simpleSpacecraft

Tight Rope v0.6

September 27, 2015

1 Network

section *NetworkChannels* **parents** *scj_prelude*, *MissionId*, *MissionIds*,
SchedulableId, *SchedulableIds*, *MissionChan*, *SchedulableChan*, *TopLevelMissionSequencerFWChan*,
FrameworkChan, *SafeletChan*

channelset *TerminateSync* ==
⦃ *schedulables_terminated*, *schedulables_stopped*, *get_activeSchedulables* ⦄

channelset *ControlTierSync* ==
⦃ *start_toplevel_sequencer*, *done_toplevel_sequencer*, *done_safeletFW* ⦄

channelset *TierSync* ==
⦃ *start_mission* ., *done_mission* .,
done_safeletFW, *done_toplevel_sequencer* ⦄

channelset *MissionSync* ==
⦃ *done_safeletFW*, *done_toplevel_sequencer*, *register*,
signalTerminationCall, *signalTerminationRet*, *activate_schedulables*, *done_schedulable*,
cleanupSchedulableCall, *cleanupSchedulableRet* ⦄

channelset *SchedulablesSync* ==
⦃ *activate_schedulables*, *done_safeletFW*, *done_toplevel_sequencer* ⦄

channelset *ClusterSync* ==
⦃ *done_toplevel_sequencer*, *done_safeletFW* ⦄

channelset *AppSync* ==
⋃{*SafeltAppSync*, *MissionSequencerAppSync*, *MissionAppSync*,
MTAppSync, *OSEHSync*, *APEHSync*,
⦃ *getSequencer*, *end_mission_app*, *end_managedThread_app*,
setCeilingPriority, *requestTerminationCall*, *requestTerminationRet*, *terminationPendingCall*,
terminationPendingRet, *handleAsyncEventCall*, *handleAsyncEventRet* ⦄}

channelset *ObjectSync* ==
⦃ ⦄

channelset *ThreadSync* ==
⦃ ⦄

channelset *LockingSync* ==
⦃ *lockAcquired*, *startSyncMeth*, *endSyncMeth*, *waitCall*, *waitRet*, *notify* ⦄

section *Program* **parents** *scj_prelude*, *MissionId*, *MissionIds*,
SchedulableId, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *MissionFW*,
SafeletFW, *TopLevelMissionSequencerFW*, *NetworkChannels*, *ManagedThreadFW*,
SchedulableMissionSequencerFW, *PeriodicEventHandlerFW*, *OneShotEventHandlerFW*,
AperiodicEventHandlerFW, *SPSafeletApp*, *MainMissionSequencerApp*,
ObjectFW, *ThreadFW*, *MainMissionApp*,

$$\mathbf{process}\ ControlTier \mathrel{\widehat=} \left(\begin{array}{l} SafeletFW \\ \qquad \llbracket ControlTierSync \rrbracket \\ TopLevelMissionSequencerFW(MainMissionSequencer) \end{array}\right)$$

$$\mathbf{process}\ Tier0 \mathrel{\widehat=} \left(\begin{array}{l} MissionFW(MainMission) \\ \qquad \llbracket MissionSync \rrbracket \\ )(\end{array}\right)$$

$$\mathbf{process}\ Framework \mathrel{\widehat=} \left(\begin{array}{l} ControlTier \\ \qquad \llbracket TierSync \rrbracket \\ (Tier0) \end{array}\right)$$

$$\mathbf{process}\ Application \mathrel{\widehat=} \left(\begin{array}{l} SPSafeletApp(hijac.tools.tightrope.environments.VariableEnv \bullet 58ce9668, hijac.tools.tightrope.environments.VariableE \\ \interleave \\ MainMissionSequencerApp \\ \interleave \\ MainMissionApp \\ \interleave \end{array}\right.$$

$$Locking \mathrel{\widehat=} \left(\begin{array}{l})(\\ \interleave \\ \left(\begin{array}{l} ObjectFW(SPSafeletObject) \\ \qquad \llbracket ObjectSync \rrbracket \\ ObjectFW(MainMissionObject) \end{array}\right) \end{array}\right)$$

$$\mathbf{process}\ Program \mathrel{\widehat=} Framework \llbracket AppSync \rrbracket Application \llbracket LockingSync \rrbracket Locking$$

2 ID Files

2.1 MissionIds

section $\mathit{MissionIds}$ **parents** $\mathit{scj\_prelude}, \mathit{MissionId}$

$\mathit{MainMission} : \mathit{MissionID}$

$\mathit{distinct}\langle \mathit{nullMissionId}, \mathit{MainMission} \rangle$

2.2 SchedulablesIds

section $\mathit{SchedulableIds}$ **parents** $\mathit{scj\_prelude}, \mathit{SchedulableId}$

$\mathit{MainMissionSequencer} : \mathit{SchedulableID}$

$\mathit{distinct}\langle \mathit{nullSequencerId}, \mathit{nullSchedulableId}, \rangle$

2.3 ThreadIds

section $\mathit{ThreadIds}$ **parents** $\mathit{scj\_prelude}, \mathit{GlobalTypes}$

$\mathit{distinct}\langle \mathit{SafeletThreadId}, \mathit{nullThreadId},$
$\rangle$

2.4 ObjectIds

section $\mathit{ObjectIds}$ **parents** $\mathit{scj\_prelude}, \mathit{GlobalTypes}$

$\mathit{SPSafeletObject} : \mathit{ObjectID}$
$\mathit{MainMissionObject} : \mathit{ObjectID}$

$\mathit{distinct}\langle \mathit{SPSafeletObject},$
$\mathit{MainMissionObject} \rangle$

3 Safelet

$\mathbf{section}\ SPSafeletApp\ \mathbf{parents}\ scj\_prelude, SchedulableId, SchedulableIds, SafeletChan$

$\mathbf{process}\, SPSafeletApp \mathrel{\widehat=} storageParameters_{t}\, opLevelSequencer : MissionID, storageParameters_{n}\, estedSequencer : Mission$

$$InitializeApplication \mathrel{\widehat=} \\ \left(\begin{array}{l} initializeApplicationCall \longrightarrow \\ initializeApplicationRet \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

$$GetSequencer \mathrel{\widehat=} \\ \left(\begin{array}{l} getSequencerCall \longrightarrow \\ getSequencerRet\, !\, MainMissionSequencer \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

$$Methods \mathrel{\widehat=} \\ \left(\begin{array}{l} GetSequencer \\ \Box \\ InitializeApplication \end{array}\right) ;\ Methods$$

$\bullet\ (Methods) \mathrel{\triangle} (end\_safelet\_app \longrightarrow \mathbf{Skip})$

$\mathbf{end}$

4 Top Level Mission Sequencer

section $\mathit{MainMissionSequencerApp}$ **parents** $\mathit{TopLevelMissionSequencerChan}$,
$\mathit{MissionId}, \mathit{MissionIds}, \mathit{SchedulableId}, \mathit{MainMissionSequencerClass}$

process $\mathit{MainMissionSequencerApp} \mathrel{\widehat=}$ **begin**

State

$\mathit{this} : \mathbf{ref}\ \mathit{MainMissionSequencerClass}$

state State

Init

State'

$\mathit{this}' = \mathbf{new}\ \mathit{MainMissionSequencerClass}()$

$$\mathit{GetNextMission} \mathrel{\widehat=} \mathbf{var}\ \mathit{ret} : \mathit{MissionID} \bullet \left(\begin{array}{l} \mathit{getNextMissionCall} \,.\, \mathit{MainMissionSequencer} \longrightarrow \\ \mathit{ret} := \mathit{this} \,.\, \mathit{getNextMission}(); \\ \mathit{getNextMissionRet} \,.\, \mathit{MainMissionSequencer} \,!\, \mathit{ret} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

$$\mathit{Methods} \mathrel{\widehat=} \left(\mathit{GetNextMission} \right) \; ; \; \mathit{Methods}$$

$$\bullet\ (\mathit{Init} \; ; \; \mathit{Methods}) \mathbin{\triangle} (\mathit{end\_sequencer\_app} \,.\, \mathit{MainMissionSequencer} \longrightarrow \mathbf{Skip})$$

end

$\mathbf{class}\ MainMissionSequencerClass \mathrel{\widehat{=}} \mathbf{begin}$

$$\begin{array}{|l}
\hline
\mathbf{state}\ State \\
returnedMission : \mathbb{B} \\
\hline
\end{array}$$

$\mathbf{state}\ State$

$$\begin{array}{|l}
\hline
\mathbf{initial}\ Init \\
State\,' \\
\hline
returnedMission' = false \\
\hline
\end{array}$$

$$\mathbf{protected}\ getNextMission \mathrel{\widehat{=}} \mathbf{var}\ ret : MissionID \bullet$$
$$\left(\begin{array}{l}
\mathbf{if}\ (\lnot\ returnedMission = \mathbf{True}) \longrightarrow \\
\qquad \left(\begin{array}{l} this\ .\ returnedMission := true; \\ ret := MainMission \end{array}\right) \\
[\!]\ \lnot\ (\lnot\ returnedMission = \mathbf{True}) \longrightarrow \\
\qquad \left(ret := nullMissionId\right) \\
\mathbf{fi}
\end{array}\right)$$

$\bullet\ \mathbf{Skip}$

$\mathbf{end}$

5 Missions

5.1 MainMission

$\mathbf{section}\ MainMissionApp\ \mathbf{parents}\ scj\_prelude, MissionId, MissionIds,$
$\quad SchedulableId, SchedulableIds, MissionChan, SchedulableMethChan, MainMissionClass\quad , MainMissionMethChan$

$\mathbf{process}\ MainMissionApp \mathrel{\widehat=} \mathbf{begin}$

$$\begin{array}{|l}
\hline
State \\
\quad this : \mathbf{ref}\ MainMissionClass \\
\hline
\end{array}$$

$\mathbf{state}\ State$

$$\begin{array}{|l}
\hline
Init \\
\quad State\,' \\
\hline
\quad this' = \mathbf{new}\ MainMissionClass() \\
\hline
\end{array}$$

$$\begin{array}{l}
InitializePhase \mathrel{\widehat=} \\
\left(\begin{array}{l}
initializeCall\,.\,MainMission \longrightarrow \\
initializeRet\,.\,MainMission \longrightarrow \\
\mathbf{Skip}
\end{array}\right)
\end{array}$$

$$\begin{array}{l}
CleanupPhase \mathrel{\widehat=} \\
\left(\begin{array}{l}
cleanupMissionCall\,.\,MainMission \longrightarrow \\
cleanupMissionRet\,.\,MainMission\,!\,\mathbf{False} \longrightarrow \\
\mathbf{Skip}
\end{array}\right)
\end{array}$$

$$\begin{array}{l}
environmentBadMeth \mathrel{\widehat=} \\
\left(\begin{array}{l}
environmentBadCall\,.\,MainMission \longrightarrow \\
this\,.\,environmentBad(); \\
environmentBadRet\,.\,MainMission \longrightarrow \\
\mathbf{Skip}
\end{array}\right)
\end{array}$$

$$Methods \mathrel{\widehat=} \left(\begin{array}{l}
InitializePhase \\
\Box \\
CleanupPhase \\
\Box \\
environmentBadMeth
\end{array}\right) \; ; \; Methods$$

$\bullet\ (Init\ ;\ Methods) \mathbin{\triangle} (end\_mission\_app\,.\,MainMission \longrightarrow \mathbf{Skip})$

$\mathbf{end}$

class $MainMissionClass \mathrel{\widehat=}$ **begin**

public $environmentBad \mathrel{\widehat=}$
$(\mathbf{Skip})$

$\bullet$ **Skip**

end

section $MainMissionMethChan$ **parents** $scj\_prelude, GlobalTypes, MissionId, SchedulableId$

channel $environmentBadCall : MissionID$
channel $environmentBadRet : MissionID$

5.2 Schedulables of