aircraft

Tight Rope v0.6

30th November 2015

1 ID Files

1.1 MissionIds

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

$$MainMissionID : MissionID$$
$$TakeOffMissionID : MissionID$$
$$CruiseMissionID : MissionID$$
$$LandMissionID : MissionID$$

$$distinct\langle nullMissionId, MainMissionID, TakeOffMissionID, CruiseMissionID, LandMissionID\rangle$$

1.2 SchedulablesIds

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

$$
\begin{array}{l}
MainMissionSequencerID : SchedulableID \\
ACModeChangerID : SchedulableID \\
EnvironmentMonitorID : SchedulableID \\
ControlHandlerID : SchedulableID \\
FlightSensorsMonitorID : SchedulableID \\
CommunicationsHandlerID : SchedulableID \\
AperiodicSimulatorID : SchedulableID \\
LandingGearHandlerTakeOffID : SchedulableID \\
TakeOffMonitorID : SchedulableID \\
TakeOffFailureHandlerID : SchedulableID \\
BeginLandingHandlerID : SchedulableID \\
NavigationMonitorID : SchedulableID \\
GroundDistanceMonitorID : SchedulableID \\
LandingGearHandlerLandID : SchedulableID \\
InstrumentLandingSystemMonitorID : SchedulableID \\
SafeLandingHandlerID : SchedulableID
\end{array}
$$

$$
\begin{array}{l}
distinct\langle nullSequencerId, nullSchedulableId, MainMissionSequencerID, \\
ACModeChangerID, EnvironmentMonitorID, \\
ControlHandlerID, FlightSensorsMonitorID, \\
CommunicationsHandlerID, AperiodicSimulatorID, \\
LandingGearHandlerTakeOffID, TakeOffMonitorID, \\
TakeOffFailureHandlerID, BeginLandingHandlerID, \\
NavigationMonitorID, GroundDistanceMonitorID, \\
LandingGearHandlerLandID, InstrumentLandingSystemMonitorID, \\
SafeLandingHandlerID\rangle
\end{array}
$$

1.3 ThreadIds

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

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

1.4 ObjectIds

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

$$
\begin{array}{l}
ACSafeletObjectID : ObjectID \\
MainMissionObjectID : ObjectID \\
ACModeChangerObjectID : ObjectID \\
EnvironmentMonitorObjectID : ObjectID \\
ControlHandlerObjectID : ObjectID \\
FlightSensorsMonitorObjectID : ObjectID \\
CommunicationsHandlerObjectID : ObjectID \\
AperiodicSimulatorObjectID : ObjectID \\
TakeOffMissionObjectID : ObjectID \\
LandingGearHandlerTakeOffObjectID : ObjectID \\
TakeOffMonitorObjectID : ObjectID \\
TakeOffFailureHandlerObjectID : ObjectID \\
CruiseMissionObjectID : ObjectID \\
BeginLandingHandlerObjectID : ObjectID \\
NavigationMonitorObjectID : ObjectID \\
LandMissionObjectID : ObjectID \\
GroundDistanceMonitorObjectID : ObjectID \\
LandingGearHandlerLandObjectID : ObjectID \\
InstrumentLandingSystemMonitorObjectID : ObjectID \\
SafeLandingHandlerObjectID : ObjectID
\end{array}
$$

$$
\begin{array}{l}
distinct\langle ACSafeletObjectID, MainMissionObjectID, \\
ACModeChangerObjectID, EnvironmentMonitorObjectID, \\
ControlHandlerObjectID, FlightSensorsMonitorObjectID, \\
CommunicationsHandlerObjectID, AperiodicSimulatorObjectID, \\
TakeOffMissionObjectID, LandingGearHandlerTakeOffObjectID, \\
TakeOffMonitorObjectID, TakeOffFailureHandlerObjectID, \\
CruiseMissionObjectID, BeginLandingHandlerObjectID, \\
NavigationMonitorObjectID, LandMissionObjectID, \\
GroundDistanceMonitorObjectID, LandingGearHandlerLandObjectID, \\
InstrumentLandingSystemMonitorObjectID, SafeLandingHandlerObjectID\rangle
\end{array}
$$

2 Network

section *NetworkChannels* **parents** *scj_prelude*, *MissionId*, *MissionIds*,
SchedulableId, *SchedulableIds*, *MissionChan*, *SchedulableChan*, *TopLevelMissionSequencerFWChan*,
FrameworkChan, *SafeletChan*

channelset *TerminateSync* ==
{| *schedulables_terminated*, *schedulables_stopped*, *get_activeSchedulables* |}

channelset *ControlTierSync* ==
{| *start_toplevel_sequencer*, *done_toplevel_sequencer*, *done_safeletFW* |}

channelset *TierSync* ==
{| *start_mission* . , *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 *Tier*0*Sync* ==
{| *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 $Tier0 \mathrel{\widehat=}$
$$\left(\begin{array}{l} MissionFW(MainMissionID) \\ \quad [\![MissionSync]\!] \\ \left(\begin{array}{l} SchedulableMissionSequencerFW(ACModeChangerID) \\ \quad [\![SchedulablesSync]\!] \\ \left(\begin{array}{l} AperiodicEventHandlerFW(ControlHandlerID, (time(10,0), null)) \\ \quad [\![SchedulablesSync]\!] \\ AperiodicEventHandlerFW(CommunicationsHandlerID, (NULL, nullSchedulableId)) \end{array}\right) \\ \quad [\![SchedulablesSync]\!] \\ \left(\begin{array}{l} PeriodicEventHandlerFW(EnvironmentMonitorID, (time(10,0), NULL, NULL, nullSchedulableId)) \\ \quad [\![SchedulablesSync]\!] \\ PeriodicEventHandlerFW(FlightSensorsMonitorID, (time(10,0), NULL, NULL, nullSchedulableId)) \\ \quad [\![SchedulablesSync]\!] \\ PeriodicEventHandlerFW(AperiodicSimulatorID, (time(10,0), NULL, NULL, nullSchedulableId)) \end{array}\right) \end{array}\right) \end{array}\right)$$

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

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

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

$$
\begin{array}{l}
Threads \mathrel{\widehat{=}} \\
\left(\begin{array}{l}
ThreadFW(SafeLandingHandlerThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(ACModeChangerThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(TakeOffFailureHandlerThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(InstrumentLandingSystemMonitorThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(FlightSensorsMonitorThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(TakeOffMonitorThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(AperiodicSimulatorThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(LandingGearHandlerLandThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(LandingGearHandlerTakeOffThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(GroundDistanceMonitorThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(ControlHandlerThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(CommunicationsHandlerThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(BeginLandingHandlerThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(NavigationMonitorThreadID, 5) \\
\quad [\![ThreadSync]\!] \\
ThreadFW(EnvironmentMonitorThreadID, 5)
\end{array}\right)
\end{array}
$$

$$
\begin{array}{l}
Objects \mathrel{\widehat{=}} \\
\left(\begin{array}{l}
ObjectFW(ACSafeletObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(MainMissionObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(ACModeChangerObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(EnvironmentMonitorObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(ControlHandlerObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(FlightSensorsMonitorObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(CommunicationsHandlerObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(AperiodicSimulatorObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(TakeOffMissionObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(LandingGearHandlerTakeOffObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(TakeOffMonitorObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(TakeOffFailureHandlerObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(CruiseMissionObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(BeginLandingHandlerObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(NavigationMonitorObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(LandMissionObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(GroundDistanceMonitorObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(LandingGearHandlerLandObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(InstrumentLandingSystemMonitorObjectID) \\
\quad [\![ObjectSync]\!] \\
ObjectFW(SafeLandingHandlerObjectID)
\end{array}\right)
\end{array}
$$

$$Locking \mathrel{\widehat{=}} Threads \;|||\; Objects$$

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

3 Safelet

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

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

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

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

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

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

end

4 Top Level Mission Sequencer

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

$$State'$$

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

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

$\bullet$ **Skip**

end

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

channel $getNextMissionCall : SchedulableID$
channel $getNextMissionRet : SchedulableID \times MissionID$

5 Missions

5.1 MainMission

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

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

State

$this : \mathbf{ref}\ MainMissionClass$

state *State*

Init

$State'$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

end

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

state *State*

$ALTITUDE\_READING\_ON\_GROUND : double$
$test : \mathbb{Z}$
$cabinPressure : double$
$emergencyOxygen : double$
$fuelRemaining : double$
$altitude : double$
$airSpeed : double$
$heading : double$

state *State*

initial *Init*

$State'$

$ALTITUDE\_READING\_ON\_GROUND' = 0.0$
$test' = 0$

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 MainMission

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

process $ACModeChangerApp \mathrel{\widehat=}$
• **begin**

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

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

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

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

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

end

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

state *State*

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

state *State*

initial *Init*

$State'$

$modesLeft' = 3$
ref $currentModeClass' = \mathbf{new}\ ModeClass()$
ref $launchModeClass' = \mathbf{new}\ ModeClass()$
ref $cruiseModeClass' = \mathbf{new}\ ModeClass()$
ref $landModeClass' = \mathbf{new}\ ModeClass()$

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

$$
\begin{pmatrix}
\mathbf{if}\ (modesLeft = 3) \longrightarrow \\
\quad \begin{pmatrix} modesLeft := modesLeft - 1; \\ ret := TakeOffMission \end{pmatrix} \\
[]\ \neg\ (modesLeft = 3) \longrightarrow \\
\quad \mathbf{if}\ (modesLeft = 2) \longrightarrow \\
\quad \begin{pmatrix} modesLeft := modesLeft - 1; \\ ret := CruiseMission \end{pmatrix} \\
[]\ \neg\ (modesLeft = 2) \longrightarrow \\
\quad \mathbf{if}\ (modesLeft = 1) \longrightarrow \\
\quad \begin{pmatrix} modesLeft := modesLeft - 1; \\ ret := LandMission \end{pmatrix} \\
[]\ \neg\ (modesLeft = 1) \longrightarrow \\
\quad \big(ret := nullMissionId\big) \\
\mathbf{fi} \\
\mathbf{fi} \\
\mathbf{fi}
\end{pmatrix}
$$

• **Skip**

end

section $ACModeChangerMethChan$ **parents** $scj\_prelude, GlobalTypes, MissionId, SchedulableId$

channel $changeToCall : SchedulableID \times$
channel $changeToRet : SchedulableID$

channel $advanceModeCall : SchedulableID \times ThreadID$
channel $advanceModeRet : SchedulableID \times ThreadID$

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

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

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

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

• $(Methods) \triangle (end\_\_app\,.\,ControlHandler \longrightarrow \mathbf{Skip})$

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**

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

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

- $(Methods) \triangle (end\_\_app\,.\,CommunicationsHandler \longrightarrow \mathbf{Skip})$

end

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

- **Skip**

end

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

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

process $EnvironmentMonitorApp \mathrel{\widehat=}$
- **begin**

$handlerAsyncEvent \mathrel{\widehat=}$
$\Big($ *handleAsyncEventCall* . *EnvironmentMonitor* $\longrightarrow$
$\Big($ **Skip**;
setCabinPressureCall . *controllingMission* ! 0 $\longrightarrow$
setCabinPressureRet . *controllingMission* $\longrightarrow$
Skip;
setEmergencyOxygenCall . *controllingMission* ! 0 $\longrightarrow$
setEmergencyOxygenRet . *controllingMission* $\longrightarrow$
Skip;
setFuelRemainingCall . *controllingMission* ! 0 $\longrightarrow$
setFuelRemainingRet . *controllingMission* $\longrightarrow$
Skip $\Big)$;
handleAsyncEventRet . *EnvironmentMonitor* $\longrightarrow$
Skip $\Big)$

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

• $(Methods) \triangle (end\_periodic\_app \,.\, EnvironmentMonitor \longrightarrow \mathbf{Skip})$

end

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

- **Skip**

end

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

process *FlightSensorsMonitorApp* $\widehat{=}$
- **begin**

$$
\begin{array}{l}
handlerAsyncEvent \mathrel{\widehat{=}} \\
\left(\begin{array}{l}
handleAsyncEventCall\,.\,FlightSensorsMonitor \longrightarrow \\
\left(\begin{array}{l}
\textbf{Skip}; \\
setAirSpeedCall\,.\,controllingMission\,!\,0 \longrightarrow \\
setAirSpeedRet\,.\,controllingMission \longrightarrow \\
\textbf{Skip}; \\
setAltitudeCall\,.\,controllingMission\,!\,0 \longrightarrow \\
setAltitudeRet\,.\,controllingMission \longrightarrow \\
\textbf{Skip}; \\
setHeadingCall\,.\,controllingMission\,!\,0 \longrightarrow \\
setHeadingRet\,.\,controllingMission \longrightarrow \\
\textbf{Skip}
\end{array}\right) \\
handleAsyncEventRet\,.\,FlightSensorsMonitor \longrightarrow \\
\textbf{Skip}
\end{array}\right)
\end{array}
$$

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

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

end

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

- **Skip**

end

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

process $AperiodicSimulatorApp \mathrel{\widehat=}$
- **begin**

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

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

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

end

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

- **Skip**

end

5.3 TakeOffMission

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

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

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

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

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

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

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

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

• **Skip**

end

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

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

channel *getControllingMissionCall* : *MissionID*
channel *getControllingMissionRet* : *MissionID* × *MissionID*

channel *setControllingMissionCall* : *MissionID* × *MissionID*
channel *setControllingMissionRet* : *MissionID*

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

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

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

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

5.4 Schedulables of TakeOffMission

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

process $LandingGearHandlerTakeOffApp \mathrel{\widehat=}$
• **begin**

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

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

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

• $(Methods) \triangle (end\_\_app\ .\ LandingGearHandlerTakeOff \longrightarrow \mathbf{Skip})$

end

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

- **Skip**

end

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

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

process $TakeOffFailureHandlerApp \mathrel{\widehat=}$
• **begin**

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

var *currentSpeed* : *double* • *currentSpeed* := *getAirSpeed*
if (*currentSpeed* < *threshold*) $\longrightarrow$
$\Big($ **Skip**;
abortCall . *takeoffMission* $\longrightarrow$
abortRet . *takeoffMission* $\longrightarrow$
Skip;
requestTerminationCall . *takeoffMission* $\longrightarrow$
requestTerminationRet . *takeoffMission* ? *requestTermination* $\longrightarrow$
Skip $\Big)$
[] ¬ (*currentSpeed* < *threshold*) $\longrightarrow$
$\big($**Skip**$\big)$
fi Skip $\Big)$;
handleAsyncEventRet . *TakeOffFailureHandler* $\longrightarrow$
Skip $\Big)$

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

• (*Methods*) $\triangle$ (*end__app* . *TakeOffFailureHandler* $\longrightarrow$ **Skip**)

end

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

state *State*

$threshold : double$

state *State*

initial *Init*

$State'$

- **Skip**

end

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

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

process $TakeOffMonitorApp \mathrel{\widehat=}$
• **begin**

$handlerAsyncEvent \mathrel{\widehat=}$
$\Big($ *handleAsyncEventCall . TakeOffMonitor* $\longrightarrow$
$\Big($ **Skip**;
getControllingMissionCall . takeoffMission.getControllingMission() $\longrightarrow$
getControllingMissionRet . takeoffMission.getControllingMission() ? *getControllingMission* $\longrightarrow$

var *altitude* : *double* • *altitude* := *getAltitude*
if (*altitude* > *takeOffAltitude*) $\longrightarrow$
$\Big($ **Skip**;
releaseCall . landingGearHandler $\longrightarrow$
releaseRet . landingGearHandler ? *release* $\longrightarrow$
requestTerminationCall . takeoffMission $\longrightarrow$
requestTerminationRet . takeoffMission ? *requestTermination* $\longrightarrow$
Skip $\Big)$
$[]$ ¬ (*altitude* > *takeOffAltitude*) $\longrightarrow$ **Skip**
fi ;
Skip $\Big)$;
handleAsyncEventRet . TakeOffMonitor $\longrightarrow$
Skip $\Big)$

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

• (*Methods*) $\triangle$ (*end_periodic_app . TakeOffMonitor* $\longrightarrow$ **Skip**)

end

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

state *State*

$takeOffAltitude : double$

state *State*

initial *Init*

$State'$

- **Skip**

end

5.5 CruiseMission

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

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

State

$this : \textbf{ref}\ CruiseMissionClass$

state *State*

Init

$State'$

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

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

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

$$getControllingMissionMeth \mathrel{\widehat=} \textbf{var}\ ret : MissionID \bullet \begin{pmatrix} getControllingMissionCall\,.\,CruiseMission \longrightarrow \\ ret := this\,.\,getControllingMission(); \\ getControllingMissionRet\,.\,CruiseMission\,!\,ret \longrightarrow \\ \textbf{Skip} \end{pmatrix}$$

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

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

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 CruiseMission

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

process *BeginLandingHandlerApp* $\widehat{=}$
• **begin**

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

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

• $(Methods) \triangle (end\_\_app\,.\,BeginLandingHandler \longrightarrow \textbf{Skip})$

end

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

- **Skip**

end

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

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

process $NavigationMonitorApp \mathrel{\widehat=}$
• **begin**

$$
\begin{array}{l}
handlerAsyncEvent \mathrel{\widehat=} \\
\left(\begin{array}{l}
handleAsyncEventCall \,.\, NavigationMonitor \longrightarrow \\
\left(\begin{array}{l}
getControllingMissionCall \,.\, mission.getControllingMission() \longrightarrow \\
getControllingMissionRet \,.\, mission.getControllingMission() \,?\, getControllingMission \longrightarrow \\
\\
\textbf{var}\ heading : double \bullet heading := getHeading \\
getControllingMissionCall \,.\, mission.getControllingMission() \longrightarrow \\
getControllingMissionRet \,.\, mission.getControllingMission() \,?\, getControllingMission \longrightarrow \\
\\
\textbf{var}\ airSpeed : double \bullet airSpeed := getAirSpeed \\
getControllingMissionCall \,.\, mission.getControllingMission() \longrightarrow \\
getControllingMissionRet \,.\, mission.getControllingMission() \,?\, getControllingMission \longrightarrow \\
\\
\textbf{var}\ altitude : double \bullet altitude := getAltitude \\
\textbf{Skip}
\end{array}\right) \\
handleAsyncEventRet \,.\, NavigationMonitor \longrightarrow \\
\textbf{Skip}
\end{array}\right) \\
\end{array}
;
$$

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

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

end

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

- **Skip**

end

5.7 LandMission

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

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

State

$this : \mathbf{ref}\ LandMissionClass$

state *State*

Init

$State'$

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

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

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

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

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

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

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

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

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

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

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

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

• **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 LandMission

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

process $LandingGearHandlerLandApp \mathrel{\widehat=}$
- **begin**

$handlerAsyncEvent \mathrel{\widehat=}$
$$\left(\begin{array}{l} handleAsyncEventCall\,.\,LandingGearHandlerLand \longrightarrow \\ \left(\begin{array}{l} \textbf{Skip}; \\ isLandingGearDeployedCall\,.\,mission \longrightarrow \\ isLandingGearDeployedRet\,.\,mission\,?\,isLandingGearDeployed \longrightarrow \\ \\ \textbf{var}\ landingGearIsDeployed : \mathbb{B} \bullet landingGearIsDeployed := isLandingGearDeployed \\ \textbf{if}\ landingGearIsDeployed = \textbf{True} \longrightarrow \\ \qquad \left(\begin{array}{l} stowLandingGearCall\,.\,mission \longrightarrow \\ stowLandingGearRet\,.\,mission \longrightarrow \\ \textbf{Skip} \end{array}\right) \\ [] \neg landingGearIsDeployed = \textbf{True} \longrightarrow \\ \qquad \left(\begin{array}{l} deployLandingGearCall\,.\,mission\,.\,LandingGearHandlerLandThread \longrightarrow \\ deployLandingGearRet\,.\,mission\,.\,LandingGearHandlerLandThread \longrightarrow \\ \textbf{Skip} \end{array}\right) \\ \textbf{fi} \end{array}\right) \\ handleAsyncEventRet\,.\,LandingGearHandlerLand \longrightarrow \\ \textbf{Skip} \end{array}\right) ;$$

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

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

end

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

- **Skip**

end

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

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

process $SafeLandingHandlerApp \mathrel{\widehat=}$
• **begin**

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

var *altitude* : *double* • *altitude* := *getAltitude*
if (*altitude* < *threshold*) $\longrightarrow$
$\big($**Skip**$\big)$
$[]\ \neg$ (*altitude* < *threshold*) $\longrightarrow$
$\big($**Skip**$\big)$
fi $\Big)$;
handleAsyncEventRet . *SafeLandingHandler* $\longrightarrow$
Skip $\Big)$

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

• (*Methods*) $\triangle$ (*end__app* . *SafeLandingHandler* $\longrightarrow$ **Skip**)

end

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

state *State*

$threshold : double$

state *State*

initial *Init*

$State'$

- **Skip**

end

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

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

process *GroundDistanceMonitorApp* $\widehat{=}$
• **begin**

$$
\begin{array}{l}
\mathit{handlerAsyncEvent} \mathrel{\widehat{=}} \\
\left(\begin{array}{l}
\mathit{handleAsyncEventCall} \,.\, \mathit{GroundDistanceMonitor} \longrightarrow \\
\left(\begin{array}{l}
\textbf{Skip}; \\
\mathit{getControllingMissionCall} \,.\, \mathit{mission.getControllingMission}() \longrightarrow \\
\mathit{getControllingMissionRet} \,.\, \mathit{mission.getControllingMission}() \,?\, \mathit{getControllingMission} \longrightarrow \\
\\
\textbf{var}\ \mathit{distance} : \mathit{double} \bullet \mathit{distance} := \mathit{getAltitude} \\
\textbf{if}\ (\mathit{distance} = \mathit{readingOnGround}) \longrightarrow \\
\quad \left(\begin{array}{l}
\textbf{Skip}; \\
\mathit{requestTerminationCall} \,.\, \mathit{mission} \longrightarrow \\
\mathit{requestTerminationRet} \,.\, \mathit{mission} \,?\, \mathit{requestTermination} \longrightarrow \\
\textbf{Skip}
\end{array}\right) \\
[\!] \neg\, (\mathit{distance} = \mathit{readingOnGround}) \longrightarrow \textbf{Skip} \\
\textbf{fi}\,; \\
\textbf{Skip}
\end{array}\right) \\
\mathit{handleAsyncEventRet} \,.\, \mathit{GroundDistanceMonitor} \longrightarrow \\
\textbf{Skip}
\end{array}\right);
\end{array}
$$

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

• $(\mathit{Methods}) \triangle (\mathit{end\_periodic\_app} \,.\, \mathit{GroundDistanceMonitor} \longrightarrow \textbf{Skip})$

end

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

state *State*

$readingOnGround : double$

state *State*

initial *Init*

$State'$

- **Skip**

end

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

process *InstrumentLandingSystemMonitorApp* $\widehat{=}$
- **begin**

$$handlerAsyncEvent \mathrel{\widehat{=}} \begin{pmatrix} handleAsyncEventCall\,.\,InstrumentLandingSystemMonitor \longrightarrow \\ (\mathbf{Skip})\,; \\ handleAsyncEventRet\,.\,InstrumentLandingSystemMonitor \longrightarrow \\ \mathbf{Skip} \end{pmatrix}$$

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

- $(Methods) \triangle (end\_periodic\_app\,.\,InstrumentLandingSystemMonitor \longrightarrow \mathbf{Skip})$

end

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

- **Skip**

end