MODULE *Agent*

Reliable Interface to *GPT* via *Gmail*

EXTENDS *FiniteSets*, *Naturals*, *Sequences*, *TLC*

CONSTANTS *Emails* — Set of incoming *Emails*

VARIABLES
Archived, — Set of archived *Emails*
Arrived, — Queue of incoming *Emails*
Completed, — Queue of completion responses
RemoteOutbox, — Set of outgoing *Emails*
Queued, — Set of parsed *Emails*
Abandoned — Set of failed *Emails*

$vars \triangleq \langle Abandoned, Archived, Arrived, Completed, Queued, RemoteOutbox \rangle$

$EmailsInQueue \triangleq Abandoned \cup Archived \cup Arrived \cup Completed \cup Queued$

$$
\begin{aligned}
TypeOK \triangleq \quad & \land Abandoned \subseteq Emails \\
& \land Archived \subseteq Emails \\
& \land Arrived \subseteq Emails \\
& \land Completed \subseteq Emails \\
& \land Queued \subseteq Emails \\
& \land RemoteOutbox \in Seq(Emails)
\end{aligned}
$$

$Range(S) \triangleq \{S[n] : n \in \text{DOMAIN } S\}$

$Invariants \triangleq$

$\land \forall email \in Completed : email \notin Queued \Rightarrow email \notin Arrived$

Don't parse e-mails more than once.

$\land \forall email \in Range(RemoteOutbox) : email \notin Completed \Rightarrow email \notin Queued$

Don't complete e-mails more than once.

$\land \forall email \in Abandoned : email \notin Arrived \cup Completed \cup Queued$

Abandoned e-mails not to appear anywhere else, as *Abandoned* is a general queue state separate from e-mail processing state.

$\land \forall email \in Archived : email \notin Arrived \cup Completed \cup Queued$

Same with archived emails.

$\land Len(RemoteOutbox) = Cardinality(Range(RemoteOutbox))$

Don't send e-mails more than once.

$ReceiveEmailOK(email) \triangleq$

Enqueues an *Email* from *Inbox* to *Arrived*.

$\land\ Arrived' = Arrived \cup \{email\}$
$\land$ UNCHANGED $\langle Abandoned,\ Archived,\ Completed,\ Queued,\ RemoteOutbox\rangle$

$ReceiveEmailError(email) \triangleq$

Fails reading an *email* from *Inbox*. Logs it, marks it and moves it to *RemoteArchived* folder. Support engineer can move the *email* back to *Inbox* after addressing the issue.

$\land\ Abandoned' = Abandoned \cup \{email\}$
$\land$ UNCHANGED $\langle Archived,\ Arrived,\ Completed,\ Queued,\ RemoteOutbox\rangle$

$ReceiveEmail \triangleq \land \exists\, email \in Emails \setminus EmailsInQueue :$
$\lor\ ReceiveEmailOK(email)$
$\lor\ ReceiveEmailError(email)$

$PrepareEmail1OK(email) \triangleq$

The first step of preparing an e-mail for completion is to parse the e-mail and update its status as *Queued*. It then places the parsed message in the queue. Thus there are two forms of the same e-mail in the queue at this point. This is an atomic operation.

$\land\ email \notin Queued$
$\land\ Queued' = Queued \cup \{email\}$
$\land$ UNCHANGED $\langle Abandoned,\ Archived,\ Arrived,\ Completed,\ RemoteOutbox\rangle$

$PrepareEmail2OK(email) \triangleq$

The second step of preparing removes the e-mail response from the Arrival queue only after the parsing is successful. This ensures we don't lose any e-mails in case of a failure.

$\land\ email \in Queued$
$\land\ Arrived' = Arrived \setminus \{email\}$
$\land$ UNCHANGED $\langle Abandoned,\ Archived,\ Completed,\ Queued,\ RemoteOutbox\rangle$

$PrepareEmailOK(email) \triangleq$

Prepares an *email* for completion. The sub-operations occur over distributed settings and may fail. Each sub-operation is atomic, and their order of execution is important.

$\lor\ PrepareEmail1OK(email)$
$\lor\ PrepareEmail2OK(email)$

$PrepareEmail1Error(email) \triangleq$

Fails preparing an *email*.

$\land\ email \notin Queued$
$\land\ Abandoned' = Abandoned \cup \{email\}$
$\land\ Arrived' = Arrived \setminus \{email\}$
$\land$ UNCHANGED $\langle Archived,\ Completed,\ Queued,\ RemoteOutbox\rangle$

$PrepareEmail \triangleq$

$\exists\, email \in Arrived \setminus Abandoned :$
$\lor\ PrepareEmailOK(email)$
$\lor\ PrepareEmail1Error(email)$

$CompleteMessage1OK(email) \triangleq$
$\land\ email \notin Completed$
$\land\ Completed' = Completed \cup \{email\}$
$\land$ UNCHANGED $\langle Abandoned,\ Archived,\ Arrived,\ Queued,\ RemoteOutbox\rangle$

$CompleteMessage2OK(email) \triangleq$
$\land\ email \in Completed$
$\land\ Queued' = Queued \setminus \{email\}$
$\land$ UNCHANGED $\langle Abandoned,\ Archived,\ Arrived,\ Completed,\ RemoteOutbox\rangle$

$CompleteMessageOK(email) \triangleq$
$\lor\ CompleteMessage1OK(email)$
$\lor\ CompleteMessage2OK(email)$

$CompleteMessage1Error(email) \triangleq$
$\land\ email \notin Completed$
$\land\ Abandoned' = Abandoned \cup \{email\}$
$\land\ Queued' = Queued \setminus \{email\}$
$\land$ UNCHANGED $\langle Archived,\ Arrived,\ Completed,\ RemoteOutbox\rangle$

$CompleteMessage \triangleq$
$\exists\, email \in Queued \setminus (Arrived \cup Abandoned) :$
$\lor\ CompleteMessageOK(email)$
$\lor\ CompleteMessage1Error(email)$

$SendOutCompletion1OK(email) \triangleq$
Sends out a completion response e-mail.
$\land\ email \notin Range(RemoteOutbox)$ We haven't already sent this e-mail
$\land\ RemoteOutbox' = Append(RemoteOutbox,\ email)$
$\land$ UNCHANGED $\langle Abandoned,\ Archived,\ Arrived,\ Completed,\ Queued\rangle$

$SendOutCompletion2OK(email) \triangleq$
Marks an *email* as sent.
$\land\ email \in Range(RemoteOutbox)$ Previous step to send this e-mail succeeded.
$\land\ Archived' = Archived \cup \{email\}$
$\land\ Completed' = Completed \setminus \{email\}$
$\land$ UNCHANGED $\langle Abandoned,\ Arrived,\ Queued,\ RemoteOutbox\rangle$

$SendOutCompletion1Error(email) \triangleq$
Fails sending the e-mail.
$\land\ email \notin Range(RemoteOutbox)$ We haven't already sent this e-mail
$\land\ Abandoned' = Abandoned \cup \{email\}$

$\land\ Completed' = Completed \setminus \{email\}$
$\land$ UNCHANGED $\langle Archived,\ Arrived,\ Queued,\ RemoteOutbox\rangle$

$SendOutCompletion \triangleq$
$\exists\, email \in Completed \setminus (Abandoned \cup Queued) :$
$\lor\ SendOutCompletion1OK(email)$
$\lor\ SendOutCompletion2OK(email)$
$\lor\ SendOutCompletion1Error(email)$

$AllDone \triangleq$
All done and system comes to equilibrium.
$\land\ Archived \cup Abandoned = Emails$
$\land\ Queued \setminus Abandoned = \{\}$
$\land$ UNCHANGED $vars$

$Init \triangleq \land\ Abandoned = \{\}$
$\land\ Archived = \{\}$
$\land\ Arrived = \{\}$
$\land\ Completed = \{\}$
$\land\ Queued = \{\}$
$\land\ RemoteOutbox = \langle\rangle$

$Next \triangleq \lor\ ReceiveEmail$
$\lor\ PrepareEmail$
$\lor\ CompleteMessage$
$\lor\ SendOutCompletion$
$\lor\ AllDone$

$Spec \triangleq Init \land \Box[Next]_{vars} \land \mathrm{WF}_{vars}(Next)$

Temporal properties for verification

$NoLostEmails \triangleq$
No e-mails should be lost. This is a safety property.
$\forall\, email \in Emails :$
$\Box(email \in EmailsInQueue \Rightarrow \Diamond\Box(email \in Abandoned \cup Range(RemoteOutbox)))$

THEOREM $Spec \Rightarrow \Box TypeOK$
THEOREM $Spec \Rightarrow \Box Invariants$
THEOREM $Spec \Rightarrow NoLostEmails$

* Modification History
* Last modified *Wed* May 10 14:00:01 *KST* 2023 by *hcs*
* Created *Fri Apr* 28 13:04:37 *KST* 2023 by *hcs*