Naturals*, *Sequences*, *Bags*, *TLC*, *SEC*

CONSTANTS
Data the set of data

$Instance \triangleq [d : Data, r : Replica, k : Nat]$

VARIABLES
sSet, *sSet*[*r*]: set of active *Instance*(*s*) maintained by $r \in Replica$
seq, *seq*[*r*]: local sequence number at replica $r \in Replica$

Network variables

incoming, *incoming*[*r*]: incoming messages at replica $r \in Replica$
msg,
messageset

$vars \triangleq \langle sSet, seq, incoming, msg, messageset, SECvars \rangle$

$Msg \triangleq [r : Replica, update : \text{SUBSET } Update, seq : Nat, S : \text{SUBSET } Instance]$

$Network \triangleq \text{INSTANCE } ReliableNetwork$

$TypeOK \triangleq$
$\land \quad sSet \in [Replica \to \text{SUBSET } Instance]$
$\land \quad seq \in [Replica \to Nat]$

$Init \triangleq$
$\land\ seq = [r \in Replica \mapsto 0]$
$\land\ sSet = [r \in Replica \mapsto \{\}]$
$\land\ incoming = [r \in Replica \mapsto \langle\rangle]$
$\land\ Network\,!\,RInit$
$\land\ SECInit$

$Add(d, r) \triangleq$
$\land\ seq' = [seq \text{ EXCEPT } ![r] = @ + 1]$
$\land\ SECUpdate(r, seq[r])$
$\land\ sSet' = [sSet \text{ EXCEPT } ![r] = @ \cup \{[d \mapsto d, r \mapsto r, k \mapsto seq'[r]]\}]$
$\land\ \text{UNCHANGED } \langle incoming, msg, messageset \rangle$

$Remove(d, r) \triangleq$
$\land\ seq' = [seq \text{ EXCEPT } ![r] = @ + 1]$
$\land\ SECUpdate(r, seq[r])$
$\land\ \text{LET } D \triangleq \{ins \in sSet[r] : ins.d = d\}$

$\quad$ IN $\quad sSet' = [sSet$ EXCEPT $![r] = @ \setminus D]$
$\land$ UNCHANGED $\langle incoming,\ msg,\ messageset \rangle$

$Broadcast(s,\ m) \triangleq$
$[r \in Replica \mapsto$ IF $s = r$ THEN $incoming[s]$
ELSE $incoming[r] \oplus SetToBag(\{m\})]$

$Send(r) \triangleq$
$\land\ Network!RBroadcast(r,\ [r \mapsto r,\ seq \mapsto seq[r],\ update \mapsto OpUpdate(r),\ S \mapsto sSet[r]])$
$\land\ SECSend(r)$
$\land$ UNCHANGED $\langle sSet,\ seq,\ sSet \rangle$

$Receive(r) \triangleq$
$\land\ \ Network!RDeliver(r)$
$\land\ \ SECDeliver(r,\ msg'[r])$
$\land\ \ sSet' = [sSet$ EXCEPT $![r] = @ \cup msg'[r].S]$
$\land\ \ $ UNCHANGED $\langle seq \rangle$

$Next \triangleq$
$\lor \exists\, r \in Replica : \exists\, a \in Data :$
$\quad Add(a,\ r) \lor Remove(a,\ r)$
$\lor \exists\, r \in Replica :$
$\quad Send(r) \lor Receive(r)$

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

$Read(r) \triangleq \{ins.d : ins \in sSet[r]\}$

QC: Quiescent Consistency
$Quiescence \triangleq$
$\forall\, r \in Replica : incoming[r] = \langle\rangle$

$Convergence \triangleq$
$\forall\, r,\ s \in Replica : Read(r) = Read(s)$

$QC \triangleq Quiescence \Rightarrow Convergence$

SEC: Strong Eventual Consistency
$SEC \triangleq \forall\, r1,\ r2 \in Replica :$
$\quad Sameupdate(r1,\ r2) \Rightarrow Read(r1) = Read(r2)$

---

* Modification History
* Last modified Sun May 12 15:10:13 *CST* 2019 by *zfwang*
* Created *Wed Feb* 27 17:23:32 *CST* 2019 by *zfwang*