Flatbuffer

Tight Rope v0.6

18th January 2016

1 ID Files

1.1 MissionIds

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

$$FlatBufferMissionID : MissionID$$

$$distinct\langle nullMissionId, FlatBufferMissionID\rangle$$

1.2 SchedulablesIds

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

$$
\begin{array}{l}
FlatBufferMissionSequencerID : SchedulableID \\
ReaderID : SchedulableID \\
WriterID : SchedulableID \\
\hline
distinct\langle nullSequencerId, nullSchedulableId, FlatBufferMissionSequencerID, \\
ReaderID, WriterID\rangle
\end{array}
$$

1.3 ThreadIds

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

$$ReaderThreadID : ThreadID$$
$$WriterThreadID : ThreadID$$

$$distinct\langle SafeletThreadId, nullThreadId, ReaderThreadID, WriterThreadID\rangle$$

1.4 ObjectIds

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

$$
\begin{array}{|l}
FlatBufferObjectID : ObjectID \\
FlatBufferMissionObjectID : ObjectID \\
ReaderObjectID : ObjectID \\
WriterObjectID : ObjectID \\
\hline
distinct\langle FlatBufferObjectID, FlatBufferMissionObjectID, \\
ReaderObjectID, WriterObjectID\rangle
\end{array}
$$

2 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* . *FlatBufferMission*, *done_mission* . *FlatBufferMission*, *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* ==
$\bigcup\{$ *SafeltAppSync*, *MissionSequencerAppSync*, *MissionAppSync*, *MTAppSync*, *OSEHSync*, *APEHSync*, {| *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* |}

section *Program* **parents** *scj_prelude*, *MissionId*, *MissionIds*,
SchedulableId, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *MissionFW*,
SafeletFW, *TopLevelMissionSequencerFW*, *NetworkChannels*, *ManagedThreadFW*,
SchedulableMissionSequencerFW, *PeriodicEventHandlerFW*, *OneShotEventHandlerFW*,
AperiodicEventHandlerFW, *ObjectFW*, *ThreadFW*,
FlatBufferApp, *FlatBufferMissionSequencerApp*, *FlatBufferMissionApp*, *ReaderApp*, *WriterApp*

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

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

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

process $Application \mathrel{\widehat=}$
$$\left(\begin{array}{l} FlatBufferApp \\ ||| \\ FlatBufferMissionSequencerApp \\ ||| \\ FlatBufferMissionApp \\ ||| \\ ReaderApp \\ ||| \\ WriterApp \end{array}\right)$$

process $MethodCallBinder \mathrel{\widehat=}$
$$\left(\begin{array}{l} terminationPending\_MethodBinder \\ ||| \\ read\_MethodBinder \\ ||| \\ terminationPending\_MethodBinder \\ ||| \\ write\_MethodBinder \end{array}\right)$$

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

$terminationPendingLocs == \{FlatBufferMissionID\}$
$terminationPendingCallers == \{ReaderID, WriterID\}$

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

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

$readLocs == \{FlatBufferMissionID\}$
$readCallers == \{ReaderID\}$

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

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

$terminationPendingLocs == \{FlatBufferMissionID\}$
$terminationPendingCallers == \{WriterID\}$

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

channel $binder\_writeCall : MissionID \times SchedulableID$
channel $binder\_writeRet : MissionID \times SchedulableID$

$$writeLocs == \{FlatBufferMissionID\}$$
$$writeCallers == \{WriterID\}$$

$$write\_MethodBinder \mathrel{\widehat{=}} \left(\begin{array}{l} binder\_writeCall \\ \quad ?\, loc : (loc \in writeLocs) \\ \quad ?\, caller : (caller \in writeCallers) \longrightarrow \\ writeCall\,.\,loc\,.\,caller \longrightarrow \\ writeRet\,.\,loc\,.\,caller\,?\,ret \longrightarrow \\ binder\_writeRet\,.\,loc\,.\,caller\,!\,ret \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

process $ApplicationB \mathrel{\widehat{=}} Application \llbracket MethodCallBinderSync \rrbracket MethodCallBinder$

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

process $Objects \mathrel{\widehat{=}}$
$$\left(\begin{array}{l} ObjectFW(FlatBufferObjectID) \\ ||| \\ ObjectFW(FlatBufferMissionObjectID) \\ ||| \\ ObjectFW(ReaderObjectID) \\ ||| \\ ObjectFW(WriterObjectID) \end{array}\right)$$

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

process $Program \mathrel{\widehat{=}} \big(Framework \llbracket AppSync \rrbracket ApplicationB\big) \llbracket LockingSync \rrbracket Locking$

3 Safelet

section *FlatBufferApp* **parents** *scj_prelude*, *SchedulableId*, *SchedulableIds*, *SafeletChan*

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

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

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

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

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

end

4 Top Level Mission Sequencer

section *FlatBufferMissionSequencerApp* **parents** *TopLevelMissionSequencerChan*, *MissionId*, *MissionIds*, *SchedulableId*, *FlatBufferMissionSequencerClass*

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

State

$this : \textbf{ref}\ FlatBufferMissionSequencerClass$

state *State*

Init

$State'$

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

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

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

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

end

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

state *State*

$$returnedMission : \mathbb{B}$$

state *State*

initial *Init*

$$State'$$

$$returnedMission' = false$$

protected *getNextMission* $\widehat{=}$ **var** *ret* : *MissionID* •

$$\begin{pmatrix} \textbf{if } (\neg\ returnedMission = \textbf{True}) \longrightarrow \\ \quad \begin{pmatrix} this\ .\ returnedMission := true; \\ ret := FlatBufferMission \end{pmatrix} \\ [] \neg\ (\neg\ returnedMission = \textbf{True}) \longrightarrow \\ \quad \big(ret := nullMissionId\big) \\ \textbf{fi} \end{pmatrix}$$

• **Skip**

end

5 Missions

5.1 FlatBufferMission

section *FlatBufferMissionApp* **parents** *scj_prelude*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *FlatBufferMissionClass*, *ObjectChan*, *ObjectIds*, *ThreadIds*, *FlatBufferMissionMethChan*

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

State

$this : \mathbf{ref}\ FlatBufferMissionClass$

state *State*

Init

$State'$

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

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

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

$$bufferEmptyMeth \mathrel{\widehat=} \mathbf{var}\ ret : \mathbb{B} \bullet \left(\begin{array}{l} bufferEmptyCall\,.\,FlatBufferMission \longrightarrow \\ ret := this\,.\,bufferEmpty(); \\ bufferEmptyRet\,.\,FlatBufferMission\,!\,ret \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

$$cleanUpMeth \mathrel{\widehat=} \mathbf{var}\ ret : \mathbb{B} \bullet \left(\begin{array}{l} cleanUpCall\,.\,FlatBufferMission \longrightarrow \\ ret := this\,.\,cleanUp(); \\ cleanUpRet\,.\,FlatBufferMission\,!\,ret \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

$$
\begin{array}{l}
writeSyncMeth \mathrel{\widehat=} \\
\left(\begin{array}{l}
writeCall\,.\,FlatBufferMission\,?\,thread\,?\,update \longrightarrow \\
\left(\begin{array}{l}
startSyncMeth\,.\,FlatBufferMissionObject\,.\,thread \longrightarrow \\
lockAcquired\,.\,FlatBufferMissionObject\,.\,thread \longrightarrow \\
\left(\begin{array}{l}
\left(\begin{array}{l}
\mu X \bullet \\
\left(\begin{array}{l}
\textbf{var}\ loopVar : \mathbb{B} \bullet loopVar := (\neg\ bufferEmpty()); \\
\textbf{if}\ (loopVar) \longrightarrow \\
\qquad \left(\begin{array}{l}
waitCall\,.\,FlatBufferMissionObject\,!\,thread \longrightarrow \\
waitRet\,.\,FlatBufferMissionObject\,!\,thread \longrightarrow \\
\textbf{Skip}
\end{array}\right)\ ;\ X \\
[\!]\ \neg\ (loopVar) \longrightarrow \textbf{Skip} \\
\textbf{fi}
\end{array}\right)
\end{array}\right) \\
; \\
this\,.\,buffer := update; \\
notify\,.\,FlatBufferMissionObject\,!\,thread \longrightarrow \\
\textbf{Skip}
\end{array}\right) \\
endSyncMeth\,.\,FlatBufferMissionObject\,.\,thread \longrightarrow \\
writeRet\,.\,FlatBufferMission\,.\,thread \longrightarrow \\
\textbf{Skip}
\end{array}\right)
\end{array}
$$

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

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

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

end

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

state *State*

$buffer : \mathbb{Z}$
$t : testClass$

state *State*

initial *Init*

$State'$

$buffer' = 0$
$t' = testClass$

public *bufferEmpty* $\widehat{=}$ **var** $ret : \mathbb{B}$ •

$$\begin{pmatrix} \textbf{if } (buffer = 0) \longrightarrow \\ \quad ret := \textbf{True} \\ [] \neg (buffer = 0) \longrightarrow \\ \quad ret := \textbf{False} \\ \textbf{fi} \end{pmatrix}$$

public *cleanUp* $\widehat{=}$ **var** $ret : \mathbb{B}$ •
$\big(ret := \textbf{False}\big)$

• **Skip**

end

section *FlatBufferMissionMethChan* **parents** *scj_prelude*, *GlobalTypes*, *MissionId*, *SchedulableId*

channel *bufferEmptyCall* : *SchedulableID*
channel *bufferEmptyRet* : *SchedulableID* $\times$ $\mathbb{B}$

channel *cleanUpCall* : *SchedulableID*
channel *cleanUpRet* : *SchedulableID* $\times$ $\mathbb{B}$

channel *writeCall* : *SchedulableID* $\times$ *ThreadID* $\times$ $\mathbb{Z}$
channel *writeRet* : *SchedulableID* $\times$ *ThreadID*

channel *readCall* : *SchedulableID* $\times$ *ThreadID*
channel *readRet* : *SchedulableID* $\times$ *ThreadID* $\times$ $\mathbb{Z}$

5.2 Schedulables of FlatBufferMission

section *ReaderApp* **parents** *ManagedThreadChan*, *SchedulableId*, *SchedulableIds*
,
MissionMethChan, *FlatBufferMissionMethChan*, *ObjectIds*, *ThreadIds*

process $ReaderApp \mathrel{\widehat=}$
$fbMission : MissionID \bullet$ **begin**

$Run \mathrel{\widehat=}$
$\Big($ *runCall . Reader* $\longrightarrow$
$\Big($ $\Big($ $\Big($ $\Big($ $\mu X \bullet$
$\Big($ *terminationPendingCall . fbMission* $\longrightarrow$
terminationPendingRet . fbMission ? terminationPending $\longrightarrow$
var $loopVar : \mathbb{B} \bullet loopVar := (\neg\ terminationPending)$;
if $(loopVar) \longrightarrow$
$\Big($ **var** $result : \mathbb{Z} \bullet result := 999$;
$\Big($ $\Big($ *readCall . fbMission . ReaderThread* $\longrightarrow$
readRet . fbMission . ReaderThread ? read $\longrightarrow$ $\Big)$ **Skip**
Skip $\Big)$; X
$[]\ \neg\ (loopVar) \longrightarrow$ **Skip**
fi $\Big)$
Skip $\Big)$
runRet . Reader $\longrightarrow$
Skip $\Big)$;

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

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

end

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

state *State*

$fbMission : FlatBufferMission$

state *State*

initial *Init*

$State'$

- **Skip**

end

section *WriterApp* **parents** *ManagedThreadChan*, *SchedulableId*, *SchedulableIds*
,
MissionMethChan, *FlatBufferMissionMethChan*, *ObjectIds*, *ThreadIds*

process $WriterApp \mathrel{\widehat=}$
$fbMission : MissionID \bullet$ **begin**

$Run \mathrel{\widehat=}$
$\Big($ *runCall* . *Writer* $\longrightarrow$
$\Big($ $\Big($ $\Big($ $\mu X \bullet$
$\Big($ *terminationPendingCall* . *fbMission* $\longrightarrow$
terminationPendingRet . *fbMission* ? *terminationPending* $\longrightarrow$
var *loopVar* : $\mathbb{B} \bullet$ *loopVar* := $(\neg$ *terminationPending*);
if (*loopVar*) $\longrightarrow$
$\Big($ $\Big($ *writeCall* . *fbMission* . *WriterThread* ! $i \longrightarrow$
writeRet . *fbMission* . *WriterThread* $\longrightarrow$ $\Big)$;
Skip $\Big)$
$i := i + 1$;
var *keepWriting* : $\mathbb{B} \bullet$ *keepWriting* := $(i \geq 5)$;
if $(\neg$ *keepWriting* = **True**$) \longrightarrow$
$\Big($ *requestTerminationCall* . *fbMission* $\longrightarrow$
requestTerminationRet . *fbMission* ? *requestTermination* $\longrightarrow$ $\Big)$
Skip
$[] \neg (\neg$ *keepWriting* = **True**$) \longrightarrow$ **Skip**
fi ;
Skip $\Big)$
$[] \neg$ (*loopVar*) $\longrightarrow$ **Skip**
fi $\Big)$; X $\Big)$ $\Big)$ $\Big)$;
Skip
runRet . *Writer* $\longrightarrow$
Skip $\Big)$

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

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

end

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

state *State*

$fbMission : FlatBufferMission$

$i : \mathbb{Z}$

state *State*

initial *Init*

$State'$

$i' = 1$

- **Skip**

end