nestedSequencer3

Tight Rope v0.75

1st March 2017

1 ID Files

1.1 MissionIds

section *MissionIds* **parents** *scj_prelude*, *MissionId*

$$MainMissionMID : MissionID$$
$$NestedMissionAMID : MissionID$$
$$NestedMissionBMID : MissionID$$

$$distinct\langle nullMissionId, MainMissionMID, NestedMissionAMID, NestedMissionBMID\rangle$$

1.2 SchedulablesIds

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

$$
\begin{array}{|l}
mainSequencerSID : SchedulableID \\
NestedMissionSequencerSID : SchedulableID \\
MT1SID : SchedulableID \\
MT2SID : SchedulableID \\
\hline
distinct\langle nullSequencerId, nullSchedulableId, mainSequencerSID, \\
NestedMissionSequencerSID, MT1SID, \\
MT2SID\rangle
\end{array}
$$

1.3 Non-Paradigm Objects

1.4 ThreadIds

section *ThreadIds* **parents** *scj_prelude*, *GlobalTypes*

$$SafeletTId : ThreadID$$
$$nullThreadId : ThreadID$$

$$distinct\langle SafeletTId, nullThreadId\rangle$$

1.5 ObjectIds

section *ObjectIds* **parents** *scj_prelude*, *GlobalTypes*

$$\vdash \; distinct\langle\rangle$$

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* $\widehat{=}$
{| *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 *Tier*0*Sync* ==
{| *done_toplevel_sequencer*, *done_safeletFW*,
start_mission . *NestedMissionA*, *done_mission* . *NestedMissionA*,
initializeRet . *NestedMissionA*, *requestTermination* . *NestedMissionA* . *mainSequencer*,
start_mission . *NestedMissionB*, *done_mission* . *NestedMissionB*,
initializeRet . *NestedMissionB*, *requestTermination* . *NestedMissionB* . *mainSequencer* |}

2.2 Locking

section *NetworkLocking* **parents** *scj_prelude*, *GlobalTypes*, *FrameworkChan*, *MissionId*, *MissionIds*, *ThreadIds*, *NetworkChannels*, *ObjectFW*, *ThreadFW*, *Priority*

process *Threads* $\widehat{=}$
$(\mathbf{Skip})$

process *Objects* $\widehat{=}$
$(\mathbf{Skip})$

process *Locking* $\widehat{=}$ $(Threads \llbracket ThreadSync \rrbracket Objects) \triangle (done\_toplevel\_sequencer \longrightarrow \mathbf{Skip})$

2.3 Program

section *Program* **parents** *scj_prelude*, *MissionId*, *MissionIds*,
SchedulableId, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *MissionFW*,
SafeletFW, *TopLevelMissionSequencerFW*, *NetworkChannels*, *ManagedThreadFW*,
SchedulableMissionSequencerFW, *PeriodicEventHandlerFW*, *OneShotEventHandlerFW*,
AperiodicEventHandlerFW, *ObjectFW*, *ThreadFW*,
MyAppApp, *mainSequencerApp*, *MainMissionApp*, *NestedMissionSequencerApp*, *NestedMissionAApp*, *MT*1*App*, *Nest*

process $ControlTier \mathrel{\widehat=}$
$$\left(\begin{array}{l} SafeletFW \\ \quad [\![ControlTierSync]\!] \\ TopLevelMissionSequencerFW(mainSequencer) \end{array}\right)$$

process $Tier0 \mathrel{\widehat=}$
$$\left(\begin{array}{l} MissionFW(MainMissionID) \\ \quad [\![MissionSync]\!] \\ (SchedulableMissionSequencerFW(NestedMissionSequencerID)) \end{array}\right)$$

process $Tier1 \mathrel{\widehat=}$
$$\left(\begin{array}{l} MissionFW(NestedMissionAID) \\ \quad [\![MissionSync]\!] \\ (ManagedThreadFW(MT1ID)) \end{array}\right)$$
$$[\![ClusterSync]\!]$$
$$\left(\begin{array}{l} MissionFW(NestedMissionBID) \\ \quad [\![MissionSync]\!] \\ (ManagedThreadFW(MT2ID)) \end{array}\right)$$

process $Framework \mathrel{\widehat=}$
$$\left(\begin{array}{l} ControlTier \\ \quad [\![TierSync]\!] \\ \left(\begin{array}{l} Tier0 \\ \quad [\![Tier0Sync]\!] \\ Tier1 \end{array}\right) \end{array}\right)$$

process $Application \mathrel{\widehat=}$
$$\left(\begin{array}{l} MyAppApp \\ ||| \\ mainSequencerApp \\ ||| \\ MainMissionApp \\ ||| \\ NestedMissionSequencerApp \\ ||| \\ NestedMissionAApp \\ ||| \\ MT1App \\ ||| \\ NestedMissionBApp \\ ||| \\ MT2App \end{array}\right)$$

process $Program \mathrel{\widehat=} (Framework \; [\![\; AppSync \;]\!] \; Application) \; [\![\; LockingSync \;]\!] \; Locking$

3 Safelet

section $MyAppApp$ **parents** $scj\_prelude, SchedulableId, SchedulableIds, SafeletChan, MethodCallBindingChannels$

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

$$InitializeApplication \mathrel{\widehat=} \begin{pmatrix} initializeApplicationCall \longrightarrow \\ initializeApplicationRet \longrightarrow \\ \mathbf{Skip} \end{pmatrix}$$

$$GetSequencer \mathrel{\widehat=} \begin{pmatrix} getSequencerCall \longrightarrow \\ getSequencerRet\,!\,mainSequencerSID \longrightarrow \\ \mathbf{Skip} \end{pmatrix}$$

$$Methods \mathrel{\widehat=} \begin{pmatrix} GetSequencer \\ \Box \\ InitializeApplication \end{pmatrix} ;\ Methods$$

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

end

4 Top Level Mission Sequencer

section *mainSequencerApp* **parents** *TopLevelMissionSequencerChan*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *mainSequencerClass*, *MethodCallBindingChannels*

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

State

$this : \mathbf{ref}\ mainSequencerClass$

state *State*

Init

$State'$

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

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

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

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

end

section *mainSequencerClass* **parents** *scj_prelude*, *SchedulableId*, *SchedulableIds*, *SafeletChan*
, *MethodCallBindingChannels*, *MissionId*, *MissionIds*

class *mainSequencerClass* $\widehat{=}$ **begin**

state *State*

$$notReleased : \mathbb{B}$$

state *State*

initial *Init*

$$State'$$

$$notReleased' = true$$

protected *getNextMission* $\widehat{=}$

$$\left(\begin{array}{l}
\textbf{if } notReleased \longrightarrow \\
\quad \left(\begin{array}{l} notReleased := \textbf{False}; \\ ret := MainMissionMID \end{array}\right) \\
[\!] \neg\, notReleased \longrightarrow \\
\quad \left(ret := nullMissionId\right) \\
\textbf{fi}
\end{array}\right)$$

- **Skip**

end

5 Missions

5.1 MainMission

section *MainMissionApp* **parents** *scj_prelude*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *MainMissionMethChan*, *MethodCallBindingChannels*

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

State

$this : \textbf{ref}\ MainMissionClass$

state *State*

Init

$State'$

$this' = \textbf{new}\ MainMissionClass()$

$$InitializePhase \mathrel{\widehat=} \begin{pmatrix} initializeCall\,.\,MainMissionMID \longrightarrow \\ register\,!\,NestedMissionSequencerSID\,!\,MainMissionMID \longrightarrow \\ initializeRet\,.\,MainMissionMID \longrightarrow \\ \textbf{Skip} \end{pmatrix}$$

$$CleanupPhase \mathrel{\widehat=} \begin{pmatrix} cleanupMissionCall\,.\,MainMissionMID \longrightarrow \\ cleanupMissionRet\,.\,MainMissionMID\,!\,\textbf{True} \longrightarrow \\ \textbf{Skip} \end{pmatrix}$$

$$Methods \mathrel{\widehat=} \begin{pmatrix} InitializePhase \\ \Box \\ CleanupPhase \end{pmatrix} ;\ Methods$$

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

end

5.2 Schedulables of MainMission

section *NestedMissionSequencerApp* **parents** *TopLevelMissionSequencerChan*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *NestedMissionSequencerClass*, *MethodCallBindingChannels*

process $NestedMissionSequencerApp \mathrel{\widehat=} \textbf{begin}$

State

$this : \textbf{ref}\ NestedMissionSequencerClass$

state *State*

Init

$State'$

$this' = \textbf{new}\ NestedMissionSequencerClass()$

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

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

$\bullet\ (Init\ ;\ Methods) \triangle (end\_sequencer\_app\,.\,NestedMissionSequencerSID \longrightarrow \textbf{Skip})$

end

section *NestedMissionSequencerClass* **parents** *scj_prelude*, *SchedulableId*, *SchedulableIds*, *SafeletChan*, *MethodCallBindingChannels*, *MissionId*, *MissionIds*

class *NestedMissionSequencerClass* $\widehat{=}$ **begin**

state *State*

$$releases : \mathbb{Z}$$

state *State*

initial *Init*

$$State'$$

$$releases' = 0$$

protected *getNextMission* $\widehat{=}$

$$\left(\begin{array}{l}
\textbf{if } (releases = 0) \longrightarrow \\
\quad \left(\begin{array}{l} releases := releases + 1; \\ ret := NestedMissionAMID \end{array}\right) \\
[\!] \neg (releases = 0) \longrightarrow \\
\quad \textbf{if } (releases = 1) \longrightarrow \\
\quad \left(\begin{array}{l} releases := releases + 1; \\ ret := NestedMissionBMID \end{array}\right) \\
[\!] \neg (releases = 1) \longrightarrow \\
\quad \left(ret := nullMissionId\right) \\
\textbf{fi} \\
\textbf{fi}
\end{array}\right)$$

- **Skip**

end

5.3 NestedMissionA

section *NestedMissionAApp* **parents** *scj_prelude*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *NestedMissionAMethChan*, *MethodCallBindingChannels*

process $NestedMissionAApp \mathrel{\widehat=} \textbf{begin}$

State

$this : \textbf{ref}\ NestedMissionAClass$

state *State*

Init

$State'$

$this' = \textbf{new}\ NestedMissionAClass()$

$$InitializePhase \mathrel{\widehat=} \begin{pmatrix} initializeCall\,.\,NestedMissionAMID \longrightarrow \\ register\,!\,MT1SID\,!\,NestedMissionAMID \longrightarrow \\ initializeRet\,.\,NestedMissionAMID \longrightarrow \\ \textbf{Skip} \end{pmatrix}$$

$$CleanupPhase \mathrel{\widehat=} \begin{pmatrix} cleanupMissionCall\,.\,NestedMissionAMID \longrightarrow \\ cleanupMissionRet\,.\,NestedMissionAMID\,!\,\textbf{True} \longrightarrow \\ \textbf{Skip} \end{pmatrix}$$

$$Methods \mathrel{\widehat=} \begin{pmatrix} InitializePhase \\ \Box \\ CleanupPhase \end{pmatrix} ;\ Methods$$

$$\bullet\ (Init\ ;\ Methods) \triangle (end\_mission\_app\,.\,NestedMissionAMID \longrightarrow \textbf{Skip})$$

end

5.4 Schedulables of NestedMissionA

section $MT1App$ **parents** $ManagedThreadChan, SchedulableId, SchedulableIds, MethodCallBindingChannels$

process $MT1App \mathrel{\widehat=}$ **begin**

$$Run \mathrel{\widehat=} \left(\begin{array}{l} runCall\,.\,MT1SID \longrightarrow \\ \left(\begin{array}{l}\textbf{Skip};\\ \textbf{Skip}\end{array}\right); \\ runRet\,.\,MT1SID \longrightarrow \\ \textbf{Skip}\end{array}\right)$$

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

$\bullet\ (Methods) \triangle (end\_managedThread\_app\,.\,MT1SID \longrightarrow \textbf{Skip})$

end

5.5 NestedMissionB

section *NestedMissionBApp* **parents** *scj_prelude*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *NestedMissionBMethChan*, *MethodCallBindingChannels*

process $NestedMissionBApp \mathrel{\widehat=} \textbf{begin}$

State

$this : \textbf{ref}\ NestedMissionBClass$

state *State*

Init

$State'$

$this' = \textbf{new}\ NestedMissionBClass()$

$$InitializePhase \mathrel{\widehat=} \begin{pmatrix} initializeCall\,.\,NestedMissionBMID \longrightarrow \\ register\,!\,MT2SID\,!\,NestedMissionBMID \longrightarrow \\ initializeRet\,.\,NestedMissionBMID \longrightarrow \\ \textbf{Skip} \end{pmatrix}$$

$$CleanupPhase \mathrel{\widehat=} \begin{pmatrix} cleanupMissionCall\,.\,NestedMissionBMID \longrightarrow \\ cleanupMissionRet\,.\,NestedMissionBMID\,!\,\textbf{True} \longrightarrow \\ \textbf{Skip} \end{pmatrix}$$

$$Methods \mathrel{\widehat=} \begin{pmatrix} InitializePhase \\ \Box \\ CleanupPhase \end{pmatrix} ;\ Methods$$

$\bullet\ (Init\ ;\ Methods) \triangle (end\_mission\_app\,.\,NestedMissionBMID \longrightarrow \textbf{Skip})$

end

5.6 Schedulables of NestedMissionB

section $MT2App$ **parents** $ManagedThreadChan, SchedulableId, SchedulableIds, MethodCallBindingChannels$

process $MT2App \mathrel{\widehat=}$ **begin**

$$Run \mathrel{\widehat=} \left(\begin{array}{l} runCall\,.\,MT2SID \longrightarrow \\ \left(\begin{array}{l}\textbf{Skip};\\ \textbf{Skip}\end{array}\right); \\ runRet\,.\,MT2SID \longrightarrow \\ \textbf{Skip}\end{array}\right)$$

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

- $(Methods) \triangle (end\_managedThread\_app\,.\,MT2SID \longrightarrow \textbf{Skip})$

end