MODULE *spec*

High level description of a system persisting messages in two distinct databases

the set of all possible messages
CONSTANT $Message$

VARIABLE $db1$
VARIABLE $db2$

the tuple of all variables
$vars \triangleq \langle db1, db2 \rangle$

one message chosen as default value
$default \triangleq$ CHOOSE $m \in Message$: TRUE

$TypeOK \triangleq$
$\quad \wedge \quad db1 \in Message$
$\quad \wedge \quad db2 \in Message$

$Init \triangleq$
$\quad \wedge\, db1 = default$
$\quad \wedge\, db2 = default$

the first consumer step is to persist a received message in the first database
$Write1 \triangleq \exists\, m \in Message \setminus \{default\}$:
$\quad \wedge \quad db1' = m$
$\quad \wedge$ UNCHANGED $db2$

the second consumer step is to align the second database
$Write2 \triangleq$
$\quad \wedge \quad db2' = db1$
$\quad \wedge$ UNCHANGED $db1$

$Next \triangleq$
$\quad \vee\, Write1$
$\quad \vee\, Write2$

the second step must eventally occur in order to guarantee the consistency of the two databases
$Liveness \triangleq \mathrm{WF}_{vars}(Write2)$

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

in every state (always) the two database values are (or eventually will be) the same
$DbConsistency \triangleq \Box\Diamond(db2 = db1)$