aircraft

Tight Rope v0.6

November 1, 2015

1 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* . , *done_mission* . ,
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 *ObjectSync* ==
{| |}

channelset *ThreadSync* ==
{| |}

channelset *LockingSync* ==
{| *lockAcquired*, *startSyncMeth*, *endSyncMeth*, *waitCall*, *waitRet*, *notify* |}

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

section *Program* **parents** *scj_prelude*, *MissionId*, *MissionIds*,
SchedulableId, *SchedulableIds*, *MissionChan*, *SchedulableMethChan*, *MissionFW*,
SafeletFW, *TopLevelMissionSequencerFW*, *NetworkChannels*, *ManagedThreadFW*,
SchedulableMissionSequencerFW, *PeriodicEventHandlerFW*, *OneShotEventHandlerFW*,
AperiodicEventHandlerFW, *ACSafeletApp*, *MainMissionSequencerApp*,
ObjectFW, *ThreadFW*, *MainMissionApp*, *ACModeChangerApp*, *ControlHandlerApp*, *CommunicationsHandlerAp*

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

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

process $Tier1 \mathrel{\widehat=}$
$$\left(\begin{array}{l} MissionFW(TakeOffMission) \\ \quad [\![MissionSync]\!] \\ \left(\begin{array}{l} \left(\begin{array}{l} AperiodicEventHandlerFW() \\ \quad [\![SchedulablesSync]\!] \\ AperiodicEventHandlerFW() \end{array}\right) \\ \quad [\![SchedulablesSync]\!] \\ PeriodicEventHandlerFW() \end{array}\right) \end{array}\right)$$
$$[\![ClusterSync]\!]$$
$$\left(\begin{array}{l} MissionFW(CruiseMission) \\ \quad [\![MissionSync]\!] \\ \left(\begin{array}{l} AperiodicEventHandlerFW() \\ \quad [\![SchedulablesSync]\!] \\ PeriodicEventHandlerFW() \end{array}\right) \end{array}\right)$$
$$[\![ClusterSync]\!]$$
$$\left(\begin{array}{l} MissionFW(LandMission) \\ \quad [\![MissionSync]\!] \\ \left(\begin{array}{l} \left(\begin{array}{l} AperiodicEventHandlerFW() \\ \quad [\![SchedulablesSync]\!] \\ AperiodicEventHandlerFW() \end{array}\right) \\ \quad [\![SchedulablesSync]\!] \\ \left(\begin{array}{l} PeriodicEventHandlerFW() \\ \quad [\![SchedulablesSync]\!] \\ PeriodicEventHandlerFW() \end{array}\right) \end{array}\right) \end{array}\right)$$

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 $Application \mathrel{\widehat{=}}$

$ACSafeletApp$

$|||$

$MainMissionSequencerApp$

$|||$

$MainMissionApp(hijac.tools.tightrope.environments.VariableEnv \bullet 71c27ee8, hijac.tools.tightrope.environments.Variab$

$|||$

$ACModeChangerApp(MainMission)$

$|||$

$ControlHandlerApp$

$|||$

$CommunicationsHandlerApp$

$|||$

$EnvironmentMonitorApp(MainMission)$

$|||$

$FlightSensorsMonitorApp(MainMission)$

$|||$

$AperiodicSimulatorApp(AperiodicEventHandler)$

$|||$

$TakeOffMissionApp(hijac.tools.tightrope.environments.VariableEnv \bullet 6e950bcf, hijac.tools.tightrope.environments.Var$

$|||$

$LandingGearHandlerTakeOffApp(TakeOffMission)$

$|||$

$TakeOffFailureHandlerApp(TakeOffMission)$

$|||$

$TakeOffMonitorApp(TakeOffMission, AperiodicEventHandler)$

$|||$

$CruiseMissionApp(hijac.tools.tightrope.environments.VariableEnv \bullet 46dffdc3, hijac.tools.tightrope.environments.Varia$

$|||$

$BeginLandingHandlerApp(Mission)$

$|||$

$NavigationMonitorApp(CruiseMission)$

$|||$

$LandMissionApp(hijac.tools.tightrope.environments.VariableEnv \bullet 53dbe163, hijac.tools.tightrope.environments.Variab$

$|||$

$LandingGearHandlerLandApp(LandMission)$

$|||$

$SafeLandingHandlerApp(LandMission)$

$|||$

$GroundDistanceMonitorApp(LandMission)$

$|||$

$InstrumentLandingSystemMonitorApp(LandMission)$

$$
\begin{array}{l}
Locking \mathrel{\widehat{=}} \\
\left(\begin{array}{l}
\left(\begin{array}{l}
ThreadFW(LandingGearHandlerLandThread, MinPriority) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(SafeLandingHandlerThread, MinPriority) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(GroundDistanceMonitorThread, MinPriority) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(InstrumentLandingSystemMonitorThread, MinPriority)
\end{array}\right) \\
|||
\left(\begin{array}{l}
ObjectFW(ACSafeletObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(MainMissionObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(TakeOffMissionObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(CruiseMissionObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(LandMissionObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(ACModeChangerObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(EnvironmentMonitorObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(ControlHandlerObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(FlightSensorsMonitorObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(CommunicationsHandlerObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(AperiodicSimulatorObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(LandingGearHandlerTakeOffObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(TakeOffMonitorObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(TakeOffFailureHandlerObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(BeginLandingHandlerObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(NavigationMonitorObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(GroundDistanceMonitorObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(LandingGearHandlerLandObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(InstrumentLandingSystemMonitorObject) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(SafeLandingHandlerObject)
\end{array}\right)
\end{array}\right)
\end{array}
$$

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

2 ID Files

2.1 MissionIds

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

$$
\begin{array}{|l}
MainMission : MissionID \\
TakeOffMission : MissionID \\
CruiseMission : MissionID \\
LandMission : MissionID \\
\hline
distinct\langle nullMissionId, MainMission, \\
TakeOffMission, \\
CruiseMission, \\
LandMission\rangle
\end{array}
$$

2.2 SchedulablesIds

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

$$
\begin{array}{|l}
MainMissionSequencer : SchedulableID \\
ACModeChanger : SchedulableID \\
EnvironmentMonitor : SchedulableID \\
ControlHandler : SchedulableID \\
FlightSensorsMonitor : SchedulableID \\
CommunicationsHandler : SchedulableID \\
AperiodicSimulator : SchedulableID \\
LandingGearHandlerTakeOff : SchedulableID \\
TakeOffMonitor : SchedulableID \\
TakeOffFailureHandler : SchedulableID \\
BeginLandingHandler : SchedulableID \\
NavigationMonitor : SchedulableID \\
GroundDistanceMonitor : SchedulableID \\
LandingGearHandlerLand : SchedulableID \\
InstrumentLandingSystemMonitor : SchedulableID \\
SafeLandingHandler : SchedulableID \\
\hline
distinct\langle nullSequencerId, nullSchedulableId, ACModeChanger, \\
EnvironmentMonitor, \\
ControlHandler, \\
FlightSensorsMonitor, \\
CommunicationsHandler, \\
AperiodicSimulator, \\
LandingGearHandlerTakeOff, \\
TakeOffMonitor, \\
TakeOffFailureHandler, \\
BeginLandingHandler, \\
NavigationMonitor, \\
GroundDistanceMonitor, \\
LandingGearHandlerLand, \\
InstrumentLandingSystemMonitor, \\
SafeLandingHandler\rangle
\end{array}
$$

2.3 ThreadIds

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

$ACModeChangerThread : ThreadID$
$EnvironmentMonitorThread : ThreadID$
$ControlHandlerThread : ThreadID$
$FlightSensorsMonitorThread : ThreadID$
$CommunicationsHandlerThread : ThreadID$
$AperiodicSimulatorThread : ThreadID$
$LandingGearHandlerTakeOffThread : ThreadID$
$TakeOffMonitorThread : ThreadID$
$TakeOffFailureHandlerThread : ThreadID$
$BeginLandingHandlerThread : ThreadID$
$NavigationMonitorThread : ThreadID$
$GroundDistanceMonitorThread : ThreadID$
$LandingGearHandlerLandThread : ThreadID$
$InstrumentLandingSystemMonitorThread : ThreadID$
$SafeLandingHandlerThread : ThreadID$

$distinct\langle SafeletThreadId, nullThreadId,$
$ACModeChangerThread,$
$EnvironmentMonitorThread,$
$ControlHandlerThread,$
$FlightSensorsMonitorThread,$
$CommunicationsHandlerThread,$
$AperiodicSimulatorThread,$
$LandingGearHandlerTakeOffThread,$
$TakeOffMonitorThread,$
$TakeOffFailureHandlerThread,$
$BeginLandingHandlerThread,$
$NavigationMonitorThread,$
$GroundDistanceMonitorThread,$
$LandingGearHandlerLandThread,$
$InstrumentLandingSystemMonitorThread,$
$SafeLandingHandlerThread\rangle$

2.4 ObjectIds

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

$ACSafeletObject : ObjectID$
$MainMissionObject : ObjectID$
$TakeOffMissionObject : ObjectID$
$CruiseMissionObject : ObjectID$
$LandMissionObject : ObjectID$
$ACModeChangerObject : ObjectID$
$EnvironmentMonitorObject : ObjectID$
$ControlHandlerObject : ObjectID$
$FlightSensorsMonitorObject : ObjectID$
$CommunicationsHandlerObject : ObjectID$
$AperiodicSimulatorObject : ObjectID$
$LandingGearHandlerTakeOffObject : ObjectID$
$TakeOffMonitorObject : ObjectID$
$TakeOffFailureHandlerObject : ObjectID$
$BeginLandingHandlerObject : ObjectID$
$NavigationMonitorObject : ObjectID$
$GroundDistanceMonitorObject : ObjectID$
$LandingGearHandlerLandObject : ObjectID$
$InstrumentLandingSystemMonitorObject : ObjectID$
$SafeLandingHandlerObject : ObjectID$

$distinct\langle ACSafeletObject,$
$MainMissionObject,$
$TakeOffMissionObject,$
$CruiseMissionObject,$
$LandMissionObject,$
$ACModeChangerObject,$
$EnvironmentMonitorObject,$
$ControlHandlerObject,$
$FlightSensorsMonitorObject,$
$CommunicationsHandlerObject,$
$AperiodicSimulatorObject,$
$LandingGearHandlerTakeOffObject,$
$TakeOffMonitorObject,$
$TakeOffFailureHandlerObject,$
$BeginLandingHandlerObject,$
$NavigationMonitorObject,$
$GroundDistanceMonitorObject,$
$LandingGearHandlerLandObject,$
$InstrumentLandingSystemMonitorObject,$
$SafeLandingHandlerObject\rangle$

3 Safelet

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

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

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

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

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

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

end

4 Top Level Mission Sequencer

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

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

State

$this : \textbf{ref}\ MainMissionSequencerClass$

state *State*

Init

$State'$

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

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

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

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

end

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

state *State*

$$returnedMission : \mathbb{B}$$

state *State*

initial *Init*

$$State'$$

$$returnedMission' = false$$

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

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

• **Skip**

end

5 Missions

5.1 MainMission

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

process $MainMissionApp \mathrel{\widehat=} storageParameters : MissionID, storageParametersSchedulable : MissionID, aCModeChange$

State

$this : \mathbf{ref}\ MainMissionClass$

state *State*

Init

$State'$

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

$$InitializePhase \mathrel{\widehat=} \left(\begin{array}{l} initializeCall\,.\,MainMission \longrightarrow \\ register\,!\,ACModeChanger\,!\,MainMission \longrightarrow \\ register\,!\,EnvironmentMonitor\,!\,MainMission \longrightarrow \\ register\,!\,ControlHandler\,!\,MainMission \longrightarrow \\ register\,!\,FlightSensorsMonitor\,!\,MainMission \longrightarrow \\ register\,!\,CommunicationsHandler\,!\,MainMission \longrightarrow \\ register\,!\,AperiodicSimulator\,!\,MainMission \longrightarrow \\ initializeRet\,.\,MainMission \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

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

$$getAirSpeedMeth \mathrel{\widehat=} \mathbf{var}\ ret : double \bullet \left(\begin{array}{l} getAirSpeedCall\,.\,MainMission \longrightarrow \\ ret := this\,.\,getAirSpeed(); \\ getAirSpeedRet\,.\,MainMission\,!\,ret \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

$$getAltitudeMeth \mathrel{\widehat=} \mathbf{var}\ ret : double \bullet \left(\begin{array}{l} getAltitudeCall\,.\,MainMission \longrightarrow \\ ret := this\,.\,getAltitude(); \\ getAltitudeRet\,.\,MainMission\,!\,ret \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

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

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

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

$$getHeadingMeth \mathrel{\widehat=} \textbf{var}\ ret : double \bullet \left(\begin{array}{l} getHeadingCall\,.\,MainMission \longrightarrow \\ ret := this\,.\,getHeading(); \\ getHeadingRet\,.\,MainMission\,!\,ret \longrightarrow \\ \textbf{Skip} \end{array}\right)$$

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

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

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

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

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

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

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

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

end

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

state *State*

$ALTITUDE\_READING\_ON\_GROUND : double$
$cabinPressure : double$
$emergencyOxygen : double$
$fuelRemaining : double$
$altitude : double$
$airSpeed : double$
$heading : double$

state *State*

initial *Init*

$State'$

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

public $getAirSpeed \mathrel{\widehat{=}} \textbf{var}\ ret : double \bullet$
$(ret := airSpeed)$

public $getAltitude \mathrel{\widehat{=}} \textbf{var}\ ret : double \bullet$
$(ret := altitude)$

public $getCabinPressure \mathrel{\widehat{=}} \textbf{var}\ ret : double \bullet$
$(ret := cabinPressure)$

public $getEmergencyOxygen \mathrel{\widehat{=}} \textbf{var}\ ret : double \bullet$
$(ret := emergencyOxygen)$

public $getFuelRemaining \mathrel{\widehat{=}} \textbf{var}\ ret : double \bullet$
$(ret := fuelRemaining)$

public $getHeading \mathrel{\widehat{=}} \textbf{var}\ ret : double \bullet$
$(ret := heading)$

public $setAirSpeed \mathrel{\widehat{=}}$
$(this\,.\,this.airSpeed := airSpeed)$

public $setAltitude \mathrel{\widehat{=}}$
$(this\,.\,this.altitude := altitude)$

public $setCabinPressure \mathrel{\widehat{=}}$
$(this\,.\,this.cabinPressure := cabinPressure)$

public $setEmergencyOxygen \mathrel{\widehat{=}}$
$(this\,.\,this.emergencyOxygen := emergencyOxygen)$

public $setFuelRemaining \mathrel{\widehat{=}}$
$\big(this\,.\,this.fuelRemaining := fuelRemaining\big)$

public $setHeading \mathrel{\widehat{=}}$
$\big(this\,.\,this.heading := heading\big)$

- **Skip**

end

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

channel *getAirSpeedCall* : *MissionID*
channel *getAirSpeedRet* : *MissionID* × *double*

channel *getAltitudeCall* : *MissionID*
channel *getAltitudeRet* : *MissionID* × *double*

channel *getCabinPressureCall* : *MissionID*
channel *getCabinPressureRet* : *MissionID* × *double*

channel *getEmergencyOxygenCall* : *MissionID*
channel *getEmergencyOxygenRet* : *MissionID* × *double*

channel *getFuelRemainingCall* : *MissionID*
channel *getFuelRemainingRet* : *MissionID* × *double*

channel *getHeadingCall* : *MissionID*
channel *getHeadingRet* : *MissionID* × *double*

channel *setAirSpeedCall* : *MissionID* × *double*
channel *setAirSpeedRet* : *MissionID*

channel *setAltitudeCall* : *MissionID* × *double*
channel *setAltitudeRet* : *MissionID*

channel *setCabinPressureCall* : *MissionID* × *double*
channel *setCabinPressureRet* : *MissionID*

channel *setEmergencyOxygenCall* : *MissionID* × *double*
channel *setEmergencyOxygenRet* : *MissionID*

channel *setFuelRemainingCall* : *MissionID* × *double*
channel *setFuelRemainingRet* : *MissionID*

channel *setHeadingCall* : *MissionID* × *double*
channel *setHeadingRet* : *MissionID*

5.2 Schedulables of

section *ACModeChangerApp* **parents** *TopLevelMissionSequencerChan*, *MissionId*, *MissionIds*, *SchedulableId*

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

State

$modesLeft : \mathbb{Z}$
ref $currentModeClass : ModeClass$
ref $launchModeClass : ModeClass$
ref $cruiseModeClass : ModeClass$
ref $landModeClass : ModeClass$

state *State*

Init

$State'$

$modesLeft' = 3$
ref $currentModeClass' =$ **new** $ModeClass()$
ref $launchModeClass' =$ **new** $ModeClass()$
ref $cruiseModeClass' =$ **new** $ModeClass()$
ref $landModeClass' =$ **new** $ModeClass()$

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

$changeToMeth \mathrel{\widehat=}$
$\begin{pmatrix} changeToCall\,.\,ACModeChanger\,?\,newMode \longrightarrow \\ (this\,.\,currentMode := newMode)\,; \\ changeToRet\,.\,ACModeChanger \longrightarrow \\ \textbf{Skip} \end{pmatrix}$

$$
\begin{array}{l}
getNextMissionMeth \mathrel{\widehat=} \textbf{var}\ ret : MissionID \bullet \\
\left(\begin{array}{l}
getNextMissionCall\,.\,ACModeChanger \longrightarrow \\
\left(\begin{array}{l}
\textbf{if}\ (modesLeft = 3) \longrightarrow \\
\quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ ret := TakeOffMission \end{array}\right) \\
[]\ \neg\ (modesLeft = 3) \longrightarrow \\
\quad \textbf{if}\ (modesLeft = 2) \longrightarrow \\
\quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ ret := CruiseMission \end{array}\right) \\
[]\ \neg\ (modesLeft = 2) \longrightarrow \\
\quad \textbf{if}\ (modesLeft = 1) \longrightarrow \\
\quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ ret := LandMission \end{array}\right) \\
[]\ \neg\ (modesLeft = 1) \longrightarrow \\
\quad \big(ret := nullMissionId\big) \\
\textbf{fi} \\
\textbf{fi} \\
\textbf{fi}
\end{array}\right) \\
getNextMissionRet\,.\,ACModeChanger\,!\,ret \longrightarrow \\
\textbf{Skip}
\end{array}\right)
\end{array}
$$

$$
\begin{array}{l}
advanceModeSyncMeth \mathrel{\widehat=} \\
\left(\begin{array}{l}
advanceModeCall\,.\,ACModeChanger\,?\,thread \longrightarrow \\
\left(\begin{array}{l}
startSyncMeth\,.\,ACModeChangerObject\,.\,thread \longrightarrow \\
lockAcquired\,.\,ACModeChangerObject\,.\,thread \longrightarrow \\
\left(\begin{array}{l}
; \\
\textbf{if}\ (modesLeft = 3) \longrightarrow \\
\quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ changeTo(launchMode) \end{array}\right) \\
[]\ \neg\ (modesLeft = 3) \longrightarrow \\
\quad \textbf{if}\ (modesLeft = 2) \longrightarrow \\
\quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ changeTo(cruiseMode) \end{array}\right) \\
[]\ \neg\ (modesLeft = 2) \longrightarrow \\
\quad \textbf{if}\ (modesLeft = 1) \longrightarrow \\
\quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ changeTo(landMode) \end{array}\right) \\
[]\ \neg\ (modesLeft = 1) \longrightarrow \\
\quad \big(changeTo(\textbf{null})\big) \\
\textbf{fi} \\
\textbf{fi} \\
\textbf{fi}
\end{array}\right) \\
endSyncMeth\,.\,ACModeChangerObject\,.\,thread \longrightarrow \\
advanceModeRet\,.\,ACModeChanger\,.\,thread \longrightarrow \\
\textbf{Skip}
\end{array}\right)
\end{array}\right)
\end{array}
$$

$$
\begin{array}{l}
Methods \mathrel{\widehat=} \\
\left(\begin{array}{l}
GetNextMission \\
\Box \\
changeToMeth \\
\Box \\
getNextMissionMeth \\
\Box \\
advanceModeSyncMeth
\end{array}\right) ;\ Methods
\end{array}
$$

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

end

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

$$
\begin{array}{l}
\circ\ \textbf{sync}\ advanceMode\ \mathrel{\widehat{=}} \\
\left(\begin{array}{l}
; \\
\textbf{if}\ (modesLeft = 3) \longrightarrow \\
\quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ changeTo(launchMode) \end{array}\right) \\
[]\ \neg\ (modesLeft = 3) \longrightarrow \\
\quad \textbf{if}\ (modesLeft = 2) \longrightarrow \\
\quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ changeTo(cruiseMode) \end{array}\right) \\
[]\ \neg\ (modesLeft = 2) \longrightarrow \\
\quad \textbf{if}\ (modesLeft = 1) \longrightarrow \\
\quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ changeTo(landMode) \end{array}\right) \\
[]\ \neg\ (modesLeft = 1) \longrightarrow \\
\quad \big(changeTo(\textbf{null})\big) \\
\textbf{fi} \\
\textbf{fi} \\
\textbf{fi}
\end{array}\right)
\end{array}
$$

- **Skip**

end

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

channel *changeToCall* : *SchedulableID*×
channel *changeToRet* : *SchedulableID*

channel *getNextMissionCall* : *SchedulableID*
channel *getNextMissionRet* : *SchedulableID* × *MissionID*

channel *advanceModeCall* : *SchedulableID* × *ThreadID*
channel *advanceModeRet* : *SchedulableID* × *ThreadID*

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

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

$$
\begin{array}{l}
handlerAsyncEvent \mathrel{\widehat{=}} \\
\left(\begin{array}{l}
handleAsyncEventCall\,.\,ControlHandler \longrightarrow \\
\Big(\!\!\Big(handleAsyncEventRet\,.\,ControlHandler \longrightarrow \\
\mathbf{Skip}
\end{array}\right)
\end{array}
$$

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

$$\triangle(end\_aperiodic\_app\,.\,ControlHandler \longrightarrow \mathbf{Skip})$$

end

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

- **Skip**

end

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

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

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

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

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

$$\triangle(end\_aperiodic\_app\,.\,CommunicationsHandler \longrightarrow \textbf{Skip})$$

end

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

- **Skip**

end

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

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

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

$$handlerAsyncEvent \mathrel{\widehat=}$$
$$\left(\begin{array}{l} handleAsyncEventCall\,.\,EnvironmentMonitor \longrightarrow \\ \left(\begin{array}{l} ; \\ setCabinPressureCall\,.\,controllingMission0 \longrightarrow \\ setCabinPressureRet\,.\,controllingMission \longrightarrow \\ \textbf{Skip}; \\ setEmergencyOxygenCall\,.\,controllingMission0 \longrightarrow \\ setEmergencyOxygenRet\,.\,controllingMission \longrightarrow \\ \textbf{Skip}; \\ setFuelRemainingCall\,.\,controllingMission0 \longrightarrow \\ setFuelRemainingRet\,.\,controllingMission \longrightarrow \\ \textbf{Skip} \end{array}\right) \\ \textbf{Skip} \end{array}\right) \; handleAsyncEventRet\,.\,EnvironmentMonitor \longrightarrow$$

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

$$\triangle(end\_periodic\_app\,.\,EnvironmentMonitor \longrightarrow \textbf{Skip})$$

end

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

- **Skip**

end

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

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

$$handlerAsyncEvent \mathrel{\widehat=}$$
$$\left(\begin{array}{l} handleAsyncEventCall\,.\,FlightSensorsMonitor \longrightarrow \\ \left(\begin{array}{l} ; \\ setAirSpeedCall\,.\,controllingMission0 \longrightarrow \\ setAirSpeedRet\,.\,controllingMission \longrightarrow \\ \textbf{Skip}; \\ setAltitudeCall\,.\,controllingMission0 \longrightarrow \\ setAltitudeRet\,.\,controllingMission \longrightarrow \\ \textbf{Skip}; \\ setHeadingCall\,.\,controllingMission0 \longrightarrow \\ setHeadingRet\,.\,controllingMission \longrightarrow \\ \textbf{Skip} \end{array}\right) \\ \textbf{Skip} \end{array}\right) \; handleAsyncEventRet\,.\,FlightSensorsMonitor \longrightarrow \Bigg)$$

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

$$\triangle(end\_periodic\_app\,.\,FlightSensorsMonitor \longrightarrow \textbf{Skip})$$

end

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

- **Skip**

end

section $AperiodicSimulatorApp$ **parents** $PeriodicEventHandlerChan, SchedulableId, SchedulableIds$

process $AperiodicSimulatorApp \mathrel{\widehat=} event : MissionID \bullet$ **begin**

$$handlerAsyncEvent \mathrel{\widehat=}$$
$$\left(\begin{array}{l} handleAsyncEventCall\,.\,AperiodicSimulator \longrightarrow \\ \left(\begin{array}{l} ; \\ releaseCall\,.\,event \longrightarrow \\ releaseRet\,.\,event\,?\,release \longrightarrow \\ \textbf{Skip} \end{array}\right) \\ \textbf{Skip} \end{array}\right) handleAsyncEventRet\,.\,AperiodicSimulator \longrightarrow \Bigg)$$

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

$$\triangle(end\_periodic\_app\,.\,AperiodicSimulator \longrightarrow \textbf{Skip})$$

end

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

- **Skip**

end

5.3 TakeOffMission

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

process $TakeOffMissionApp \mathrel{\widehat=} storageParametersSchedulable : MissionID, landingGearHandler : MissionID, takeOffMon$

State

$this : \mathbf{ref}\ TakeOffMissionClass$

state *State*

Init

$State'$

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

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

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

$$abortMeth \mathrel{\widehat=} \left(\begin{array}{l} abortCall\,.\,TakeOffMission \longrightarrow \\ this\,.\,abort(); \\ abortRet\,.\,TakeOffMission \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

$$getControllingMissionMeth \mathrel{\widehat=} \mathbf{var}\ ret : MissionID \bullet \left(\begin{array}{l} getControllingMissionCall\,.\,TakeOffMission \longrightarrow \\ ret := this\,.\,getControllingMission(); \\ getControllingMissionRet\,.\,TakeOffMission\,!\,ret \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

$$setControllingMissionMeth \mathrel{\widehat=} \left(\begin{array}{l} setControllingMissionCall\,.\,TakeOffMission\,?\,controllingMission \longrightarrow \\ this\,.\,setControllingMission(controllingMission); \\ setControllingMissionRet\,.\,TakeOffMission \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

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

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

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

$$
\begin{array}{l}
deployLandingGearSyncMeth \mathrel{\widehat=} \\
\left(\begin{array}{l}
deployLandingGearCall\,.\,TakeOffMission\,?\,thread \longrightarrow \\
\left(\begin{array}{l}
startSyncMeth\,.\,TakeOffMissionObject\,.\,thread \longrightarrow \\
lockAcquired\,.\,TakeOffMissionObject\,.\,thread \longrightarrow \\
\left(this\,.\,landingGearDeployed := true\right);\\
endSyncMeth\,.\,TakeOffMissionObject\,.\,thread \longrightarrow \\
deployLandingGearRet\,.\,TakeOffMission\,.\,thread \longrightarrow \\
\textbf{Skip}
\end{array}\right)
\end{array}\right)
\end{array}
$$

$$
Methods \mathrel{\widehat=} \left(\begin{array}{l}
InitializePhase \\
\Box \\
CleanupPhase \\
\Box \\
abortMeth \\
\Box \\
getControllingMissionMeth \\
\Box \\
setControllingMissionMeth \\
\Box \\
cleanUpMeth \\
\Box \\
stowLandingGearMeth \\
\Box \\
isLandingGearDeployedMeth \\
\Box \\
deployLandingGearSyncMeth
\end{array}\right) ;\ Methods
$$

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

end

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

state *State*

$SAFE\_AIRSPEED\_THRESHOLD : double$
$TAKEOFF\_ALTITUDE : double$
$abort : \mathbb{B}$
$landingGearDeployed : \mathbb{B}$

state *State*

initial *Init*

$State'$

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

public $abort \mathrel{\widehat{=}}$
$\big(this\,.\,abort := true\big)$

public $getControllingMission \mathrel{\widehat{=}}$ **var** $ret : MissionID \bullet$
$\big(ret := controllingMission\big)$

public $setControllingMission \mathrel{\widehat{=}}$
$\big(this\,.\,this.controllingMission := controllingMission\big)$

public $cleanUp \mathrel{\widehat{=}}$ **var** $ret : \mathbb{B} \bullet$
$\begin{pmatrix} ; \\ ret := (\neg\ abort = \mathbf{True}) \end{pmatrix}$

public $stowLandingGear \mathrel{\widehat{=}}$
$\big(this\,.\,landingGearDeployed := false\big)$

public $isLandingGearDeployed \mathrel{\widehat{=}}$ **var** $ret : \mathbb{B} \bullet$
$\big(ret := landingGearDeployed = \mathbf{True}\big)$

• **Skip**

end

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

channel $abortCall : MissionID$
channel $abortRet : MissionID$

channel $getControllingMissionCall : MissionID$
channel $getControllingMissionRet : MissionID \times MissionID$

channel $setControllingMissionCall : MissionID \times MissionID$
channel $setControllingMissionRet : MissionID$

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

channel $stowLandingGearCall : MissionID$
channel $stowLandingGearRet : MissionID$

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

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

5.4 Schedulables of

section *LandingGearHandlerTakeOffApp* **parents** *AperiodicEventHandlerChan*, *SchedulableId*, *SchedulableIds* , *TakeOffMissionMethChan*, *ObjectIds*, *ThreadIds*

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

$handlerAsyncEvent \mathrel{\widehat=}$
$\Big($ *handleAsyncEventCall . LandingGearHandlerTakeOff* $\longrightarrow$
$\Big($;
isLandingGearDeployedCall . mission $\longrightarrow$
isLandingGearDeployedRet . mission ? *isLandingGearDeployed* $\longrightarrow$

var *landingGearIsDeployed* : $\mathbb{B} \bullet$ *landingGearIsDeployed* := *isLandingGearDeployed*
if *landingGearIsDeployed* = **True** $\longrightarrow$
$\quad\Big($ *stowLandingGearCall . mission* $\longrightarrow$
$\quad$ *stowLandingGearRet . mission* $\longrightarrow$
$\quad$ **Skip** $\Big)$
$[]\ \neg$ *landingGearIsDeployed* = **True** $\longrightarrow$
$\quad\Big($ *deployLandingGearCall . mission . LandingGearHandlerTakeOffThread* $\longrightarrow$
$\quad$ *deployLandingGearRet . mission . LandingGearHandlerTakeOffThread* $\longrightarrow$
$\quad$ **Skip** $\Big)$
fi
$\Big)$ *handleAsyncEventRet . Landi*
Skip
$\Big)$

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

$\triangle($ *end_aperiodic_app . LandingGearHandlerTakeOff* $\longrightarrow$ **Skip**$)$

end

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

- **Skip**

end

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

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

process $TakeOffFailureHandlerApp \mathrel{\widehat=} takeoffMission : MissionID \bullet$ **begin**

State

$threshold : double$

state *State*

Init

$State'$

$threshold' = threshold$

$handlerAsyncEvent \mathrel{\widehat=}$
$(handleAsyncEventCall\,.\,TakeOffFailureHandler \longrightarrow$
$(getControllingMissionCall\,.\,takeoffMission.getControllingMission() \longrightarrow$
$getControllingMissionRet\,.\,takeoffMission.getControllingMission()\,?\,getControllingMission \longrightarrow$

var $currentSpeed : double \bullet currentSpeed := getAirSpeed$
if $(currentSpeed < threshold) \longrightarrow$
$(;$
$abortCall\,.\,takeoffMission \longrightarrow$
$abortRet\,.\,takeoffMission \longrightarrow$
Skip;
$requestTerminationCall\,.\,takeoffMission \longrightarrow$
$requestTerminationRet\,.\,takeoffMission\,?\,requestTermination \longrightarrow$
Skip
$)$
$[]\,\neg\,(currentSpeed < threshold) \longrightarrow$
$)($
fi Skip
$)$ $handleAsyncEventR$
Skip

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

$\triangle(end\_aperiodic\_app\,.\,TakeOffFailureHandler \longrightarrow$ **Skip**$)$

end

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

- **Skip**

end

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

section *TakeOffMonitorApp* **parents** *PeriodicEventHandlerChan*, *SchedulableId*, *SchedulableIds* , *TakeOffMissionMethChan*

process $TakeOffMonitorApp \mathrel{\widehat=} takeoffMission : MissionID, landingGearHandler : MissionID \bullet$ **begin**

State

$takeOffAltitude : double$

state *State*

Init

$State'$

$takeOffAltitude' = takeOffAltitude$

$handlerAsyncEvent \mathrel{\widehat=}$
$\Big($ $handleAsyncEventCall \,.\, TakeOffMonitor \longrightarrow$
$\Big($;
$getControllingMissionCall \,.\, takeoffMission.getControllingMission() \longrightarrow$
$getControllingMissionRet \,.\, takeoffMission.getControllingMission() \,?\, getControllingMission \longrightarrow$
var $altitude : double \bullet altitude := getAltitude$
if $(altitude > takeOffAltitude) \longrightarrow$
$\Big($;
$releaseCall \,.\, landingGearHandler \longrightarrow$
$releaseRet \,.\, landingGearHandler \,?\, release \longrightarrow$
$requestTerminationCall \,.\, takeoffMission \longrightarrow$
$requestTerminationRet \,.\, takeoffMission \,?\, requestTermination \longrightarrow$
Skip $\Big)$
$[] \neg (altitude > takeOffAltitude) \longrightarrow$ **Skip**
fi ;
Skip $\Big)$ $handleAsyncEventR$
Skip

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

$\triangle(end\_periodic\_app \,.\, TakeOffMonitor \longrightarrow$ **Skip**$)$

end

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

- **Skip**

end

5.5 CruiseMission

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

process $CruiseMissionApp \mathrel{\widehat=} storageParametersSchedulable : MissionID, beginLandingHandler : MissionID, navigationM$

State

$this : \mathbf{ref}\ CruiseMissionClass$

state *State*

Init

$State'$

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

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

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

$$getControllingMissionMeth \mathrel{\widehat=} \mathbf{var}\ ret : MissionID \bullet \left(\begin{array}{l} getControllingMissionCall\ .\ CruiseMission \longrightarrow \\ ret := this\ .\ getControllingMission(); \\ getControllingMissionRet\ .\ CruiseMission\ !\ ret \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

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

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

end

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

public *getControllingMission* $\widehat{=}$ **var** *ret* : *MissionID* $\bullet$
$\big($*ret* := *controllingMission*$\big)$

$\bullet$ **Skip**

end

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

channel $getControllingMissionCall : MissionID$
channel $getControllingMissionRet : MissionID \times MissionID$

5.6 Schedulables of

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

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

$$handlerAsyncEvent \mathrel{\widehat=}$$
$$\left(\begin{array}{l} handleAsyncEventCall\,.\,BeginLandingHandler \longrightarrow \\ \left(\begin{array}{l} ; \\ requestTerminationCall\,.\,controllingMission \longrightarrow \\ requestTerminationRet\,.\,controllingMission\,?\,requestTermination \longrightarrow \\ \textbf{Skip} \end{array}\right) \\ \textbf{Skip} \end{array}\right) handleAsyncEventRet\,.\,BeginLandingHandler$$

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

$$\triangle(end\_aperiodic\_app\,.\,BeginLandingHandler \longrightarrow \textbf{Skip})$$

end

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

- **Skip**

end

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

section *NavigationMonitorApp* **parents** *PeriodicEventHandlerChan*, *SchedulableId*, *SchedulableIds* , *CruiseMissionMethChan*

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

$handlerAsyncEvent \mathrel{\widehat=}$
$\Big($ *handleAsyncEventCall . NavigationMonitor* $\longrightarrow$
$\Big($ *getControllingMissionCall . mission.getControllingMission*$()\longrightarrow$
getControllingMissionRet . mission.getControllingMission$()$? *getControllingMission* $\longrightarrow$
var *heading* : *double* $\bullet$ *heading* := *getHeading*
getControllingMissionCall . mission.getControllingMission$()\longrightarrow$
getControllingMissionRet . mission.getControllingMission$()$? *getControllingMission* $\longrightarrow$
var *airSpeed* : *double* $\bullet$ *airSpeed* := *getAirSpeed*
getControllingMissionCall . mission.getControllingMission$()\longrightarrow$
getControllingMissionRet . mission.getControllingMission$()$? *getControllingMission* $\longrightarrow$
var *altitude* : *double* $\bullet$ *altitude* := *getAltitude*
Skip
$\Big)$ *handleAsyncEventRet . Nav*
Skip
$\Big)$

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

$\triangle($*end_periodic_app . NavigationMonitor* $\longrightarrow$ **Skip**$)$

end

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

- **Skip**

end

5.7 LandMission

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

process $LandMissionApp \mathrel{\widehat=} storageParametersSchedulable : MissionID, groundDistanceMonitor : MissionID, landingHar$

State

$this : \mathbf{ref}\ LandMissionClass$

state *State*

Init

$State'$

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

$$InitializePhase \mathrel{\widehat=} \left(\begin{array}{l} initializeCall\,.\,LandMission \longrightarrow \\ register\,!\,GroundDistanceMonitor\,!\,LandMission \longrightarrow \\ register\,!\,LandingGearHandlerLand\,!\,LandMission \longrightarrow \\ register\,!\,InstrumentLandingSystemMonitor\,!\,LandMission \longrightarrow \\ register\,!\,SafeLandingHandler\,!\,LandMission \longrightarrow \\ initializeRet\,.\,LandMission \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

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

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

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

$$getControllingMissionMeth \mathrel{\widehat=} \mathbf{var}\ ret : MissionID \bullet \left(\begin{array}{l} getControllingMissionCall\,.\,LandMission \longrightarrow \\ ret := this\,.\,getControllingMission(); \\ getControllingMissionRet\,.\,LandMission\,!\,ret \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

$$abortMeth \mathrel{\widehat=} \left(\begin{array}{l} abortCall\,.\,LandMission \longrightarrow \\ this\,.\,abort(); \\ abortRet\,.\,LandMission \longrightarrow \\ \mathbf{Skip} \end{array}\right)$$

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

$$deployLandingGearSyncMeth \mathrel{\widehat=} \left(\begin{array}{l} deployLandingGearCall\ .\ LandMission\,?\,thread \longrightarrow \\ \left(\begin{array}{l} startSyncMeth\ .\ LandMissionObject\ .\ thread \longrightarrow \\ lockAcquired\ .\ LandMissionObject\ .\ thread \longrightarrow \\ \big(this\ .\ landingGearDeployed := true\big)\ ; \\ endSyncMeth\ .\ LandMissionObject\ .\ thread \longrightarrow \\ deployLandingGearRet\ .\ LandMission\ .\ thread \longrightarrow \\ \mathbf{Skip} \end{array}\right) \end{array}\right)$$

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

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

end

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

state *State*

$SAFE\_LANDING\_ALTITUDE : double$
$abort : \mathbb{B}$
$landingGearDeployed : \mathbb{B}$

state *State*

initial *Init*

$State'$

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

public *stowLandingGear* $\widehat{=}$
$(this\,.\,landingGearDeployed := false)$

public *isLandingGearDeployed* $\widehat{=}$ **var** $ret : \mathbb{B} \bullet$
$(ret := landingGearDeployed = \mathbf{True})$

public *getControllingMission* $\widehat{=}$ **var** $ret : MissionID \bullet$
$(ret := controllingMission)$

public *abort* $\widehat{=}$
$(this\,.\,abort := true)$

public *cleanUp* $\widehat{=}$ **var** $ret : \mathbb{B} \bullet$
$\begin{pmatrix} ; \\ ret := (\neg\ abort = \mathbf{True}) \end{pmatrix}$

$\bullet$ **Skip**

end

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

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

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

channel *getControllingMissionCall* : *MissionID*
channel *getControllingMissionRet* : *MissionID* $\times$ *MissionID*

channel *abortCall* : *MissionID*
channel *abortRet* : *MissionID*

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

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

5.8 Schedulables of

section *LandingGearHandlerLandApp* **parents** *AperiodicEventHandlerChan*, *SchedulableId*, *SchedulableIds* , *LandMissionMethChan*, *ObjectIds*, *ThreadIds*

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

$handlerAsyncEvent \mathrel{\widehat=}$
$\Big($ *handleAsyncEventCall . LandingGearHandlerLand* $\longrightarrow$
$\Big($;
isLandingGearDeployedCall . mission $\longrightarrow$
isLandingGearDeployedRet . mission ? *isLandingGearDeployed* $\longrightarrow$

var *landingGearIsDeployed* : $\mathbb{B} \bullet$ *landingGearIsDeployed* := *isLandingGearDeployed*
if *landingGearIsDeployed* = **True** $\longrightarrow$
$\quad\Big($ *stowLandingGearCall . mission* $\longrightarrow$
$\quad$ *stowLandingGearRet . mission* $\longrightarrow$
$\quad$ **Skip** $\Big)$
$[]\ \neg$ *landingGearIsDeployed* = **True** $\longrightarrow$
$\quad\Big($ *deployLandingGearCall . mission . LandingGearHandlerLandThread* $\longrightarrow$
$\quad$ *deployLandingGearRet . mission . LandingGearHandlerLandThread* $\longrightarrow$
$\quad$ **Skip** $\Big)$
fi
$\Big)$; *handleAsyncEventRet . Landi*
Skip
$\Big)$

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

$\triangle($ *end_aperiodic_app . LandingGearHandlerLand* $\longrightarrow$ **Skip**$)$

end

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

- **Skip**

end

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

section *SafeLandingHandlerApp* **parents** *AperiodicEventHandlerChan*, *SchedulableId*, *SchedulableIds* , *LandMissionMethChan*

process $SafeLandingHandlerApp \mathrel{\widehat=} landMission : MissionID \bullet$ **begin**

State

$threshold : double$

state *State*

Init

$State'$

$threshold' = threshold$

$handlerAsyncEvent \mathrel{\widehat=}$
$\Big($ *handleAsyncEventCall* . *SafeLandingHandler* $\longrightarrow$
$\Big($ *getControllingMissionCall* . *landMission*.*getControllingMission*() $\longrightarrow$
getControllingMissionRet . *landMission*.*getControllingMission*() ? *getControllingMission* $\longrightarrow$

var *altitude* : *double* $\bullet$ *altitude* := *getAltitude*
if $(altitude < threshold) \longrightarrow$
$)($
$[] \neg (altitude < threshold) \longrightarrow$
$)($
fi
$\Big)$ *handleAsyncEventRet*
Skip

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

$\triangle(end\_aperiodic\_app$. *SafeLandingHandler* $\longrightarrow$ **Skip**$)$

end

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

- **Skip**

end

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

section *GroundDistanceMonitorApp* **parents** *PeriodicEventHandlerChan*, *SchedulableId*, *SchedulableIds* , *LandMissionMethChan*

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

State

$readingOnGround : double$

state *State*

Init

$State'$

$readingOnGround' =$

$handlerAsyncEvent \mathrel{\widehat=}$
$\Big($ $handleAsyncEventCall \,.\, GroundDistanceMonitor \longrightarrow$
$\Big($;
$getControllingMissionCall \,.\, mission.getControllingMission() \longrightarrow$
$getControllingMissionRet \,.\, mission.getControllingMission() \,?\, getControllingMission \longrightarrow$
var $distance : double \bullet distance := getAltitude$
if $(distance = readingOnGround) \longrightarrow$
$\Big($;
$requestTerminationCall \,.\, mission \longrightarrow$
$requestTerminationRet \,.\, mission \,?\, requestTermination \longrightarrow$
Skip $\Big)$
$[] \neg (distance = readingOnGround) \longrightarrow$ **Skip**
fi ;
Skip $\Big)$ $handleAsyncEventRet \,.\, Gro$
Skip $\Big)$

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

$\triangle(end\_periodic\_app \,.\, GroundDistanceMonitor \longrightarrow$ **Skip**$)$

end

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

- **Skip**

end

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

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

$$handlerAsyncEvent \mathrel{\widehat=} \left(\begin{array}{l} handleAsyncEventCall \,.\, InstrumentLandingSystemMonitor \longrightarrow \\ \Box\ handleAsyncEventRet \,.\, InstrumentLandingSystemMonitor \longrightarrow \\ \textbf{Skip} \end{array}\right)$$

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

$$\triangle(end\_periodic\_app \,.\, InstrumentLandingSystemMonitor \longrightarrow \textbf{Skip})$$

end

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

- **Skip**

end