nestedSequencer1 Report

4th October 2016

1 ID Files

1.1 MissionIds

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

$$
\begin{array}{|l}
\mathit{MainMissionMID} : \mathit{MissionID} \\
\mathit{NestedMissionMID} : \mathit{MissionID} \\
\hline
\mathit{distinct} \langle \mathit{nullMissionId}, \mathit{MainMissionMID}, \mathit{NestedMissionMID} \rangle
\end{array}
$$

1.2 SchedulablesIds

section *SchedulableIds* **parents** *scj_prelude*, *SchedulableId*

$$
\begin{array}{|l}
MainMissionSequencerSID : SchedulableID \\
NestedMissionSequencerSID : SchedulableID \\
NestedOneShotEventHandlerSID : SchedulableID \\
\hline
distinct \langle nullSequencerId, nullSchedulableId, MainMissionSequencerSID, \\
NestedMissionSequencerSID, NestedOneShotEventHandlerSID \rangle
\end{array}
$$

2 Network

2.1 Network Channel Sets

section $NetworkChannels$ **parents** $scj\_prelude, MissionId, MissionIds,$
$SchedulableId, SchedulableIds, MissionChan, TopLevelMissionSequencerFWChan,$
$FrameworkChan, SafeletChan, AperiodicEventHandlerChan, ManagedThreadChan,$
$OneShotEventHandlerChan, PeriodicEventHandlerChan, MissionSequencerMethChan$

channelset $TerminateSync ==$
$\{\!| schedulables\_terminated, schedulables\_stopped, get\_activeSchedulables |\!\}$

channelset $ControlTierSync ==$
$\{\!| start\_toplevel\_sequencer, done\_toplevel\_sequencer, done\_safeletFW |\!\}$

channelset $TierSync ==$
$\{\!| start\_mission . MainMission, done\_mission . MainMission,$
$done\_safeletFW, done\_toplevel\_sequencer |\!\}$

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 $SafeltAppSync \mathrel{\widehat{=}}$
$\{\!| getSequencerCall, getSequencerRet, initializeApplicationCall, initializeApplicationRet, end\_safelet\_app |\!\}$

channelset $MissionSequencerAppSync ==$
$\{\!| getNextMissionCall, getNextMissionRet, end\_sequencer\_app |\!\}$

channelset $MissionAppSync ==$
$\{\!| initializeCall, register, initializeRet, cleanupMissionCall, cleanupMissionRet |\!\}$

channelset $AppSync ==$
$\bigcup\{SafeltAppSync, MissionSequencerAppSync, MissionAppSync,$
$MTAppSync, OSEHSync, APEHSync, PEHSync,$
$\{\!| getSequencer, end\_mission\_app, end\_managedThread\_app,$
$setCeilingPriority, requestTerminationCall, requestTerminationRet, terminationPendingCall,$
$terminationPendingRet, handleAsyncEventCall, handleAsyncEventRet |\!\}\}$

channelset $ThreadSync ==$
$\{\!| raise\_thread\_priority, lower\_thread\_priority, isInterruptedCall, isInterruptedRet, get\_priorityLevel |\!\}$

channelset $LockingSync ==$
$\{\!| lockAcquired, startSyncMeth, endSyncMeth, waitCall, waitRet, notify, isInterruptedCall, isInterruptedRet,$
$interruptedCall, interruptedRet, done\_toplevel\_sequencer, get\_priorityLevel |\!\}$

channelset $Tier0Sync ==$
$\{\!| done\_toplevel\_sequencer, done\_safeletFW,$
$start\_mission . NestedMission, done\_mission . NestedMission,$
$initializeRet . NestedMission, requestTermination . NestedMission . MainMissionSequencer |\!\}$

2.2 Locking

section $\mathit{NetworkLocking}$ **parents** $\mathit{scj\_prelude}, \mathit{GlobalTypes}, \mathit{FrameworkChan}, \mathit{MissionId}, \mathit{MissionIds}, \mathit{ThreadIds}, \mathit{NetworkChannels}, \mathit{ObjectFW}, \mathit{ThreadFW}$

process $\mathit{Threads} \mathrel{\widehat=}$

$$\left(\begin{array}{l}\mathit{ThreadFW}(\mathit{NestedMissionSequencerTID}, 5)\\ |||\\ \mathit{ThreadFW}(\mathit{NestedOneShotEventHandlerTID}, 5)\end{array}\right)$$

process $\mathit{Objects} \mathrel{\widehat=}$

$(\mathbf{Skip})$

process $\mathit{Locking} \mathrel{\widehat=} \mathit{Threads} \llbracket \mathit{ThreadSync} \rrbracket \mathit{Objects}$

2.3 Program

$$\begin{array}{l}\textbf{section}\ \mathit{Program}\ \textbf{parents}\ \mathit{scj\_prelude}, \mathit{MissionId}, \mathit{MissionIds},\\ \quad \mathit{SchedulableId}, \mathit{SchedulableIds}, \mathit{MissionChan}, \mathit{SchedulableMethChan}, \mathit{MissionFW},\\ \quad \mathit{SafeletFW}, \mathit{TopLevelMissionSequencerFW}, \mathit{NetworkChannels}, \mathit{ManagedThreadFW},\\ \quad \mathit{SchedulableMissionSequencerFW}, \mathit{PeriodicEventHandlerFW}, \mathit{OneShotEventHandlerFW},\\ \quad \mathit{AperiodicEventHandlerFW}, \mathit{ObjectFW}, \mathit{ThreadFW},\\ \quad \mathit{MySafeletApp}, \mathit{MainMissionSequencerApp}, \mathit{MainMissionApp}, \mathit{NestedMissionSequencerApp}, \mathit{NestedMissionApp},\\ \quad \mathit{NestedOneShotEventHandlerApp}\end{array}$$

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

$$\begin{array}{l}\textbf{process}\ \mathit{Tier0} \mathrel{\widehat=}\\ \left(\begin{array}{l}\mathit{MissionFW}(\mathit{MainMissionID})\\ \quad \llbracket \mathit{MissionSync} \rrbracket\\ (\mathit{OneShotEventHandlerFW}(\mathit{NestedMissionSequencerID}))\end{array}\right)\end{array}$$

$$\begin{array}{l}\textbf{process}\ \mathit{Tier1} \mathrel{\widehat=}\\ \left(\begin{array}{l}\mathit{MissionFW}(\mathit{NestedMissionID})\\ \quad \llbracket \mathit{MissionSync} \rrbracket\\ (\mathit{OneShotEventHandlerFW}(\mathit{NestedOneShotEventHandlerID}, (\mathit{time}(5, 0)), (\mathit{NULL}, \mathit{nullSchedulableId})))\end{array}\right)\end{array}$$

$$\begin{array}{l}\textbf{process}\ \mathit{Framework} \mathrel{\widehat=}\\ \left(\begin{array}{l}\mathit{ControlTier}\\ \quad \llbracket \mathit{TierSync} \rrbracket\\ \left(\begin{array}{l}\mathit{Tier0}\\ \quad \llbracket \mathit{Tier0Sync} \rrbracket\\ \mathit{Tier1}\end{array}\right)\end{array}\right)\end{array}$$

$$\begin{array}{l}\textbf{process}\ \mathit{Application} \mathrel{\widehat=}\\ \left(\begin{array}{l}\mathit{MySafeletApp}\\ \interleave\\ \mathit{MainMissionSequencerApp}\\ \interleave\\ \mathit{MainMissionApp}\\ \interleave\\ \mathit{NestedMissionSequencerApp}\\ \interleave\\ \mathit{NestedMissionApp}\\ \interleave\\ \mathit{NestedOneShotEventHandlerApp}\end{array}\right)\end{array}$$

$$\textbf{process}\ \mathit{Program} \mathrel{\widehat=} \left(\mathit{Framework} \llbracket \mathit{AppSync} \rrbracket \mathit{Application}\right) \llbracket \mathit{LockingSync} \rrbracket \mathit{Locking}$$

3 Safelet

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

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

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

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

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

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

$\mathbf{end}$

4 Top Level Mission Sequencer

section *MainMissionSequencerApp* **parents** *TopLevelMissionSequencerChan*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *MainMissionSequencerClass*, *MethodCallBindingChannels*

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

State

$this : \mathbf{ref}\ MainMissionSequencerClass$

state *State*

Init

$State~'$

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

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

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

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

end

section $\mathit{MainMissionSequencerClass}$ **parents** $\mathit{scj\_prelude}, \mathit{SchedulableId}, \mathit{SchedulableIds}, \mathit{SafeletChan}$
$, \mathit{MethodCallBindingChannels}, \mathit{MissionId}, \mathit{MissionIds}$

class $\mathit{MainMissionSequencerClass} \mathrel{\widehat=}$ **begin**

state State

$$\begin{array}{|l}
\mathit{returnedMission} : \mathbb{B}
\end{array}$$

state State

initial Init

$$\begin{array}{|l}
\mathit{State}\,' \\
\hline
\mathit{returnedMission}' = \mathbf{False}
\end{array}$$

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

$\bullet$ **Skip**

end

5 Missions

5.1 MainMission

$$\begin{array}{l}\mathbf{section}\ MainMissionApp\ \mathbf{parents}\ scj\_prelude, MissionId, MissionIds, \\ \quad SchedulableId, SchedulableIds, MissionChan, SchedulableMethChan, MainMissionMethChan \\ , MethodCallBindingChannels\end{array}$$

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

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

$$\begin{array}{l} CleanupPhase \mathrel{\widehat=} \\ \left(\begin{array}{l} \mathbf{var}\,\mathbb{B} : ret \bullet cleanupMissionCall\,.\,MainMissionMID \longrightarrow \\ cleanupMissionRet\,.\,MainMissionMID\,!\,\mathbf{True} \longrightarrow \\ \mathbf{Skip} \end{array}\right) \end{array}$$

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

$$\bullet\ (Init\ ;\ Methods) \vartriangle (end\_mission\_app\,.\,MainMissionMID \longrightarrow \mathbf{Skip})$$

end

5.2 Schedulables of MainMission

section $\mathit{NestedMissionSequencerApp}$ **parents** $\mathit{TopLevelMissionSequencerChan}$,
$\mathit{MissionId}, \mathit{MissionIds}, \mathit{SchedulableId}, \mathit{SchedulableIds}, \mathit{NestedMissionSequencerClass}, \mathit{MethodCallBindingChannels}$

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

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

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

$$\bullet\ (\mathit{Methods}) \mathrel{\triangle} (\mathit{end\_sequencer\_app} \,.\, \mathit{NestedMissionSequencerSID} \longrightarrow \mathbf{Skip})$$

end

$\mathbf{section}\ NestedMissionSequencerClass\ \mathbf{parents}\ scj\_prelude, SchedulableId, SchedulableIds, SafeletChan$
$, MethodCallBindingChannels, MissionId, MissionIds$

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

$\mathbf{state}\ State$

$returnedMission : \mathbb{B}$

$\mathbf{state}\ State$

$\mathbf{initial}\ Init$

$State~'$

$returnedMission = \mathbf{False}$

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

$\bullet\ \mathbf{Skip}$

$\mathbf{end}$

5.3 NestedMission

$\mathbf{section}\ \mathit{NestedMissionApp}\ \mathbf{parents}\ \mathit{scj\_prelude}, \mathit{MissionId}, \mathit{MissionIds},$
$\quad \mathit{SchedulableId}, \mathit{SchedulableIds}, \mathit{MissionChan}, \mathit{SchedulableMethChan}, \mathit{NestedMissionMethChan}$
$, \mathit{MethodCallBindingChannels}$

$\mathbf{process}\ \mathit{NestedMissionApp} \mathrel{\widehat=} \mathbf{begin}$

$$\mathit{InitializePhase} \mathrel{\widehat=}$$
$$\left(\begin{array}{l} \mathit{initializeCall} \,.\, \mathit{NestedMissionMID} \longrightarrow \\ \mathit{register} \,!\, \mathit{NestedOneShotEventHandlerSID} \,!\, \mathit{NestedMissionMID} \longrightarrow \\ \mathit{initializeRet} \,.\, \mathit{NestedMissionMID} \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

$$\mathit{CleanupPhase} \mathrel{\widehat=}$$
$$\left(\begin{array}{l} \mathbf{var}\, \mathbb{B} : \mathit{ret} \bullet \mathit{cleanupMissionCall} \,.\, \mathit{NestedMissionMID} \longrightarrow \\ \mathit{cleanupMissionRet} \,.\, \mathit{NestedMissionMID} \,!\, \mathbf{True} \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

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

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

end

5.4 Schedulables of NestedMission

section *NestedOneShotEventHandlerApp* **parents** *OneShotEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBindingChannels*

process *NestedOneShotEventHandlerApp* $\widehat{=}$
begin

$$handleAsyncEvent \mathrel{\widehat{=}} \left(\begin{array}{l} handleAsyncEventCall \,.\, NestedOneShotEventHandlerSID \longrightarrow \\ \mathbf{Skip}; \\ handleAsyncEventRet \,.\, NestedOneShotEventHandlerSID \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

$$Methods \mathrel{\widehat{=}} \big(handleAsyncEvent\big) \;;\; Methods$$

$$\bullet\ (Methods) \mathbin{\triangle} (end\_oneShot\_app \,.\, NestedOneShotEventHandlerSID \longrightarrow \mathbf{Skip})$$

end