aircraft

Tight Rope v0.75

24th February 2017

1 ID Files

1.1 MissionIds

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

$$MainMissionMID : MissionID$$
$$TakeOffMissionMID : MissionID$$
$$CruiseMissionMID : MissionID$$
$$LandMissionMID : MissionID$$

$$distinct\langle nullMissionId, MainMissionMID, TakeOffMissionMID, CruiseMissionMID, LandMissionMID\rangle$$

1.2 SchedulablesIds

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

$$
\begin{array}{l}
MainMissionSequencerSID : SchedulableID \\
ACModeChanger2SID : SchedulableID \\
EnvironmentMonitorSID : SchedulableID \\
ControlHandlerSID : SchedulableID \\
FlightSensorsMonitorSID : SchedulableID \\
CommunicationsHandlerSID : SchedulableID \\
LandingGearHandlerSID : SchedulableID \\
TakeOffMonitorSID : SchedulableID \\
TakeOffFailureHandlerSID : SchedulableID \\
BeginLandingHandlerSID : SchedulableID \\
NavigationMonitorSID : SchedulableID \\
GroundDistanceMonitorSID : SchedulableID \\
LandingGearHandlerLandSID : SchedulableID \\
InstrumentLandingSystemMonitorSID : SchedulableID \\
SafeLandingHandlerSID : SchedulableID \\
\hline
distinct\langle nullSequencerId, nullSchedulableId, MainMissionSequencerSID, \\
ACModeChanger2SID, EnvironmentMonitorSID, \\
ControlHandlerSID, FlightSensorsMonitorSID, \\
CommunicationsHandlerSID, LandingGearHandlerSID, \\
TakeOffMonitorSID, TakeOffFailureHandlerSID, \\
BeginLandingHandlerSID, NavigationMonitorSID, \\
GroundDistanceMonitorSID, LandingGearHandlerLandSID, \\
InstrumentLandingSystemMonitorSID, SafeLandingHandlerSID\rangle
\end{array}
$$

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 . *TakeOffMission*, *done_mission* . *TakeOffMission*,
initializeRet . *TakeOffMission*, *requestTermination* . *TakeOffMission* . *MainMissionSequencer*,
start_mission . *CruiseMission*, *done_mission* . *CruiseMission*,
initializeRet . *CruiseMission*, *requestTermination* . *CruiseMission* . *MainMissionSequencer*,
start_mission . *LandMission*, *done_mission* . *LandMission*,
initializeRet . *LandMission*, *requestTermination* . *LandMission* . *MainMissionSequencer* |}

2.2 MethodCallBinder

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

channel $binder\_setCabinPressureCall : MissionID \times SchedulableID \times \mathbb{P}\,\mathbb{A}$
channel $binder\_setCabinPressureRet : MissionID \times SchedulableID$

$setCabinPressureLocs == \{MainMissionMID\}$
$setCabinPressureCallers == \{EnvironmentMonitorSID\}$

channel $binder\_setFuelRemainingCall : MissionID \times SchedulableID \times \mathbb{P}\,\mathbb{A}$
channel $binder\_setFuelRemainingRet : MissionID \times SchedulableID$

$setFuelRemainingLocs == \{MainMissionMID\}$
$setFuelRemainingCallers == \{EnvironmentMonitorSID\}$

channel $binder\_getAltitudeCall : MissionID \times SchedulableID$
channel $binder\_getAltitudeRet : MissionID \times SchedulableID \times \mathbb{P}\,\mathbb{A}$

$getAltitudeLocs == \{MainMissionMID\}$
$getAltitudeCallers == \{NavigationMonitorSID, TakeOffMonitorSID, GroundDistanceMonitorSID, SafeLandingHandlerS$

channel $binder\_setHeadingCall : MissionID \times SchedulableID \times \mathbb{P}\,\mathbb{A}$
channel $binder\_setHeadingRet : MissionID \times SchedulableID$

$setHeadingLocs == \{MainMissionMID\}$
$setHeadingCallers == \{FlightSensorsMonitorSID\}$

channel $binder\_stowLandingGearCall : MissionID \times SchedulableID$
channel $binder\_stowLandingGearRet : MissionID \times SchedulableID$

$stowLandingGearLocs == \{TakeOffMissionMID, LandMissionMID\}$
$stowLandingGearCallers == \{LandingGearHandlerSID, LandingGearHandlerLandSID\}$

channel $binder\_takeOffAbortCall : MissionID \times SchedulableID$
channel $binder\_takeOffAbortRet : MissionID \times SchedulableID$

$takeOffAbortLocs == \{TakeOffMissionMID\}$
$takeOffAbortCallers == \{TakeOffFailureHandlerSID\}$

channel $binder\_setAltitudeCall : MissionID \times SchedulableID \times \mathbb{P}\,\mathbb{A}$
channel $binder\_setAltitudeRet : MissionID \times SchedulableID$

$setAltitudeLocs == \{MainMissionMID\}$
$setAltitudeCallers == \{FlightSensorsMonitorSID\}$

channel $binder\_getHeadingCall : MissionID \times SchedulableID$
channel $binder\_getHeadingRet : MissionID \times SchedulableID \times \mathbb{P}\,\mathbb{A}$

$getHeadingLocs == \{MainMissionMID\}$
$getHeadingCallers == \{NavigationMonitorSID\}$

channel $binder\_getAirSpeedCall : MissionID \times SchedulableID$
channel $binder\_getAirSpeedRet : MissionID \times SchedulableID \times \mathbb{P}\,\mathbb{A}$

$getAirSpeedLocs == \{MainMissionMID\}$
$getAirSpeedCallers == \{NavigationMonitorSID, TakeOffFailureHandlerSID\}$

channel $binder\_deployLandingGearCall : MissionID \times SchedulableID$
channel $binder\_deployLandingGearRet : MissionID \times SchedulableID$

$deployLandingGearLocs == \{TakeOffMissionMID, LandMissionMID\}$
$deployLandingGearCallers == \{LandingGearHandlerSID, LandingGearHandlerLandSID\}$

channel $binder\_setEmergencyOxygenCall : MissionID \times SchedulableID \times \mathbb{P}\,\mathbb{A}$
channel $binder\_setEmergencyOxygenRet : MissionID \times SchedulableID$

$setEmergencyOxygenLocs == \{MainMissionMID\}$
$setEmergencyOxygenCallers == \{EnvironmentMonitorSID\}$

channel $binder\_setAirSpeedCall : MissionID \times SchedulableID \times \mathbb{P}\,\mathbb{A}$
channel $binder\_setAirSpeedRet : MissionID \times SchedulableID$

$setAirSpeedLocs == \{MainMissionMID\}$
$setAirSpeedCallers == \{FlightSensorsMonitorSID\}$

channel $binder\_isLandingGearDeployedCall : MissionID \times SchedulableID$
channel $binder\_isLandingGearDeployedRet : MissionID \times SchedulableID \times \mathbb{B}$

$isLandingGearDeployedLocs == \{TakeOffMissionMID, LandMissionMID\}$
$isLandingGearDeployedCallers == \{LandingGearHandlerSID, LandingGearHandlerLandSID\}$

channelset $MethodCallBinderSync == \{\!|\ done\_toplevel\_sequencer,$
$binder\_setCabinPressureCall, binder\_setCabinPressureRet,$
$binder\_setFuelRemainingCall, binder\_setFuelRemainingRet,$
$binder\_getAltitudeCall, binder\_getAltitudeRet,$
$binder\_setHeadingCall, binder\_setHeadingRet,$
$binder\_stowLandingGearCall, binder\_stowLandingGearRet,$
$binder\_takeOffAbortCall, binder\_takeOffAbortRet,$
$binder\_setAltitudeCall, binder\_setAltitudeRet,$
$binder\_getHeadingCall, binder\_getHeadingRet,$
$binder\_getAirSpeedCall, binder\_getAirSpeedRet,$
$binder\_deployLandingGearCall, binder\_deployLandingGearRet,$
$binder\_setEmergencyOxygenCall, binder\_setEmergencyOxygenRet,$
$binder\_setAirSpeedCall, binder\_setAirSpeedRet,$
$binder\_isLandingGearDeployedCall, binder\_isLandingGearDeployedRet\ |\!\}$

section *MethodCallBinder* **parents** *scj_prelude*, *MissionId*, *MissionIds*,
SchedulableId, *SchedulableIds*, *MethodCallBindingChannels*
, *MainMissionMethChan*, *LandMissionMethChan*

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

$setCabinPressure\_MethodBinder \mathrel{\widehat=}$
$(binder\_setCabinPressureCall\,?\,loc : (loc \in setCabinPressureLocs)\,?\,caller : (caller \in setCabinPressureCallers)\,?\,p1-$
$setCabinPressureCall\,.\,loc\,.\,caller\,!\,p1 \longrightarrow$
$setCabinPressureRet\,.\,loc\,.\,caller \longrightarrow$
$binder\_setCabinPressureRet\,.\,loc\,.\,caller \longrightarrow$
$setCabinPressure\_MethodBinder)$

$setFuelRemaining\_MethodBinder \mathrel{\widehat=}$
$(binder\_setFuelRemainingCall\,?\,loc : (loc \in setFuelRemainingLocs)\,?\,caller : (caller \in setFuelRemainingCallers)\,?\,p1$
$setFuelRemainingCall\,.\,loc\,.\,caller\,!\,p1 \longrightarrow$
$setFuelRemainingRet\,.\,loc\,.\,caller \longrightarrow$
$binder\_setFuelRemainingRet\,.\,loc\,.\,caller \longrightarrow$
$setFuelRemaining\_MethodBinder)$

$getAltitude\_MethodBinder \mathrel{\widehat=}$
$(binder\_getAltitudeCall\,?\,loc : (loc \in getAltitudeLocs)\,?\,caller : (caller \in getAltitudeCallers) \longrightarrow$
$getAltitudeCall\,.\,loc\,.\,caller \longrightarrow$
$getAltitudeRet\,.\,loc\,.\,caller\,?\,ret \longrightarrow$
$binder\_getAltitudeRet\,.\,loc\,.\,caller\,!\,ret \longrightarrow$
$getAltitude\_MethodBinder)$

$setHeading\_MethodBinder \mathrel{\widehat=}$
$(binder\_setHeadingCall\,?\,loc : (loc \in setHeadingLocs)\,?\,caller : (caller \in setHeadingCallers)\,?\,p1 \longrightarrow$
$setHeadingCall\,.\,loc\,.\,caller\,!\,p1 \longrightarrow$
$setHeadingRet\,.\,loc\,.\,caller \longrightarrow$
$binder\_setHeadingRet\,.\,loc\,.\,caller \longrightarrow$
$setHeading\_MethodBinder)$

$stowLandingGear\_MethodBinder \mathrel{\widehat=}$
$(binder\_stowLandingGearCall\,?\,loc : (loc \in stowLandingGearLocs)\,?\,caller : (caller \in stowLandingGearCallers) \longrightarrow$
$stowLandingGearCall\,.\,loc\,.\,caller \longrightarrow$
$stowLandingGearRet\,.\,loc\,.\,caller \longrightarrow$
$binder\_stowLandingGearRet\,.\,loc\,.\,caller \longrightarrow$
$stowLandingGear\_MethodBinder)$

$takeOffAbort\_MethodBinder \mathrel{\widehat=}$
$(binder\_takeOffAbortCall\,?\,loc : (loc \in takeOffAbortLocs)\,?\,caller : (caller \in takeOffAbortCallers) \longrightarrow$
$takeOffAbortCall\,.\,loc\,.\,caller \longrightarrow$
$takeOffAbortRet\,.\,loc\,.\,caller \longrightarrow$
$binder\_takeOffAbortRet\,.\,loc\,.\,caller \longrightarrow$
$takeOffAbort\_MethodBinder)$

$setAltitude\_MethodBinder \mathrel{\widehat=}$
$(binder\_setAltitudeCall\,?\,loc : (loc \in setAltitudeLocs)\,?\,caller : (caller \in setAltitudeCallers)\,?\,p1 \longrightarrow$
$setAltitudeCall\,.\,loc\,.\,caller\,!\,p1 \longrightarrow$
$setAltitudeRet\,.\,loc\,.\,caller \longrightarrow$
$binder\_setAltitudeRet\,.\,loc\,.\,caller \longrightarrow$
$setAltitude\_MethodBinder)$

$$getHeading\_MethodBinder \mathrel{\widehat{=}} \left(\begin{array}{l} binder\_getHeadingCall\,?\,loc : (loc \in getHeadingLocs)\,?\,caller : (caller \in getHeadingCallers) \longrightarrow \\ getHeadingCall\,.\,loc\,.\,caller \longrightarrow \\ getHeadingRet\,.\,loc\,.\,caller\,?\,ret \longrightarrow \\ binder\_getHeadingRet\,.\,loc\,.\,caller\,!\,ret \longrightarrow \\ getHeading\_MethodBinder \end{array}\right)$$

$$getAirSpeed\_MethodBinder \mathrel{\widehat{=}} \left(\begin{array}{l} binder\_getAirSpeedCall\,?\,loc : (loc \in getAirSpeedLocs)\,?\,caller : (caller \in getAirSpeedCallers) \longrightarrow \\ getAirSpeedCall\,.\,loc\,.\,caller \longrightarrow \\ getAirSpeedRet\,.\,loc\,.\,caller\,?\,ret \longrightarrow \\ binder\_getAirSpeedRet\,.\,loc\,.\,caller\,!\,ret \longrightarrow \\ getAirSpeed\_MethodBinder \end{array}\right)$$

$$deployLandingGear\_MethodBinder \mathrel{\widehat{=}} \left(\begin{array}{l} binder\_deployLandingGearCall\,?\,loc : (loc \in deployLandingGearLocs)\,?\,caller : (caller \in deployLandingGearCallers) \\ deployLandingGearCall\,.\,loc\,.\,caller \longrightarrow \\ deployLandingGearRet\,.\,loc\,.\,caller \longrightarrow \\ binder\_deployLandingGearRet\,.\,loc\,.\,caller \longrightarrow \\ deployLandingGear\_MethodBinder \end{array}\right)$$

$$setEmergencyOxygen\_MethodBinder \mathrel{\widehat{=}} \left(\begin{array}{l} binder\_setEmergencyOxygenCall\,?\,loc : (loc \in setEmergencyOxygenLocs)\,?\,caller : (caller \in setEmergencyOxygenCa \\ setEmergencyOxygenCall\,.\,loc\,.\,caller\,!\,p1 \longrightarrow \\ setEmergencyOxygenRet\,.\,loc\,.\,caller \longrightarrow \\ binder\_setEmergencyOxygenRet\,.\,loc\,.\,caller \longrightarrow \\ setEmergencyOxygen\_MethodBinder \end{array}\right)$$

$$setAirSpeed\_MethodBinder \mathrel{\widehat{=}} \left(\begin{array}{l} binder\_setAirSpeedCall\,?\,loc : (loc \in setAirSpeedLocs)\,?\,caller : (caller \in setAirSpeedCallers)\,?\,p1 \longrightarrow \\ setAirSpeedCall\,.\,loc\,.\,caller\,!\,p1 \longrightarrow \\ setAirSpeedRet\,.\,loc\,.\,caller \longrightarrow \\ binder\_setAirSpeedRet\,.\,loc\,.\,caller \longrightarrow \\ setAirSpeed\_MethodBinder \end{array}\right)$$

$$isLandingGearDeployed\_MethodBinder \mathrel{\widehat{=}} \left(\begin{array}{l} binder\_isLandingGearDeployedCall\,?\,loc : (loc \in isLandingGearDeployedLocs)\,?\,caller : (caller \in isLandingGearDep \\ isLandingGearDeployedCall\,.\,loc\,.\,caller \longrightarrow \\ isLandingGearDeployedRet\,.\,loc\,.\,caller\,?\,ret \longrightarrow \\ binder\_isLandingGearDeployedRet\,.\,loc\,.\,caller\,!\,ret \longrightarrow \\ isLandingGearDeployed\_MethodBinder \end{array}\right)$$

$$
\begin{array}{l}
BinderActions \mathrel{\widehat{=}} \\
\left(\begin{array}{l}
setCabinPressure\_MethodBinder \\
|||\\
setFuelRemaining\_MethodBinder \\
|||\\
getAltitude\_MethodBinder \\
|||\\
setHeading\_MethodBinder \\
|||\\
stowLandingGear\_MethodBinder \\
|||\\
takeOffAbort\_MethodBinder \\
|||\\
setAltitude\_MethodBinder \\
|||\\
getHeading\_MethodBinder \\
|||\\
getAirSpeed\_MethodBinder \\
|||\\
deployLandingGear\_MethodBinder \\
|||\\
setEmergencyOxygen\_MethodBinder \\
|||\\
setAirSpeed\_MethodBinder \\
|||\\
isLandingGearDeployed\_MethodBinder
\end{array}\right)
\end{array}
$$

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

end

2.3 Locking

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

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

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

process *Locking* $\widehat{=}$ *Threads* $[\![$ *ThreadSync* $]\!]$ *Objects*

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*,
ACSafeletApp, *MainMissionSequencerApp*, *MainMissionApp*, *ACModeChanger2App*, *ControlHandlerApp*,
CommunicationsHandlerApp, *EnvironmentMonitorApp*, *FlightSensorsMonitorApp*
, *TakeOffMissionApp*, *LandingGearHandlerApp*, *TakeOffFailureHandlerApp*,
TakeOffMonitorApp, *CruiseMissionApp*, *BeginLandingHandlerApp*, *NavigationMonitorApp*
, *LandMissionApp*, *LandingGearHandlerLandApp*, *SafeLandingHandlerApp*, *GroundDistanceMonitorApp*,
InstrumentLandingSystemMonitorApp

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

process $Tier0 \mathrel{\widehat=}$
$$\left(\begin{array}{l} MissionFW(MainMissionID) \\ \quad [\![MissionSync]\!] \\ \left(\begin{array}{l} SchedulableMissionSequencerFW(ACModeChanger2ID) \\ \quad [\![SchedulablesSync]\!] \\ AperiodicEventHandlerFW(ControlHandlerID, aperiodic, (time(10,0), nullSchedulableId)) \\ \quad [\![SchedulablesSync]\!] \\ AperiodicEventHandlerFW(CommunicationsHandlerID, aperiodic, (NULL, nullSchedulableId)) \\ \quad [\![SchedulablesSync]\!] \\ PeriodicEventHandlerFW(EnvironmentMonitorID, (time(10,0), NULL, NULL, nullSchedulableId)) \\ \quad [\![SchedulablesSync]\!] \\ PeriodicEventHandlerFW(FlightSensorsMonitorID, (time(10,0), NULL, NULL, nullSchedulableId)) \end{array}\right) \end{array}\right)$$

process $Tier1 \mathrel{\widehat=}$
$$\left(\begin{array}{l} MissionFW(TakeOffMissionID) \\ \quad [\![MissionSync]\!] \\ \left(\begin{array}{l} AperiodicEventHandlerFW(LandingGearHandlerID, aperiodic, (NULL, nullSchedulableId)) \\ \quad [\![SchedulablesSync]\!] \\ AperiodicEventHandlerFW(TakeOffFailureHandlerID, aperiodic, (NULL, nullSchedulableId)) \\ \quad [\![SchedulablesSync]\!] \\ PeriodicEventHandlerFW(TakeOffMonitorID, (time(0,0), time(500,0), NULL, nullSchedulableId)) \end{array}\right) \end{array}\right)$$
$$[\![ClusterSync]\!]$$
$$\left(\begin{array}{l} MissionFW(CruiseMissionID) \\ \quad [\![MissionSync]\!] \\ \left(\begin{array}{l} AperiodicEventHandlerFW(BeginLandingHandlerID, aperiodic, (NULL, nullSchedulableId)) \\ \quad [\![SchedulablesSync]\!] \\ PeriodicEventHandlerFW(NavigationMonitorID, (time(0,0), time(10,0), NULL, nullSchedulableId)) \end{array}\right) \end{array}\right)$$
$$[\![ClusterSync]\!]$$
$$\left(\begin{array}{l} MissionFW(LandMissionID) \\ \quad [\![MissionSync]\!] \\ \left(\begin{array}{l} AperiodicEventHandlerFW(LandingGearHandlerLandID, aperiodic, (NULL, nullSchedulableId)) \\ \quad [\![SchedulablesSync]\!] \\ AperiodicEventHandlerFW(SafeLandingHandlerID, aperiodic, (NULL, nullSchedulableId)) \\ \quad [\![SchedulablesSync]\!] \\ PeriodicEventHandlerFW(GroundDistanceMonitorID, (time(0,0), time(10,0), NULL, nullSchedulableId)) \\ \quad [\![SchedulablesSync]\!] \\ PeriodicEventHandlerFW(InstrumentLandingSystemMonitorID, (time(0,0), time(10,0), NULL, nullSchedulableId)) \end{array}\right) \end{array}\right)$$

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

$$\textbf{process}\ Application \mathrel{\widehat{=}} \left(\begin{array}{l} ACSafeletApp \\ ||| \\ MainMissionSequencerApp \\ ||| \\ MainMissionApp \\ ||| \\ ACModeChanger2App(MainMissionID) \\ ||| \\ ControlHandlerApp \\ ||| \\ CommunicationsHandlerApp \\ ||| \\ EnvironmentMonitorApp(MainMissionID) \\ ||| \\ FlightSensorsMonitorApp(MainMissionID) \\ ||| \\ TakeOffMissionApp \\ ||| \\ LandingGearHandlerApp(TakeOffMissionID) \\ ||| \\ TakeOffFailureHandlerApp(MissionID, TakeOffMissionID, 10.0) \\ ||| \\ TakeOffMonitorApp(MissionID, TakeOffMissionID, 10.0, landingGearHandlerID) \\ ||| \\ CruiseMissionApp \\ ||| \\ BeginLandingHandlerApp(MissionID) \\ ||| \\ NavigationMonitorApp(MissionID) \\ ||| \\ LandMissionApp \\ ||| \\ LandingGearHandlerLandApp(LandMissionID) \\ ||| \\ SafeLandingHandlerApp(MissionID, 10.0) \\ ||| \\ GroundDistanceMonitorApp(MissionID) \\ ||| \\ InstrumentLandingSystemMonitorApp(LandMissionID) \end{array}\right)$$

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

3 Safelet

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

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

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

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

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

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

end

4 Top Level Mission Sequencer

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

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

State

$this : \textbf{ref}\ MainMissionSequencerClass$

state *State*

Init

$State'$

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

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

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

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

end

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

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

state *State*

$$returnedMission : \mathbb{B}$$

state *State*

initial *Init*

$$State'$$

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

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

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

$\bullet$ **Skip**

end

5 Missions

5.1 MainMission

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

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

State

$this : \mathbf{ref}\ MainMissionClass$

state *State*

Init

$State'$

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

$InitializePhase \mathrel{\widehat=}$
$\left(\begin{array}{l} initializeCall\,.\,MainMissionMID \longrightarrow \\ register\,!\,ACModeChanger2SID\,!\,MainMissionMID \longrightarrow \\ register\,!\,EnvironmentMonitorSID\,!\,MainMissionMID \longrightarrow \\ register\,!\,ControlHandlerSID\,!\,MainMissionMID \longrightarrow \\ register\,!\,FlightSensorsMonitorSID\,!\,MainMissionMID \longrightarrow \\ register\,!\,CommunicationsHandlerSID\,!\,MainMissionMID \longrightarrow \\ initializeRet\,.\,MainMissionMID \longrightarrow \\ \mathbf{Skip} \end{array}\right)$

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

$getAirSpeedMeth \mathrel{\widehat=} \mathbf{var}\ ret : \mathbb{P}\,\mathbb{A} \bullet$
$\left(\begin{array}{l} getAirSpeedCall\,.\,MainMissionMID\,?\,caller \longrightarrow \\ ret := this\,.\,getAirSpeed(); \\ getAirSpeedRet\,.\,MainMissionMID\,.\,caller\,!\,ret \longrightarrow \\ \mathbf{Skip} \end{array}\right)$

$getAltitudeMeth \mathrel{\widehat=} \mathbf{var}\ ret : \mathbb{P}\,\mathbb{A} \bullet$
$\left(\begin{array}{l} getAltitudeCall\,.\,MainMissionMID\,?\,caller \longrightarrow \\ ret := this\,.\,getAltitude(); \\ getAltitudeRet\,.\,MainMissionMID\,.\,caller\,!\,ret \longrightarrow \\ \mathbf{Skip} \end{array}\right)$

$getCabinPressureMeth \mathrel{\widehat=} \mathbf{var}\ ret : \mathbb{P}\,\mathbb{A} \bullet$
$\left(\begin{array}{l} getCabinPressureCall\,.\,MainMissionMID \longrightarrow \\ ret := this\,.\,getCabinPressure(); \\ getCabinPressureRet\,.\,MainMissionMID\,!\,ret \longrightarrow \\ \mathbf{Skip} \end{array}\right)$

$$getEmergencyOxygenMeth \mathrel{\widehat=} \textbf{var}\ ret : \mathbb{P}\,\mathbb{A} \bullet \left(\begin{array}{l} getEmergencyOxygenCall\,.\,MainMissionMID \longrightarrow \\ ret := this\,.\,getEmergencyOxygen(); \\ getEmergencyOxygenRet\,.\,MainMissionMID\,!\,ret \longrightarrow \\ \textbf{Skip} \end{array}\right)$$

$$getFuelRemainingMeth \mathrel{\widehat=} \textbf{var}\ ret : \mathbb{P}\,\mathbb{A} \bullet \left(\begin{array}{l} getFuelRemainingCall\,.\,MainMissionMID \longrightarrow \\ ret := this\,.\,getFuelRemaining(); \\ getFuelRemainingRet\,.\,MainMissionMID\,!\,ret \longrightarrow \\ \textbf{Skip} \end{array}\right)$$

$$getHeadingMeth \mathrel{\widehat=} \textbf{var}\ ret : \mathbb{P}\,\mathbb{A} \bullet \left(\begin{array}{l} getHeadingCall\,.\,MainMissionMID\,?\,caller \longrightarrow \\ ret := this\,.\,getHeading(); \\ getHeadingRet\,.\,MainMissionMID\,.\,caller\,!\,ret \longrightarrow \\ \textbf{Skip} \end{array}\right)$$

$$setAirSpeedMeth \mathrel{\widehat=} \left(\begin{array}{l} setAirSpeedCall\,.\,MainMissionMID\,?\,caller\,?\,airSpeed \longrightarrow \\ this\,.\,setAirSpeed(airSpeed); \\ setAirSpeedRet\,.\,MainMissionMID\,.\,caller \longrightarrow \\ \textbf{Skip} \end{array}\right)$$

$$setAltitudeMeth \mathrel{\widehat=} \left(\begin{array}{l} setAltitudeCall\,.\,MainMissionMID\,?\,caller\,?\,altitude \longrightarrow \\ this\,.\,setAltitude(altitude); \\ setAltitudeRet\,.\,MainMissionMID\,.\,caller \longrightarrow \\ \textbf{Skip} \end{array}\right)$$

$$setCabinPressureMeth \mathrel{\widehat=} \left(\begin{array}{l} setCabinPressureCall\,.\,MainMissionMID\,?\,caller\,?\,cabinPressure \longrightarrow \\ this\,.\,setCabinPressure(cabinPressure); \\ setCabinPressureRet\,.\,MainMissionMID\,.\,caller \longrightarrow \\ \textbf{Skip} \end{array}\right)$$

$$setEmergencyOxygenMeth \mathrel{\widehat=} \left(\begin{array}{l} setEmergencyOxygenCall\,.\,MainMissionMID\,?\,caller\,?\,emergencyOxygen \longrightarrow \\ this\,.\,setEmergencyOxygen(emergencyOxygen); \\ setEmergencyOxygenRet\,.\,MainMissionMID\,.\,caller \longrightarrow \\ \textbf{Skip} \end{array}\right)$$

$$setFuelRemainingMeth \mathrel{\widehat=} \left(\begin{array}{l} setFuelRemainingCall\,.\,MainMissionMID\,?\,caller\,?\,fuelRemaining \longrightarrow \\ this\,.\,setFuelRemaining(fuelRemaining); \\ setFuelRemainingRet\,.\,MainMissionMID\,.\,caller \longrightarrow \\ \textbf{Skip} \end{array}\right)$$

$$setHeadingMeth \mathrel{\widehat=} \left(\begin{array}{l} setHeadingCall\,.\,MainMissionMID\,?\,caller\,?\,heading \longrightarrow \\ this\,.\,setHeading(heading); \\ setHeadingRet\,.\,MainMissionMID\,.\,caller \longrightarrow \\ \textbf{Skip} \end{array}\right)$$

$$Methods \mathrel{\widehat{=}} \left(\begin{array}{l} InitializePhase \\ \Box \\ CleanupPhase \\ \Box \\ getAirSpeedMeth \\ \Box \\ getAltitudeMeth \\ \Box \\ getCabinPressureMeth \\ \Box \\ getEmergencyOxygenMeth \\ \Box \\ getFuelRemainingMeth \\ \Box \\ getHeadingMeth \\ \Box \\ setAirSpeedMeth \\ \Box \\ setAltitudeMeth \\ \Box \\ setCabinPressureMeth \\ \Box \\ setEmergencyOxygenMeth \\ \Box \\ setFuelRemainingMeth \\ \Box \\ setHeadingMeth \end{array} \right) ; \; Methods$$

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

end

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

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

state *State*

$ALTITUDE\_READING\_ON\_GROUND : \mathbb{P}\,\mathbb{A}$
$cabinPressure : \mathbb{P}\,\mathbb{A}$
$emergencyOxygen : \mathbb{P}\,\mathbb{A}$
$fuelRemaining : \mathbb{P}\,\mathbb{A}$
$altitude : \mathbb{P}\,\mathbb{A}$
$airSpeed : \mathbb{P}\,\mathbb{A}$
$heading : \mathbb{P}\,\mathbb{A}$

state *State*

initial *Init*

$State'$

$ALTITUDE\_READING\_ON\_GROUND' = 0.0$

public *getAirSpeed* $\widehat{=}$ **var** $ret : \mathbb{P}\,\mathbb{A}$ •

public *getAltitude* $\widehat{=}$ **var** $ret : \mathbb{P}\,\mathbb{A}$ •

public *getCabinPressure* $\widehat{=}$ **var** $ret : \mathbb{P}\,\mathbb{A}$ •

public *getEmergencyOxygen* $\widehat{=}$ **var** $ret : \mathbb{P}\,\mathbb{A}$ •

public *getFuelRemaining* $\widehat{=}$ **var** $ret : \mathbb{P}\,\mathbb{A}$ •

public *getHeading* $\widehat{=}$ **var** $ret : \mathbb{P}\,\mathbb{A}$ •

public *setAirSpeed* $\widehat{=}$

public *setAltitude* $\widehat{=}$

public *setCabinPressure* $\widehat{=}$

public *setEmergencyOxygen* $\widehat{=}$

public *setFuelRemaining* $\widehat{=}$

public *setHeading* $\widehat{=}$

- **Skip**

end

5.2 Schedulables of MainMission

section $ACModeChanger2App$ **parents** $TopLevelMissionSequencerChan$,
$MissionId$, $MissionIds$, $SchedulableId$, $SchedulableIds$, $ACModeChanger2Class$, $MethodCallBindingChannels$

process $ACModeChanger2App \mathrel{\widehat=}$
$controllingMission : MissionID \bullet$ **begin**

State

$controllingMission : MainMission$

state $State$

Init

$State'$

$controllingMission' =$

$GetNextMission \mathrel{\widehat=}$ **var** $ret : MissionID \bullet$
$\left(\begin{array}{l} getNextMissionCall \,.\, ACModeChanger2SID \longrightarrow \\ ret := this \,.\, getNextMission(); \\ getNextMissionRet \,.\, ACModeChanger2SID \,!\, ret \longrightarrow \\ \textbf{Skip} \end{array}\right)$

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

$\bullet\ (Init \;;\; Methods) \triangle (end\_sequencer\_app \,.\, ACModeChanger2SID \longrightarrow \textbf{Skip})$

end

section $ACModeChanger2Class$ **parents** $scj\_prelude$, $SchedulableId$, $SchedulableIds$, $SafeletChan$, $MethodCallBindingChannels$, $MissionId$, $MissionIds$

class $ACModeChanger2Class \mathrel{\widehat=}$ **begin**

state $State$

$$modesLeft : \mathbb{Z}$$

state $State$

initial $Init$

$$State'$$

$$modesLeft' = 3$$

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

$$\left(\begin{array}{l}
\textbf{if } (modesLeft = 3) \longrightarrow \\
\quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ ret := TakeOffMissionMID \end{array}\right) \\
[]\ \neg\,(modesLeft = 3) \longrightarrow \\
\quad \textbf{if } (modesLeft = 2) \longrightarrow \\
\quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ ret := CruiseMissionMID \end{array}\right) \\
[]\ \neg\,(modesLeft = 2) \longrightarrow \\
\quad \textbf{if } (modesLeft = 1) \longrightarrow \\
\quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ ret := LandMissionMID \end{array}\right) \\
[]\ \neg\,(modesLeft = 1) \longrightarrow \\
\quad \big(ret := nullMissionId\big) \\
\textbf{fi} \\
\textbf{fi} \\
\textbf{fi}
\end{array}\right)$$

• **Skip**

end

section *ControlHandlerApp* **parents** *AperiodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBindingCh*

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

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

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

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

end

section *CommunicationsHandlerApp* **parents** *AperiodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCallB*

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

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

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

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

end

section *EnvironmentMonitorApp* **parents** *PeriodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBindin*
, *MainMissionMethChan*

process $EnvironmentMonitorApp \mathrel{\widehat=}$
$mainMission : MissionID \bullet$ **begin**

State

$controllingMission : MainMission$

state *State*

Init

$State'$

$controllingMission' =$

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

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

$\bullet\ (Init\ ;\ Methods) \triangle (end\_periodic\_app\,.\,EnvironmentMonitorSID \longrightarrow \mathbf{Skip})$

end

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

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

state *State*

$controllingMission : MainMission$

state *State*

initial *Init*

$State'$

- **Skip**

end

section *FlightSensorsMonitorApp* **parents** *PeriodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBindi*
, *MainMissionMethChan*

process $FlightSensorsMonitorApp \mathrel{\widehat=}$
$mainMission : MissionID \bullet$ **begin**

State

$controllingMission : MainMission$

state *State*

Init

$State'$

$controllingMission' =$

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

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

$\bullet\ (Init\ ;\ \ Methods) \triangle (end\_periodic\_app\,.\,FlightSensorsMonitorSID \longrightarrow \mathbf{Skip})$

end

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

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

state *State*

$controllingMission : MainMission$

state *State*

initial *Init*

$State'$

- **Skip**

end

5.3 TakeOffMission

section *TakeOffMissionApp* **parents** *scj_prelude*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *TakeOffMissionMethChan*, *TakeOffMissionClass*, *MethodCallBindingChannels*

process $TakeOffMissionApp \mathrel{\widehat=}$
$controllingMission : MissionID \bullet$ **begin**

State

$this : \mathbf{ref}\ TakeOffMissionClass$
$controllingMission : MainMission$

state *State*

Init

$State'$

$this' = \mathbf{new}\ TakeOffMissionClass()$
$controllingMission' =$

$InitializePhase \mathrel{\widehat=}$
$\begin{pmatrix} initializeCall\ .\ TakeOffMissionMID \longrightarrow \\ register\ !\ LandingGearHandlerSID\ !\ TakeOffMissionMID \longrightarrow \\ register\ !\ TakeOffMonitorSID\ !\ TakeOffMissionMID \longrightarrow \\ register\ !\ TakeOffFailureHandlerSID\ !\ TakeOffMissionMID \longrightarrow \\ initializeRet\ .\ TakeOffMissionMID \longrightarrow \\ \mathbf{Skip} \end{pmatrix}$

$CleanupPhase \mathrel{\widehat=}$
$\begin{pmatrix} \mathbf{var}\ \mathbb{B} : ret \bullet \\ cleanupMissionCall\ .\ TakeOffMissionMID \longrightarrow \\ \\ cleanupMissionRet\ .\ TakeOffMissionMID\ !\ ret \longrightarrow \\ \mathbf{Skip} \end{pmatrix}$

$takeOffAbortMeth \mathrel{\widehat=}$
$\begin{pmatrix} takeOffAbortCall\ .\ TakeOffMissionMID\ ?\ caller \longrightarrow \\ this\ .\ takeOffAbort(); \\ takeOffAbortRet\ .\ TakeOffMissionMID\ .\ caller \longrightarrow \\ \mathbf{Skip} \end{pmatrix}$

$deployLandingGearMeth \mathrel{\widehat=}$
$\begin{pmatrix} deployLandingGearCall\ .\ TakeOffMissionMID\ ?\ caller \longrightarrow \\ this\ .\ deployLandingGear(); \\ deployLandingGearRet\ .\ TakeOffMissionMID\ .\ caller \longrightarrow \\ \mathbf{Skip} \end{pmatrix}$

$stowLandingGearMeth \mathrel{\widehat=}$
$\begin{pmatrix} stowLandingGearCall\ .\ TakeOffMissionMID\ ?\ caller \longrightarrow \\ this\ .\ stowLandingGear(); \\ stowLandingGearRet\ .\ TakeOffMissionMID\ .\ caller \longrightarrow \\ \mathbf{Skip} \end{pmatrix}$

$$isLandingGearDeployedMeth \mathrel{\widehat=} \textbf{var}\ ret : \mathbb{B} \bullet \left(\begin{array}{l} isLandingGearDeployedCall\ .\ TakeOffMissionMID\ ?\ caller \longrightarrow \\ ret := this\ .\ isLandingGearDeployed(); \\ isLandingGearDeployedRet\ .\ TakeOffMissionMID\ .\ caller\ !\ ret \longrightarrow \\ \textbf{Skip} \end{array}\right)$$

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

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

end

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

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

state *State*

$SAFE\_AIRSPEED\_THRESHOLD : \mathbb{P}\,\mathbb{A}$
$TAKEOFF\_ALTITUDE : \mathbb{P}\,\mathbb{A}$
$abort : \mathbb{B}$
$landingGearDeployed : \mathbb{B}$

state *State*

initial *Init*

$State'$

$SAFE\_AIRSPEED\_THRESHOLD' = 10.0$
$TAKEOFF\_ALTITUDE' = 10.0$
$abort' = false$

public *takeOffAbort* $\widehat{=}$

public *deployLandingGear* $\widehat{=}$

public *stowLandingGear* $\widehat{=}$

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

• **Skip**

end

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

channel *takeOffAbortCall* : $MissionID \times SchedulableID$
channel *takeOffAbortRet* : $MissionID \times SchedulableID$

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

channel *stowLandingGearCall* : $MissionID \times SchedulableID$
channel *stowLandingGearRet* : $MissionID \times SchedulableID$

channel *isLandingGearDeployedCall* : $MissionID \times SchedulableID$
channel *isLandingGearDeployedRet* : $MissionID \times SchedulableID \times \mathbb{B}$

channel *deployLandingGearCall* : $MissionID \times SchedulableID \times ThreadID$
channel *deployLandingGearRet* : $MissionID \times SchedulableID \times ThreadID$

5.4 Schedulables of TakeOffMission

section *LandingGearHandlerApp* **parents** *AperiodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBindi*
, *TakeOffMissionMethChan*

process $LandingGearHandlerApp \mathrel{\widehat=}$
$mission : MissionID \bullet$ **begin**

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

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

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

end

section *TakeOffFailureHandlerApp* **parents** *AperiodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBin*
, *MainMissionMethChan*, *TakeOffMissionMethChan*

process $TakeOffFailureHandlerApp \mathrel{\widehat=}$
$mainMission : MissionID,$
$takeoffMission : MissionID,$
$threshold : \mathbb{P}\,\mathbb{A} \bullet$ **begin**

$handleAsyncEvent \mathrel{\widehat=}$
$\begin{pmatrix} handleAsyncEventCall\,.\,TakeOffFailureHandlerSID \longrightarrow \\ ; \\ handleAsyncEventRet\,.\,TakeOffFailureHandlerSID \longrightarrow \\ \mathbf{Skip} \end{pmatrix}$

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

$\bullet\ (Methods) \triangle (end\_aperiodic\_app\,.\,TakeOffFailureHandlerSID \longrightarrow \mathbf{Skip})$

end

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

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

state *State*

$threshold : \mathbb{P}\,\mathbb{A}$

state *State*

initial *Init*

$State'$

- **Skip**

end

section *TakeOffMonitorApp* **parents** *PeriodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBindingCha*
, *MainMissionMethChan*

process $TakeOffMonitorApp \mathrel{\widehat=}$
$mainMission : MissionID,$
$takeOffMission : MissionID,$
$takeOffAltitude : \mathbb{P}\,\mathbb{A},$
$landingGearHandler : SchedulableID \bullet$ **begin**

State

$takeoffMission : TakeOffMission$

state *State*

Init

$State'$

$takeoffMission' =$

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

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

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

end

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

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

state *State*

$$takeOffAltitude : \mathbb{P}\,\mathbb{A}$$

state *State*

initial *Init*

$$State'$$

- **Skip**

end

5.5 CruiseMission

section *CruiseMissionApp* **parents** *scj_prelude*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *CruiseMissionMethChan*, *MethodCallBindingChannels*

process $CruiseMissionApp \mathrel{\widehat=}$
$controllingMission : MissionID \bullet$ **begin**

State

$this : \mathbf{ref}\ CruiseMissionClass$
$controllingMission : MainMission$

state *State*

Init

$State'$

$this' = \mathbf{new}\ CruiseMissionClass()$
$controllingMission' =$

$$InitializePhase \mathrel{\widehat=} \begin{pmatrix} initializeCall\,.\,CruiseMissionMID \longrightarrow \\ register\,!\,BeginLandingHandlerSID\,!\,CruiseMissionMID \longrightarrow \\ register\,!\,NavigationMonitorSID\,!\,CruiseMissionMID \longrightarrow \\ initializeRet\,.\,CruiseMissionMID \longrightarrow \\ \mathbf{Skip} \end{pmatrix}$$

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

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

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

end

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

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

state *State*

$controllingMission : MainMission$

state *State*

initial *Init*

$State'$

- **Skip**

end

5.6 Schedulables of CruiseMission

section *BeginLandingHandlerApp* **parents** *AperiodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBind*

process $BeginLandingHandlerApp \mathrel{\widehat=}$
$controllingMission : MissionID \bullet$ **begin**

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

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

$\bullet\ (Methods) \triangle (end\_aperiodic\_app\,.\,BeginLandingHandlerSID \longrightarrow \mathbf{Skip})$

end

section *NavigationMonitorApp* **parents** *PeriodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBinding*
, *MainMissionMethChan*

process *NavigationMonitorApp* $\widehat{=}$
mainMission : *MissionID* • **begin**

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

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

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

end

5.7 LandMission

section *LandMissionApp* **parents** *scj_prelude*, *MissionId*, *MissionIds*, *SchedulableId*, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *LandMissionMethChan*, *LandMissionClass*, *MethodCallBindingChannels*

process $LandMissionApp \mathrel{\widehat=}$
$controllingMission : MissionID \bullet$ **begin**

State

$this : \mathbf{ref}\ LandMissionClass$
$controllingMission : MainMission$

state *State*

Init

$State'$

$this' = \mathbf{new}\ LandMissionClass()$
$controllingMission' =$

$InitializePhase \mathrel{\widehat=}$
$\left(\begin{array}{l} initializeCall\,.\,LandMissionMID \longrightarrow \\ register\,!\,GroundDistanceMonitorSID\,!\,LandMissionMID \longrightarrow \\ register\,!\,LandingGearHandlerLandSID\,!\,LandMissionMID \longrightarrow \\ register\,!\,InstrumentLandingSystemMonitorSID\,!\,LandMissionMID \longrightarrow \\ register\,!\,SafeLandingHandlerSID\,!\,LandMissionMID \longrightarrow \\ initializeRet\,.\,LandMissionMID \longrightarrow \\ \mathbf{Skip} \end{array}\right)$

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

$deployLandingGearMeth \mathrel{\widehat=}$
$\left(\begin{array}{l} deployLandingGearCall\,.\,LandMissionMID\,?\,caller \longrightarrow \\ this\,.\,deployLandingGear(); \\ deployLandingGearRet\,.\,LandMissionMID\,.\,caller \longrightarrow \\ \mathbf{Skip} \end{array}\right)$

$stowLandingGearMeth \mathrel{\widehat=}$
$\left(\begin{array}{l} stowLandingGearCall\,.\,LandMissionMID\,?\,caller \longrightarrow \\ this\,.\,stowLandingGear(); \\ stowLandingGearRet\,.\,LandMissionMID\,.\,caller \longrightarrow \\ \mathbf{Skip} \end{array}\right)$

$isLandingGearDeployedMeth \mathrel{\widehat=} \mathbf{var}\ ret : \mathbb{B} \bullet$
$\left(\begin{array}{l} isLandingGearDeployedCall\,.\,LandMissionMID\,?\,caller \longrightarrow \\ ret := this\,.\,isLandingGearDeployed(); \\ isLandingGearDeployedRet\,.\,LandMissionMID\,.\,caller\,!\,ret \longrightarrow \\ \mathbf{Skip} \end{array}\right)$

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

• $(Init \; ; \; Methods) \triangle (end\_mission\_app \,.\, LandMissionMID \longrightarrow \mathbf{Skip})$

end

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

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

state *State*

$$SAFE\_LANDING\_ALTITUDE : \mathbb{P}\,\mathbb{A}$$
$$abort : \mathbb{B}$$
$$landingGearDeployed : \mathbb{B}$$

state *State*

initial *Init*

$$State'$$

$$SAFE\_LANDING\_ALTITUDE' = 10.0$$
$$abort' = false$$

public *deployLandingGear* $\widehat{=}$

public *stowLandingGear* $\widehat{=}$

public *isLandingGearDeployed* $\widehat{=}$ **var** $ret : \mathbb{B} \bullet$

• **Skip**

end

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

channel *stowLandingGearCall* : *MissionID*×
channel *stowLandingGearRet* : *MissionID*×

channel *isLandingGearDeployedCall* : *MissionID*×
channel *isLandingGearDeployedRet* : *MissionID* × ×$\mathbb{B}$

channel *cleanUpCall* : *MissionID*
channel *cleanUpRet* : *MissionID* × $\mathbb{B}$

channel *deployLandingGearCall* : *MissionID* × × *ThreadID*
channel *deployLandingGearRet* : *MissionID* × × *ThreadID*

5.8 Schedulables of LandMission

section *LandingGearHandlerLandApp* **parents** *AperiodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCall*
, *LandMissionMethChan*

process $LandingGearHandlerLandApp \mathrel{\widehat=}$
$mission : MissionID \bullet$ **begin**

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

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

$\bullet\ (Methods) \triangle (end\_aperiodic\_app\,.\,LandingGearHandlerLandSID \longrightarrow \mathbf{Skip})$

end

section *SafeLandingHandlerApp* **parents** *AperiodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBindi*
, *MainMissionMethChan*

process $SafeLandingHandlerApp \mathrel{\widehat=}$
$mainMission : MissionID,$
$threshold : \mathbb{P}\,\mathbb{A} \bullet$ **begin**

$handleAsyncEvent \mathrel{\widehat=}$
$\begin{pmatrix} handleAsyncEventCall\,.\,SafeLandingHandlerSID \longrightarrow \\ ; \\ handleAsyncEventRet\,.\,SafeLandingHandlerSID \longrightarrow \\ \mathbf{Skip} \end{pmatrix}$

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

$\bullet\ (Methods) \triangle (end\_aperiodic\_app\,.\,SafeLandingHandlerSID \longrightarrow \mathbf{Skip})$

end

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

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

state *State*

$threshold : \mathbb{P}\,\mathbb{A}$

state *State*

initial *Init*

$State'$

- **Skip**

end

section *GroundDistanceMonitorApp* **parents** *PeriodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *MethodCallBin*
, *MainMissionMethChan*

process *GroundDistanceMonitorApp* $\widehat{=}$
mainMission : *MissionID* • **begin**

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

$$
\begin{array}{l}
Methods \mathrel{\widehat{=}} \\
\big(handleAsyncEvent\big)\ ;\ Methods
\end{array}
$$

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

end

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

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

state *State*

$readingOnGround : \mathbb{P}\,\mathbb{A}$

state *State*

initial *Init*

$State'$

- **Skip**

end

section *InstrumentLandingSystemMonitorApp* **parents** *PeriodicEventHandlerChan*, *SchedulableId*, *SchedulableIds*, *Meth*

process $InstrumentLandingSystemMonitorApp \mathrel{\widehat=}$
$\quad mission : MissionID \bullet \textbf{begin}$

$$handleAsyncEvent \mathrel{\widehat=} \begin{pmatrix} handleAsyncEventCall \,.\, InstrumentLandingSystemMonitorSID \longrightarrow \\ ; \\ handleAsyncEventRet \,.\, InstrumentLandingSystemMonitorSID \longrightarrow \\ \textbf{Skip} \end{pmatrix}$$

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

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

end