producerConsumer

Tight Rope v0.88

5th March 2017

1 ID Files

1.1 MissionIds

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

$$PCMissionMID : MissionID$$

$$distinct\langle nullMissionId, PCMissionMID\rangle$$

1.2 SchedulablesIds

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

$$
\begin{array}{l}
PCMissionSequencerSID : SchedulableID \\
ProducerSID : SchedulableID \\
ConsumerSID : SchedulableID \\
\hline
distinct\langle nullSequencerId, nullSchedulableId, PCMissionSequencerSID, \\
ProducerSID, ConsumerSID\rangle
\end{array}
$$

1.3 Non-Paradigm Objects

section *BufferApp* **parents** *scj_prelude*, *SchedulableId*, *SchedulableIds*, *SafeletChan*
, *BufferClass*, *MethodCallBindingChannels* , *ObjectChan*, *ObjectIds*, *ThreadIds*, *ObjectFWChan*, *ObjectIds*

$$BufferID : NonParadigmID$$

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

State

$$this : \mathbf{ref}\ BufferClass$$

state *State*

Init

$$State'$$

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

$$
\begin{array}{l}
writeSyncMeth \mathrel{\widehat=} \\
\left(\begin{array}{l}
writeCall\,.\,BufferID\,?\,caller\,?\,thread\,?\,update \longrightarrow \\
\left(\begin{array}{l}
startSyncMeth\,.\,BufferOID\,.\,thread \longrightarrow \\
lockAcquired\,.\,BufferOID\,.\,thread \longrightarrow \\
\left(\begin{array}{l}
\mu X \bullet \\
\left(\begin{array}{l}
\mathbf{var}\ loopVar : \mathbb{B} \bullet loopVar := (\neg\ this\,.\,bufferEmpty()); \\
\mathbf{if}\ (loopVar = \mathbf{True}) \longrightarrow \\
\quad \left(\begin{array}{l} waitCall\,.\,BufferOID\,.\,thread \longrightarrow \\ waitRet\,.\,BufferOID\,.\,thread \longrightarrow \end{array}\right); \ X \\
\quad \mathbf{Skip} \\
[\!]\ (loopVar = \mathbf{False}) \longrightarrow \mathbf{Skip} \\
\mathbf{fi}
\end{array}\right)
\end{array}\right); \\
theBuffer := update; \\
notify\,.\,BufferOID\,!\,thread \longrightarrow \\
\mathbf{Skip}
\end{array}\right); \\
endSyncMeth\,.\,BufferOID\,.\,thread \longrightarrow \\
writeRet\,.\,BufferID\,.\,caller\,.\,thread \longrightarrow \\
\mathbf{Skip}
\end{array}\right)
\end{array}
$$

$$
\begin{array}{l}
readSyncMeth \mathrel{\widehat=} \textbf{var}\ ret : \mathbb{Z} \bullet \\
\left(\begin{array}{l}
readCall\ .\ BufferID\ ?\ caller\ ?\ thread \longrightarrow \\
\left(\begin{array}{l}
startSyncMeth\ .\ BufferOID\ .\ thread \longrightarrow \\
lockAcquired\ .\ BufferOID\ .\ thread \longrightarrow \\
\left(\begin{array}{l}
\mu X \bullet \\
\left(\begin{array}{l}
\textbf{var}\ loopVar : \mathbb{B} \bullet loopVar := \ this\ .\ bufferEmpty(); \\
\textbf{if}\ (loopVar = \textbf{True}) \longrightarrow \\
\qquad \left(\begin{array}{l} waitCall\ .\ BufferOID\ .\ thread \longrightarrow \\ waitRet\ .\ BufferOID\ .\ thread \longrightarrow \end{array}\right) ;\ X \\
\qquad \textbf{Skip} \\
[\!]\ (loopVar = \textbf{False}) \longrightarrow \textbf{Skip} \\
\textbf{fi}
\end{array}\right)
\end{array}\right) ; \\
\textbf{var}\ out : \mathbb{Z} \bullet out := this\ .\ theBuffer; \\
this\ .\ theBuffer := 0; \\
notify\ .\ BufferOID\ !\ thread \longrightarrow \\
\textbf{Skip}; \\
ret := out \\
endSyncMeth\ .\ BufferOID\ .\ thread \longrightarrow \\
readRet\ .\ BufferID\ .\ caller\ .\ thread\ !\ ret \longrightarrow \\
\textbf{Skip}
\end{array}\right)
\end{array}\right)
\end{array}
$$

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

$$
\bullet\ (Init\ ;\ Methods) \triangle (end\_safelet\_app \longrightarrow \textbf{Skip})
$$

end

section *BufferClass* **parents** *scj_prelude*, *SchedulableId*, *SchedulableIds*, *SafeletChan*
, *MethodCallBindingChannels*

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

state *State*

$$theBuffer : \mathbb{Z}$$

state *State*

initial *Init*

$$State'$$

$$theBuffer' = 0$$

public *bufferEmpty* $\widehat{=}$

$$\left(\begin{array}{l}\textbf{Skip};\\ \textbf{if}\ (theBuffer = 0) \longrightarrow\\ \quad ret := \textbf{True}\\ [\!]\ \neg\ (theBuffer = 0) \longrightarrow\\ \quad ret := \textbf{False}\\ \textbf{fi}\end{array}\right)$$

- **Skip**

end

1.4 ThreadIds

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

$$
\begin{array}{|l}
SafeletTId : ThreadID \\
nullThreadId : ThreadID \\
ProducerTID : ThreadID \\
ConsumerTID : ThreadID \\
\hline
distinct\langle SafeletTId, nullThreadId, \\
ProducerTID, ConsumerTID\rangle
\end{array}
$$

1.5 ObjectIds

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

$$BufferOID : ObjectID$$

$$distinct\langle BufferOID\rangle$$

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* . *PCMission*, *done_mission* . *PCMission*, *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* |}

2.2 MethodCallBinder

section *MethodCallBindingChannels* **parents** *scj_prelude*, *GlobalTypes*, *FrameworkChan*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *ThreadIds*

channel $binder\_readCall : blankID \times SchedulableID \times ThreadID$
channel $binder\_readRet : blankID \times SchedulableID \times ThreadID \times \mathbb{Z}$

$readLocs == \{BufferID\}$
$readCallers == \{ConsumerSID\}$

channel $binder\_terminationPendingCall : \times SchedulableID$
channel $binder\_terminationPendingRet : \times SchedulableID \times boolean$

$terminationPendingLocs == \{PCMissionMID\}$
$terminationPendingCallers == \{ProducerSID, ConsumerSID\}$

channel $binder\_writeCall : blankID \times SchedulableID \times ThreadID \times \mathbb{Z}$
channel $binder\_writeRet : blankID \times SchedulableID \times ThreadID$

$writeLocs == \{BufferID\}$
$writeCallers == \{ProducerSID\}$

channelset $MethodCallBinderSync == \{\!|\ done\_toplevel\_sequencer,$
$binder\_readCall, binder\_readRet,$
$binder\_terminationPendingCall, binder\_terminationPendingRet,$
$binder\_writeCall, binder\_writeRet\ |\!\}$

section *MethodCallBinder* **parents** *scj_prelude*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *MethodCallBindingChannels*
, *BuffeMethChan*, *PCMissionMethChan*

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

$read\_MethodBinder \mathrel{\widehat=}$
$$\left(\begin{array}{l} binder\_readCall\,?\,loc : (loc \in readLocs)\,?\,caller : (caller \in readCallers)\,?\,callingThread \longrightarrow \\ readCall\,.\,loc\,.\,caller\,.\,callingThread \longrightarrow \\ readRet\,.\,loc\,.\,caller\,.\,callingThread\,?\,ret \longrightarrow \\ binder\_readRet\,.\,loc\,.\,caller\,.\,callingThread\,!\,ret \longrightarrow \\ read\_MethodBinder \end{array}\right)$$

$terminationPending\_MethodBinder \mathrel{\widehat=}$
$$\left(\begin{array}{l} binder\_terminationPendingCall\,?\,loc : (loc \in terminationPendingLocs)\,?\,caller : (caller \in terminationPendingCalle \\ terminationPendingCall\,.\,loc\,.\,caller \longrightarrow \\ terminationPendingRet\,.\,loc\,.\,caller\,?\,ret \longrightarrow \\ binder\_terminationPendingRet\,.\,loc\,.\,caller\,!\,ret \longrightarrow \\ terminationPending\_MethodBinder \end{array}\right)$$

$write\_MethodBinder \mathrel{\widehat{=}}$

$$\left(\begin{array}{l} binder\_writeCall\,?\,loc : (loc \in writeLocs)\,?\,caller : (caller \in writeCallers)\,?\,callingThread\,?\,p1 \longrightarrow \\ writeCall\,.\,loc\,.\,caller\,.\,callingThread\,!\,p1 \longrightarrow \\ writeRet\,.\,loc\,.\,caller\,.\,callingThread \longrightarrow \\ binder\_writeRet\,.\,loc\,.\,caller\,.\,callingThread \longrightarrow \\ write\_MethodBinder \end{array}\right)$$

$BinderActions \mathrel{\widehat{=}}$

$$\left(\begin{array}{l} read\_MethodBinder \\ |||\\ terminationPending\_MethodBinder \\ |||\\ write\_MethodBinder \end{array}\right)$$

- $BinderActions \triangle (done\_toplevel\_sequencer \longrightarrow \mathbf{Skip})$

end

2.3 Locking

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

process $Threads \mathrel{\widehat=}$
$\left(\begin{array}{l} ThreadFW(ProducerTID, 10) \\ ||| \\ ThreadFW(ConsumerTID, 10) \end{array}\right)$

process $Objects \mathrel{\widehat=}$
$\big(ObjectFW(BufferOID)\big)$

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

2.4 Program

section *Program* **parents** *scj_prelude*, *MissionId*, *MissionIds*,
SchedulableId, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *MissionFW*,
SafeletFW, *TopLevelMissionSequencerFW*, *NetworkChannels*, *ManagedThreadFW*,
SchedulableMissionSequencerFW, *PeriodicEventHandlerFW*, *OneShotEventHandlerFW*,
AperiodicEventHandlerFW, *ObjectFW*, *ThreadFW*,
PCSafeletApp, *PCMissionSequencerApp*, *PCMissionApp*, *ProducerApp*, *ConsumerApp*

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

process $Tier0 \mathrel{\widehat=}$
$$\left(\begin{array}{l} MissionFW(PCMissionID) \\ \quad [\![MissionSync]\!] \\ \left(\begin{array}{l} ManagedThreadFW(ProducerID) \\ \quad [\![SchedulablesSync]\!] \\ ManagedThreadFW(ConsumerID) \end{array}\right) \end{array}\right)$$

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

process $Application \mathrel{\widehat=}$
$$\left(\begin{array}{l} PCSafeletApp \\ ||| \\ PCMissionSequencerApp \\ ||| \\ PCMissionApp \\ ||| \\ ProducerApp(PCMissionID) \\ ||| \\ ConsumerApp(PCMissionID) \\ ||| \\ BufferApp \end{array}\right)$$

process $Bound\_Application \mathrel{\widehat=} Application \ [\![\ MethodCallBinderSync \ ]\!] \ MethodCallBinder$
process $Program \mathrel{\widehat=} (\ Framework \ [\![\ AppSync \ ]\!] \ Bound\_Application\ ) \ [\![\ LockingSync \ ]\!] \ Locking$

3 Safelet

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

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

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

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

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

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

end

4 Top Level Mission Sequencer

section *PCMissionSequencerApp* **parents** *TopLevelMissionSequencerChan*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *PCMissionSequencerClass*, *MethodCallBindingChannels*

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

State

$this : \textbf{ref}\ PCMissionSequencerClass$

state *State*

Init

$State'$

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

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

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

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

end

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

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

state *State*

$$returnedMission : \mathbb{B}$$

state *State*

initial *Init*

$$State'$$

$$returnedMission' = \textbf{False}$$

protected *getNextMission* $\widehat{=}$

$$\left(\begin{array}{l}\textbf{if } (\neg\ returnedMission) \longrightarrow \\ \quad \left(\begin{array}{l} returnedMission := \textbf{True}; \\ ret := PCMissionMID \end{array}\right) \\ [\!]\ \neg\ (\neg\ returnedMission) \longrightarrow \\ \quad \big(ret := nullMissionId\big) \\ \textbf{fi}\end{array}\right)$$

- **Skip**

end

5 Missions

5.1 PCMission

section *PCMissionApp* **parents** *scj_prelude*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *PCMissionMethChan*, *MethodCallBindingChannels*

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

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

$$CleanupPhase \mathrel{\widehat=} \textbf{var}\,\mathbb{B} : ret \bullet \begin{pmatrix} cleanupMissionCall\,.\,PCMissionMID \longrightarrow \\ (ret := \textbf{False}) \\ cleanupMissionRet\,.\,PCMissionMID\,!\,ret \longrightarrow \\ \textbf{Skip} \end{pmatrix}$$

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

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

end

5.2 Schedulables of PCMission

section *ProducerApp* **parents** *ManagedThreadChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBindingChannels*, *MissionMethChan*, *BufferMethChan*, *ObjectIds*, *ThreadIds*

process $ProducerApp \mathrel{\widehat=}$
$pcMission : MissionID \bullet$ **begin**

$Run \mathrel{\widehat=}$
$\Big($ *runCall . ProducerSID* $\longrightarrow$
$\Big($ **var** $i : \mathbb{Z} \bullet i := 1;$
$\mu X \bullet$
$\Big($ *binder_terminationPendingCall . PcMission* $\longrightarrow$
binder_terminationPendingRet . PcMission ? terminationPending $\longrightarrow$
var $loopVar : \mathbb{B} \bullet loopVar := (\neg\ terminationPending);$
if $(loopVar =$ **True**$) \longrightarrow$
$\Big($ *binder_writeCall . BufferID . ProducerSID . ProducerTID ! i* $\longrightarrow$
binder_writeRet . BufferID . ProducerSID . ProducerTID $\longrightarrow$
Skip;
$i := i + 1;$
if $(i \geq 5) \longrightarrow$
$\Big($ *requestTerminationCall . PcMission . ProducerSID* $\longrightarrow$
requestTerminationRet . PcMission . ProducerSID ? requestTermination $\longrightarrow$
Skip $\Big)$
$[\!]\ \neg\ (i \geq 5) \longrightarrow$ **Skip**
fi $\Big)$; X
$[\!]\ (loopVar =$ **False**$) \longrightarrow$ **Skip**
fi $\Big)$ $\Big)$;
runRet . ProducerSID $\longrightarrow$
Skip $\Big)$

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

$\bullet\ (Methods) \triangle (end\_managedThread\_app\ .\ ProducerSID \longrightarrow$ **Skip**$)$

end

section *ConsumerApp* **parents** *ManagedThreadChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBindingChannels*, *MissionMethChan*, *BufferMethChan*, *ObjectIds*, *ThreadIds*

process $ConsumerApp \mathrel{\widehat=}$
$pcMission : MissionID \bullet$ **begin**

$Run \mathrel{\widehat=}$
$\Big($ *runCall* . *ConsumerSID* $\longrightarrow$
$\Big($ $\mu X \bullet$
$\Big($ *binder_terminationPendingCall* . *PcMission* $\longrightarrow$
binder_terminationPendingRet . *PcMission* ? *terminationPending* $\longrightarrow$
var *loopVar* : $\mathbb{B} \bullet$ *loopVar* := $(\neg$ *terminationPending*);
if $($*loopVar* = **True**$)$ $\longrightarrow$
$\Big($ **var** *result* : $\mathbb{Z} \bullet$ *result* := 999;
binder_readCall . *BufferID* . *ConsumerSID* . *ConsumerTID* $\longrightarrow$
binder_readRet . *BufferID* . *ConsumerSID* . *ConsumerTID* ? *read* $\longrightarrow$
Skip $\Big)$; X
$[]$ $($*loopVar* = **False**$)$ $\longrightarrow$ **Skip**
fi $\Big)\Big)$
runRet . *ConsumerSID* $\longrightarrow$
Skip $\Big)$;

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

$\bullet$ $($*Methods*$) \triangle ($*end_managedThread_app* . *ConsumerSID* $\longrightarrow$ **Skip**$)$

end