

aircraft

Tight Rope v0.6

5th December 2015

1 ID Files

1.1 MissionIds

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

MainMissionID : *MissionID*
TakeOffMissionID : *MissionID*
CruiseMissionID : *MissionID*
LandMissionID : *MissionID*

distinct(*nullMissionId*, *MainMissionID*, *TakeOffMissionID*,
CruiseMissionID, *LandMissionID*)

1.2 SchedulablesIds

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

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*

distinct(*nullSequencerId*, *nullSchedulableId*, *MainMissionSequencerID*,
ACModeChangerID, *EnvironmentMonitorID*,
ControlHandlerID, *FlightSensorsMonitorID*,
CommunicationsHandlerID, *AperiodicSimulatorID*,
LandingGearHandlerTakeOffID, *TakeOffMonitorID*,
TakeOffFailureHandlerID, *BeginLandingHandlerID*,
NavigationMonitorID, *GroundDistanceMonitorID*,
LandingGearHandlerLandID, *InstrumentLandingSystemMonitorID*,
SafeLandingHandlerID)

1.3 ThreadIDs

section *ThreadIDs* **parents** *scj_prelude, GlobalTypes*

SafeLandingHandlerThreadID : ThreadID
ACModeChangerThreadID : ThreadID
TakeOffFailureHandlerThreadID : ThreadID
InstrumentLandingSystemMonitorThreadID : ThreadID
FlightSensorsMonitorThreadID : ThreadID
TakeOffMonitorThreadID : ThreadID
AperiodicSimulatorThreadID : ThreadID
LandingGearHandlerLandThreadID : ThreadID
LandingGearHandlerTakeOffThreadID : ThreadID
GroundDistanceMonitorThreadID : ThreadID
ControlHandlerThreadID : ThreadID
CommunicationsHandlerThreadID : ThreadID
BeginLandingHandlerThreadID : ThreadID
NavigationMonitorThreadID : ThreadID
EnvironmentMonitorThreadID : ThreadID

distinct(*SafeletThreadId, nullThreadId,*
SafeLandingHandlerThreadID, ACModeChangerThreadID,
TakeOffFailureHandlerThreadID, InstrumentLandingSystemMonitorThreadID,
FlightSensorsMonitorThreadID, TakeOffMonitorThreadID,
AperiodicSimulatorThreadID, LandingGearHandlerLandThreadID,
LandingGearHandlerTakeOffThreadID, GroundDistanceMonitorThreadID,
ControlHandlerThreadID, CommunicationsHandlerThreadID,
BeginLandingHandlerThreadID, NavigationMonitorThreadID,
EnvironmentMonitorThreadID)

1.4 ObjectIds

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

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*

distinct(*ACSafeletObjectID*, *MainMissionObjectID*,
ACModeChangerObjectID, *EnvironmentMonitorObjectID*,
ControlHandlerObjectID, *FlightSensorsMonitorObjectID*,
CommunicationsHandlerObjectID, *AperiodicSimulatorObjectID*,
TakeOffMissionObjectID, *LandingGearHandlerTakeOffObjectID*,
TakeOffMonitorObjectID, *TakeOffFailureHandlerObjectID*,
CruiseMissionObjectID, *BeginLandingHandlerObjectID*,
NavigationMonitorObjectID, *LandMissionObjectID*,
GroundDistanceMonitorObjectID, *LandingGearHandlerLandObjectID*,
InstrumentLandingSystemMonitorObjectID, *SafeLandingHandlerObjectID*)

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* ==
 { *SafeltAppSync, MissionSequencerAppSync, MissionAppSync, MTAAppSync, 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, *ObjectFW*, *ThreadFW*,
ACSafeletApp, *MainMissionSequencerApp*, *MainMissionApp*, *ACModeChangerApp*, *ControlHandlerApp*,
CommunicationsHandlerApp, *EnvironmentMonitorApp*, *FlightSensorsMonitorApp*,
AperiodicSimulatorApp, *TakeOffMissionApp*, *LandingGearHandlerTakeOffApp*, *TakeOffFailureHandlerApp*,
TakeOffMonitorApp, *CruiseMissionApp*, *BeginLandingHandlerApp*, *NavigationMonitorApp*,
LandMissionApp, *LandingGearHandlerLandApp*, *SafeLandingHandlerApp*, *GroundDistanceMonitorApp*,
InstrumentLandingSystemMonitorApp

process *ControlTier* $\hat{=}$

$$\left(\begin{array}{l} \text{SafeletFW} \\ \llbracket \text{ControlTierSync} \rrbracket \\ \text{TopLevelMissionSequencerFW}(\text{MainMissionSequencer}) \end{array} \right)$$

process *Tier0* $\hat{=}$

$$\left(\begin{array}{l} \text{MissionFW}(\text{MainMissionID}) \\ \llbracket \text{MissionSync} \rrbracket \\ \left(\begin{array}{l} \text{SchedulableMissionSequencerFW}(\text{ACModeChangerID}) \\ \llbracket \text{SchedulablesSync} \rrbracket \\ \left(\begin{array}{l} \text{AperiodicEventHandlerFW}(\text{ControlHandlerID}, (\text{time}(10, 0), \text{null})) \\ \llbracket \text{SchedulablesSync} \rrbracket \\ \text{AperiodicEventHandlerFW}(\text{CommunicationsHandlerID}, (\text{NULL}, \text{nullSchedulableId})) \end{array} \right) \\ \llbracket \text{SchedulablesSync} \rrbracket \\ \left(\begin{array}{l} \text{PeriodicEventHandlerFW}(\text{EnvironmentMonitorID}, (\text{time}(10, 0), \text{NULL}, \text{NULL}, \text{nullSchedulableId})) \\ \llbracket \text{SchedulablesSync} \rrbracket \\ \text{PeriodicEventHandlerFW}(\text{FlightSensorsMonitorID}, (\text{time}(10, 0), \text{NULL}, \text{NULL}, \text{nullSchedulableId})) \\ \llbracket \text{SchedulablesSync} \rrbracket \\ \text{PeriodicEventHandlerFW}(\text{AperiodicSimulatorID}, (\text{time}(10, 0), \text{NULL}, \text{NULL}, \text{nullSchedulableId})) \end{array} \right) \end{array} \right) \end{array} \right)$$

process *Tier1* $\hat{=}$

$$\left(\begin{array}{l} \text{MissionFW}(\text{TakeOffMissionID}) \\ \llbracket \text{MissionSync} \rrbracket \\ \left(\begin{array}{l} \left(\begin{array}{l} \text{AperiodicEventHandlerFW}(\text{LandingGearHandlerTakeOffID}, (\text{NULL}, \text{nullSchedulableId})) \\ \llbracket \text{SchedulablesSync} \rrbracket \\ \text{AperiodicEventHandlerFW}(\text{TakeOffFailureHandlerID}, (\text{NULL}, \text{nullSchedulableId})) \end{array} \right) \\ \llbracket \text{SchedulablesSync} \rrbracket \\ \text{PeriodicEventHandlerFW}(\text{TakeOffMonitorID}, (\text{time}(0, 0), \text{time}(500, 0), \text{NULL}, \text{nullSchedulableId})) \end{array} \right) \\ \llbracket \text{ClusterSync} \rrbracket \\ \left(\begin{array}{l} \text{MissionFW}(\text{CruiseMissionID}) \\ \llbracket \text{MissionSync} \rrbracket \\ \left(\begin{array}{l} \text{AperiodicEventHandlerFW}(\text{BeginLandingHandlerID}, (\text{NULL}, \text{nullSchedulableId})) \\ \llbracket \text{SchedulablesSync} \rrbracket \\ \text{PeriodicEventHandlerFW}(\text{NavigationMonitorID}, (\text{time}(0, 0), \text{time}(10, 0), \text{NULL}, \text{nullSchedulableId})) \end{array} \right) \\ \llbracket \text{ClusterSync} \rrbracket \\ \left(\begin{array}{l} \text{MissionFW}(\text{LandMissionID}) \\ \llbracket \text{MissionSync} \rrbracket \\ \left(\begin{array}{l} \text{AperiodicEventHandlerFW}(\text{LandingGearHandlerLandID}, (\text{NULL}, \text{nullSchedulableId})) \\ \llbracket \text{SchedulablesSync} \rrbracket \\ \text{AperiodicEventHandlerFW}(\text{SafeLandingHandlerID}, (\text{NULL}, \text{nullSchedulableId})) \\ \llbracket \text{SchedulablesSync} \rrbracket \\ \left(\begin{array}{l} \text{PeriodicEventHandlerFW}(\text{GroundDistanceMonitorID}, (\text{time}(0, 0), \text{time}(10, 0), \text{NULL}, \text{nullSchedulableId})) \\ \llbracket \text{SchedulablesSync} \rrbracket \\ \text{PeriodicEventHandlerFW}(\text{InstrumentLandingSystemMonitorID}, (\text{time}(0, 0), \text{time}(10, 0), \text{NULL}, \text{nullSchedulableId})) \end{array} \right) \end{array} \right) \end{array} \right)$$

$$\text{process Framework} \hat{=} \left(\begin{array}{c} \text{ControlTier} \\ \llbracket \text{TierSync} \rrbracket \\ \left(\begin{array}{c} \text{Tier0} \\ \llbracket \text{Tier0Sync} \rrbracket \end{array} \right) \\ \text{Tier1} \end{array} \right)$$

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

$$\begin{aligned}
& \text{Threads} \triangleq \\
& \left(\begin{array}{l}
\text{ThreadFW}(\text{SafeLandingHandlerThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{ACModeChangerThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{TakeOffFailureHandlerThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{InstrumentLandingSystemMonitorThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{FlightSensorsMonitorThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{TakeOffMonitorThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{AperiodicSimulatorThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{LandingGearHandlerLandThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{LandingGearHandlerTakeOffThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{GroundDistanceMonitorThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{ControlHandlerThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{CommunicationsHandlerThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{BeginLandingHandlerThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{NavigationMonitorThreadID}, 5) \\
\quad \llbracket \text{ThreadSync} \rrbracket \\
\text{ThreadFW}(\text{EnvironmentMonitorThreadID}, 5)
\end{array} \right)
\end{aligned}$$

$$\begin{aligned}
\text{Objects} \hat{=} & \left(\begin{array}{l}
\text{ObjectFW}(\text{ACSafeletObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{MainMissionObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{ACModeChangerObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{EnvironmentMonitorObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{ControlHandlerObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{FlightSensorsMonitorObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{CommunicationsHandlerObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{AperiodicSimulatorObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{TakeOffMissionObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{LandingGearHandlerTakeOffObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{TakeOffMonitorObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{TakeOffFailureHandlerObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{CruiseMissionObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{BeginLandingHandlerObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{NavigationMonitorObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{LandMissionObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{GroundDistanceMonitorObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{LandingGearHandlerLandObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{InstrumentLandingSystemMonitorObjectID}) \\
\quad \llbracket \text{ObjectSync} \rrbracket \\
\text{ObjectFW}(\text{SafeLandingHandlerObjectID})
\end{array} \right)
\end{aligned}$$

$$\text{Locking} \hat{=} \text{Threads} \parallel \text{Objects}$$

$$\mathbf{process} \text{ Program} \hat{=} (\text{Framework} \llbracket \text{AppSync} \rrbracket \text{Application}) \llbracket \text{LockingSync} \rrbracket \text{Locking}$$

3 Safelet

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

process *ACSafeletApp* $\hat{=}$ **begin**

InitializeApplication $\hat{=}$
 $\left(\begin{array}{l} \textit{initializeApplicationCall} \longrightarrow \\ \textit{initializeApplicationRet} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$

GetSequencer $\hat{=}$
 $\left(\begin{array}{l} \textit{getSequencerCall} \longrightarrow \\ \textit{getSequencerRet} ! \textit{MainMissionSequencer} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$

Methods $\hat{=}$
 $\left(\begin{array}{l} \textit{GetSequencer} \\ \square \\ \textit{InitializeApplication} \end{array} \right); \textit{Methods}$

• $(\textit{Methods}) \triangle (\textit{end_safelet_app} \longrightarrow \mathbf{Skip})$

end

4 Top Level Mission Sequencer

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

process *MainMissionSequencerApp* $\hat{=}$ **begin**

<i>State</i> <i>this</i> : ref <i>MainMissionSequencerClass</i>

state *State*

<i>Init</i> <i>State</i> '
<i>this</i> ' = new <i>MainMissionSequencerClass</i> ()

GetNextMission $\hat{=}$ **var** *ret* : *MissionID* •
 $\left(\begin{array}{l} \textit{getNextMissionCall} . \textit{MainMissionSequencer} \longrightarrow \\ \textit{ret} := \textit{this} . \textit{getNextMission}(); \\ \textit{getNextMissionRet} . \textit{MainMissionSequencer} ! \textit{ret} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$

Methods $\hat{=}$
 $(\textit{GetNextMission}) ; \textit{Methods}$

• $(\textit{Init} ; \textit{Methods}) \triangle (\textit{end_sequencer_app} . \textit{MainMissionSequencer} \longrightarrow \mathbf{Skip})$

end

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

state <i>State</i> <i>returnedMission</i> : \mathbb{B}
--

state *State*

initial <i>Init</i> <i>State</i> '
<i>returnedMission</i> ' = <i>false</i>

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

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

• **Skip**

end

5 Missions

5.1 MainMission

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

process *MainMissionApp* $\hat{=}$ **begin**

State
this : **ref** *MainMissionClass*

state *State*

Init
State'

this' = **new** *MainMissionClass*()

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

CleanupPhase $\hat{=}$
 $\left(\begin{array}{l} \textit{cleanupMissionCall} . \textit{MainMission} \longrightarrow \\ \textit{cleanupMissionRet} . \textit{MainMission} ! \textbf{True} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

getAirSpeedMeth $\hat{=}$ **var** *ret* : \mathbb{R} •
 $\left(\begin{array}{l} \textit{getAirSpeedCall} . \textit{MainMission} \longrightarrow \\ \textit{ret} := \textit{this} . \textit{getAirSpeed}(); \\ \textit{getAirSpeedRet} . \textit{MainMission} ! \textit{ret} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

getAltitudeMeth $\hat{=}$ **var** *ret* : \mathbb{R} •
 $\left(\begin{array}{l} \textit{getAltitudeCall} . \textit{MainMission} \longrightarrow \\ \textit{ret} := \textit{this} . \textit{getAltitude}(); \\ \textit{getAltitudeRet} . \textit{MainMission} ! \textit{ret} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

getCabinPressureMeth $\hat{=}$ **var** *ret* : \mathbb{R} •
 $\left(\begin{array}{l} \textit{getCabinPressureCall} . \textit{MainMission} \longrightarrow \\ \textit{ret} := \textit{this} . \textit{getCabinPressure}(); \\ \textit{getCabinPressureRet} . \textit{MainMission} ! \textit{ret} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

$$\text{getEmergencyOxygenMeth} \hat{=} \mathbf{var} \text{ ret} : \mathbb{R} \bullet \left(\begin{array}{l} \text{getEmergencyOxygenCall} . \text{MainMission} \longrightarrow \\ \text{ret} := \text{this} . \text{getEmergencyOxygen}(); \\ \text{getEmergencyOxygenRet} . \text{MainMission} ! \text{ret} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

$$\text{getFuelRemainingMeth} \hat{=} \mathbf{var} \text{ ret} : \mathbb{R} \bullet \left(\begin{array}{l} \text{getFuelRemainingCall} . \text{MainMission} \longrightarrow \\ \text{ret} := \text{this} . \text{getFuelRemaining}(); \\ \text{getFuelRemainingRet} . \text{MainMission} ! \text{ret} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

$$\text{getHeadingMeth} \hat{=} \mathbf{var} \text{ ret} : \mathbb{R} \bullet \left(\begin{array}{l} \text{getHeadingCall} . \text{MainMission} \longrightarrow \\ \text{ret} := \text{this} . \text{getHeading}(); \\ \text{getHeadingRet} . \text{MainMission} ! \text{ret} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

$$\text{setAirSpeedMeth} \hat{=} \left(\begin{array}{l} \text{setAirSpeedCall} . \text{MainMission} ? \text{airSpeed} \longrightarrow \\ \text{this} . \text{setAirSpeed}(\text{airSpeed}); \\ \text{setAirSpeedRet} . \text{MainMission} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

$$\text{setAltitudeMeth} \hat{=} \left(\begin{array}{l} \text{setAltitudeCall} . \text{MainMission} ? \text{altitude} \longrightarrow \\ \text{this} . \text{setAltitude}(\text{altitude}); \\ \text{setAltitudeRet} . \text{MainMission} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

$$\text{setCabinPressureMeth} \hat{=} \left(\begin{array}{l} \text{setCabinPressureCall} . \text{MainMission} ? \text{cabinPressure} \longrightarrow \\ \text{this} . \text{setCabinPressure}(\text{cabinPressure}); \\ \text{setCabinPressureRet} . \text{MainMission} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

$$\text{setEmergencyOxygenMeth} \hat{=} \left(\begin{array}{l} \text{setEmergencyOxygenCall} . \text{MainMission} ? \text{emergencyOxygen} \longrightarrow \\ \text{this} . \text{setEmergencyOxygen}(\text{emergencyOxygen}); \\ \text{setEmergencyOxygenRet} . \text{MainMission} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

$$\text{setFuelRemainingMeth} \hat{=} \left(\begin{array}{l} \text{setFuelRemainingCall} . \text{MainMission} ? \text{fuelRemaining} \longrightarrow \\ \text{this} . \text{setFuelRemaining}(\text{fuelRemaining}); \\ \text{setFuelRemainingRet} . \text{MainMission} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

$$\text{setHeadingMeth} \hat{=} \left(\begin{array}{l} \text{setHeadingCall} . \text{MainMission} ? \text{heading} \longrightarrow \\ \text{this} . \text{setHeading}(\text{heading}); \\ \text{setHeadingRet} . \text{MainMission} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

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

- $(Init ; Methods) \triangle (end_mission_app . MainMission \longrightarrow \mathbf{Skip})$

end

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

state *State*

ALTITUDE_READING_ON_GROUND : \mathbb{R}
test : \mathbb{Z}
cabinPressure : \mathbb{R}
emergencyOxygen : \mathbb{R}
fuelRemaining : \mathbb{R}
altitude : \mathbb{R}
airSpeed : \mathbb{R}
heading : \mathbb{R}

state *State*

initial *Init*

State'
ALTITUDE_READING_ON_GROUND' = 0.0
test' = 0

public *getAirSpeed* $\hat{=}$ **var** *ret* : \mathbb{R} •
(*ret* := *airSpeed*)

public *getAltitude* $\hat{=}$ **var** *ret* : \mathbb{R} •
(*ret* := *altitude*)

public *getCabinPressure* $\hat{=}$ **var** *ret* : \mathbb{R} •
(*ret* := *cabinPressure*)

public *getEmergencyOxygen* $\hat{=}$ **var** *ret* : \mathbb{R} •
(*ret* := *emergencyOxygen*)

public *getFuelRemaining* $\hat{=}$ **var** *ret* : \mathbb{R} •
(*ret* := *fuelRemaining*)

public *getHeading* $\hat{=}$ **var** *ret* : \mathbb{R} •
(*ret* := *heading*)

public *setAirSpeed* $\hat{=}$
(*this.this.airSpeed* := *airSpeed*)

public *setAltitude* $\hat{=}$
(*this.this.altitude* := *altitude*)

public *setCabinPressure* $\hat{=}$
(*this.this.cabinPressure* := *cabinPressure*)

public *setEmergencyOxygen* $\hat{=}$
(*this.this.emergencyOxygen* := *emergencyOxygen*)


```
public setFuelRemaining  $\hat{=}$   
(this . this.fuelRemaining := fuelRemaining)
```

```
public setHeading  $\hat{=}$   
(this . this.heading := heading)
```

- **Skip**

```
end
```

5.2 Schedulables of MainMission

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

process *ACModeChangerApp* $\hat{=}$
controllingMission : *MissionID* • **begin**

GetNextMission $\hat{=}$ **var** *ret* : *MissionID* •
 $\left(\begin{array}{l} \textit{getNextMissionCall} . \textit{ACModeChanger} \longrightarrow \\ \textit{ret} := \textit{this} . \textit{getNextMission}(); \\ \textit{getNextMissionRet} . \textit{ACModeChanger} ! \textit{ret} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$

Methods $\hat{=}$
 $(\textit{GetNextMission}) ; \textit{Methods}$

• $(\textit{Methods}) \triangle (\textit{end_sequencer_app} . \textit{ACModeChanger} \longrightarrow \mathbf{Skip})$

end

```
class ACModeChangerClass  $\hat{=}$  begin
```

```
  state State  
    modesLeft :  $\mathbb{Z}$ 
```

```
state State
```

```
  initial Init  
    State'  
    modesLeft' = 3
```

```
protected getNextMission  $\hat{=}$  var ret : MissionID •
```

```
  ( if (modesLeft = 3)  $\longrightarrow$   
    ( modesLeft := modesLeft - 1;  
      ret := TakeOffMission )  
  |  $\neg$  (modesLeft = 3)  $\longrightarrow$   
    if (modesLeft = 2)  $\longrightarrow$   
      ( modesLeft := modesLeft - 1;  
        ret := CruiseMission )  
  |  $\neg$  (modesLeft = 2)  $\longrightarrow$   
    if (modesLeft = 1)  $\longrightarrow$   
      ( modesLeft := modesLeft - 1;  
        ret := LandMission )  
  |  $\neg$  (modesLeft = 1)  $\longrightarrow$   
    (ret := nullMissionId)  
  fi  
  fi  
  fi )
```

```
• Skip
```

```
end
```

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

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

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{ControlHandler} \longrightarrow \\ (\mathbf{Skip}) ; \\ \text{handleAsyncEventRet} . \text{ControlHandler} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

Methods $\hat{=}$
 $(\text{handlerAsyncEvent}) ; \text{Methods}$

• $(\text{Methods}) \triangle (\text{end_aperiodic_app} . \text{ControlHandler} \longrightarrow \mathbf{Skip})$

end

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

process *CommunicationsHandlerApp* $\hat{=}$ **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{CommunicationsHandler} \longrightarrow \\ (\mathbf{Skip}) ; \\ \text{handleAsyncEventRet} . \text{CommunicationsHandler} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

Methods $\hat{=}$
 $(\text{handlerAsyncEvent}) ; \text{Methods}$

• $(\text{Methods}) \triangle (\text{end_aperiodic_app} . \text{CommunicationsHandler} \longrightarrow \mathbf{Skip})$

end

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

process *EnvironmentMonitorApp* $\hat{=}$
mainMission : *MissionID* • **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{EnvironmentMonitor} \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{setCabinPressureCall} . \text{controllingMission} ! 0 \longrightarrow \\ \text{setCabinPressureRet} . \text{controllingMission} \longrightarrow \\ \mathbf{Skip}; \\ \text{setEmergencyOxygenCall} . \text{controllingMission} ! 0 \longrightarrow \\ \text{setEmergencyOxygenRet} . \text{controllingMission} \longrightarrow \\ \mathbf{Skip}; \\ \text{setFuelRemainingCall} . \text{controllingMission} ! 0 \longrightarrow \\ \text{setFuelRemainingRet} . \text{controllingMission} \longrightarrow \\ \mathbf{Skip} \end{array} \right) \\ \text{handleAsyncEventRet} . \text{EnvironmentMonitor} \longrightarrow \\ \mathbf{Skip} \end{array} \right) ;$$

Methods $\hat{=}$
(*handlerAsyncEvent*) ; *Methods*

• (*Methods*) \triangle (*end_periodic_app* . *EnvironmentMonitor* \longrightarrow **Skip**)

end

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

process *FlightSensorsMonitorApp* $\hat{=}$
mainMission : *MissionID* • **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{FlightSensorsMonitor} \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{setAirSpeedCall} . \text{controllingMission} ! 0 \longrightarrow \\ \text{setAirSpeedRet} . \text{controllingMission} \longrightarrow \\ \mathbf{Skip}; \\ \text{setAltitudeCall} . \text{controllingMission} ! 0 \longrightarrow \\ \text{setAltitudeRet} . \text{controllingMission} \longrightarrow \\ \mathbf{Skip}; \\ \text{setHeadingCall} . \text{controllingMission} ! 0 \longrightarrow \\ \text{setHeadingRet} . \text{controllingMission} \longrightarrow \\ \mathbf{Skip} \end{array} \right) ; \\ \text{handleAsyncEventRet} . \text{FlightSensorsMonitor} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

Methods $\hat{=}$
(*handlerAsyncEvent*) ; *Methods*

• (*Methods*) \triangle (*end_periodic_app* . *FlightSensorsMonitor* \longrightarrow **Skip**)

end

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

process *AperiodicSimulatorApp* $\hat{=}$
aperiodicEvent : *SchedulableID* • **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{AperiodicSimulator} \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{releaseCall} . \text{event} \longrightarrow \\ \text{releaseRet} . \text{event} ? \text{release} \longrightarrow \end{array} \right); \\ \mathbf{Skip} \\ \text{handleAsyncEventRet} . \text{AperiodicSimulator} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

Methods $\hat{=}$
(*handlerAsyncEvent*) ; *Methods*

• (*Methods*) \triangle (*end_periodic_app* . *AperiodicSimulator* \longrightarrow **Skip**)

end

5.3 TakeOffMission

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

process *TakeOffMissionApp* $\hat{=}$
controllingMission : *MissionID* • **begin**

State
this : **ref** *TakeOffMissionClass*

state *State*

Init
State'

this' = **new** *TakeOffMissionClass*()

InitializePhase $\hat{=}$
 $\left(\begin{array}{l} \textit{initializeCall} . \textit{TakeOffMission} \longrightarrow \\ \textit{register} ! \textit{LandingGearHandlerTakeOff} ! \textit{TakeOffMission} \longrightarrow \\ \textit{register} ! \textit{TakeOffMonitor} ! \textit{TakeOffMission} \longrightarrow \\ \textit{register} ! \textit{TakeOffFailureHandler} ! \textit{TakeOffMission} \longrightarrow \\ \textit{initializeRet} . \textit{TakeOffMission} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

CleanupPhase $\hat{=}$
 $\left(\begin{array}{l} \textit{cleanupMissionCall} . \textit{TakeOffMission} \longrightarrow \\ \textit{cleanupMissionRet} . \textit{TakeOffMission} ! \textbf{True} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

abortMeth $\hat{=}$
 $\left(\begin{array}{l} \textit{abortCall} . \textit{TakeOffMission} \longrightarrow \\ \textit{this} . \textit{abort}(); \\ \textit{abortRet} . \textit{TakeOffMission} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

getControllingMissionMeth $\hat{=}$ **var** *ret* : *MissionID* •
 $\left(\begin{array}{l} \textit{getControllingMissionCall} . \textit{TakeOffMission} \longrightarrow \\ \textit{ret} := \textit{this} . \textit{getControllingMission}(); \\ \textit{getControllingMissionRet} . \textit{TakeOffMission} ! \textit{ret} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

setControllingMissionMeth $\hat{=}$
 $\left(\begin{array}{l} \textit{setControllingMissionCall} . \textit{TakeOffMission} ? \textit{controllingMission} \longrightarrow \\ \textit{this} . \textit{setControllingMission}(\textit{controllingMission}); \\ \textit{setControllingMissionRet} . \textit{TakeOffMission} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

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

$$\text{stowLandingGearMeth} \hat{=} \left(\begin{array}{l} \text{stowLandingGearCall} . \text{TakeOffMission} \longrightarrow \\ \text{this} . \text{stowLandingGear}(); \\ \text{stowLandingGearRet} . \text{TakeOffMission} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

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

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

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

$$\bullet (\text{Init} ; \text{Methods}) \triangle (\text{end_mission_app} . \text{TakeOffMission} \longrightarrow \mathbf{Skip})$$

end

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

state *State*

SAFE_AIRSPPEED_THRESHOLD : \mathbb{R}

TAKEOFF_ALTITUDE : \mathbb{R}

abort : \mathbb{B}

landingGearDeployed : \mathbb{B}

state *State*

initial *Init*

State'

SAFE_AIRSPPEED_THRESHOLD' = 10.0

TAKEOFF_ALTITUDE' = 10.0

abort' = *false*

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

public *getControllingMission* $\hat{=}$ **var** *ret* : *MissionID* •
(*ret* := *controllingMission*)

public *setControllingMission* $\hat{=}$
(*this* . *this* . *controllingMission* := *controllingMission*)

public *cleanUp* $\hat{=}$ **var** *ret* : \mathbb{B} •
(**Skip**;
ret := (\neg *abort* = **True**))

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

public *isLandingGearDeployed* $\hat{=}$ **var** *ret* : \mathbb{B} •
(*ret* := *landingGearDeployed* = **True**)

• **Skip**

end

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

channel *abortCall* : *SchedulableID*
channel *abortRet* : *SchedulableID*

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

channel *setControllingMissionCall* : *SchedulableID* \times *MissionID*
channel *setControllingMissionRet* : *SchedulableID*

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

channel *stowLandingGearCall* : *SchedulableID*
channel *stowLandingGearRet* : *SchedulableID*

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

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

5.4 Schedulables of TakeOffMission

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

process *LandingGearHandlerTakeOffApp* $\hat{=}$
mission : *MissionID* • **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{LandingGearHandlerTakeOff} \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{isLandingGearDeployedCall} . \text{mission} \longrightarrow \\ \text{isLandingGearDeployedRet} . \text{mission} ? \text{isLandingGearDeployed} \longrightarrow \\ \\ \mathbf{var} \text{landingGearIsDeployed} : \mathbb{B} \bullet \text{landingGearIsDeployed} := \text{isLandingGearDeployed} \\ \mathbf{if} \text{landingGearIsDeployed} = \mathbf{True} \longrightarrow \\ \left(\begin{array}{l} \text{stowLandingGearCall} . \text{mission} \longrightarrow \\ \text{stowLandingGearRet} . \text{mission} \longrightarrow \\ \mathbf{Skip} \end{array} \right) \\ \square \neg \text{landingGearIsDeployed} = \mathbf{True} \longrightarrow \\ \left(\begin{array}{l} \text{deployLandingGearCall} . \text{mission} . \text{LandingGearHandlerTakeOffThread} \longrightarrow \\ \text{deployLandingGearRet} . \text{mission} . \text{LandingGearHandlerTakeOffThread} \longrightarrow \\ \mathbf{Skip} \end{array} \right) \\ \mathbf{fi} \end{array} \right) ; \\ \text{handleAsyncEventRet} . \text{LandingGearHandlerTakeOff} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

Methods $\hat{=}$
(*handlerAsyncEvent*) ; *Methods*

• (*Methods*) \triangle (*end_aperiodic_app* . *LandingGearHandlerTakeOff* \longrightarrow **Skip**)

end

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

process *TakeOffFailureHandlerApp* $\hat{=}$
takeoffMission : *MissionID*,
threshold : *Double* • **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{TakeOffFailureHandler} \longrightarrow \\ \left(\begin{array}{l} \text{getAirSpeedCall} . \text{mission} \longrightarrow \\ \text{getAirSpeedRet} . \text{mission} ? \text{getAirSpeed} \longrightarrow \end{array} \right) \\ \\ \mathbf{var} \text{ currentSpeed} : \mathbb{R} \bullet \text{currentSpeed} := \text{getAirSpeed} \\ \mathbf{if} (\text{currentSpeed} < \text{threshold}) \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \left(\begin{array}{l} \text{abortCall} . \text{takeoffMission} \longrightarrow \\ \text{abortRet} . \text{takeoffMission} \longrightarrow \end{array} \right) \\ \mathbf{Skip}; \\ \left(\begin{array}{l} \text{requestTerminationCall} . \text{takeoffMission} \longrightarrow \\ \text{requestTerminationRet} . \text{takeoffMission} ? \text{requestTermination} \longrightarrow \end{array} \right) \\ \mathbf{Skip} \end{array} \right) \\ \parallel \neg (\text{currentSpeed} < \text{threshold}) \longrightarrow \\ (\mathbf{Skip}) \\ \mathbf{fi} \mathbf{Skip} \end{array} \right) ; \\ \text{handleAsyncEventRet} . \text{TakeOffFailureHandler} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

Methods $\hat{=}$
(*handlerAsyncEvent*) ; *Methods*

• (*Methods*) \triangle (*end_aperiodic_app* . *TakeOffFailureHandler* \longrightarrow **Skip**)

end

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

state <i>State</i> <i>threshold</i> : \mathbb{R}
--

state *State*

initial <i>Init</i> <i>State'</i>

- **Skip**

end

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

process *TakeOffMonitorApp* $\hat{=}$
takeoffMission : *MissionID*,
takeOffAltitude : \mathbb{R} ,
landingGearHandler : *SchedulableID* • **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{TakeOffMonitor} \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{getControllingMissionCall} . \text{takeoffMission} . \text{getControllingMission}() \longrightarrow \\ \text{getControllingMissionRet} . \text{takeoffMission} . \text{getControllingMission}() ? \text{getControllingMission} \longrightarrow \\ \\ \mathbf{var} \text{altitude} : \mathbb{R} \bullet \text{altitude} := \text{getAltitude} \\ \mathbf{if} (\text{altitude} > \text{takeOffAltitude}) \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{releaseCall} . \text{landingGearHandler} \longrightarrow \\ \text{releaseRet} . \text{landingGearHandler} ? \text{release} \longrightarrow \\ \text{requestTerminationCall} . \text{takeoffMission} \longrightarrow \\ \text{requestTerminationRet} . \text{takeoffMission} ? \text{requestTermination} \longrightarrow \\ \mathbf{Skip} \end{array} \right) \\ \parallel \neg (\text{altitude} > \text{takeOffAltitude}) \longrightarrow \mathbf{Skip} \\ \mathbf{fi}; \\ \mathbf{Skip} \end{array} \right) ; \\ \text{handleAsyncEventRet} . \text{TakeOffMonitor} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

Methods $\hat{=}$
(*handlerAsyncEvent*) ; *Methods*

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

end

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

state *State*

takeOffAltitude : \mathbb{R}

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* $\hat{=}$
controllingMission : *MissionID* • **begin**

State
this : **ref** *CruiseMissionClass*

state *State*

Init
State'

this' = **new** *CruiseMissionClass*()

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

CleanupPhase $\hat{=}$
 $\left(\begin{array}{l} \textit{cleanupMissionCall} . \textit{CruiseMission} \longrightarrow \\ \textit{cleanupMissionRet} . \textit{CruiseMission!True} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

getControllingMissionMeth $\hat{=}$ **var** *ret* : *MissionID* •
 $\left(\begin{array}{l} \textit{getControllingMissionCall} . \textit{CruiseMission} \longrightarrow \\ \textit{ret} := \textit{this} . \textit{getControllingMission}(); \\ \textit{getControllingMissionRet} . \textit{CruiseMission!ret} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

Methods $\hat{=}$ $\left(\begin{array}{l} \textit{InitializePhase} \\ \square \\ \textit{CleanupPhase} \\ \square \\ \textit{getControllingMissionMeth} \end{array} \right)$; *Methods*

• (*Init* ; *Methods*) \triangle (*end_mission_app* . *CruiseMission* \longrightarrow **Skip**)

end

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

public *getControllingMission* $\hat{=}$ **var** *ret* : *MissionID* •
(*ret* := *controllingMission*)

• **Skip**

end

5.6 Schedulables of CruiseMission

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

process *BeginLandingHandlerApp* $\hat{=}$
controllingMission : *MissionID* • **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{BeginLandingHandler} \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{requestTerminationCall} . \text{controllingMission} \longrightarrow \\ \text{requestTerminationRet} . \text{controllingMission} ? \text{requestTermination} \longrightarrow \\ \mathbf{Skip} \end{array} \right) ; \\ \text{handleAsyncEventRet} . \text{BeginLandingHandler} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

Methods $\hat{=}$
(*handlerAsyncEvent*) ; *Methods*

• (*Methods*) \triangle (*end_aperiodic_app* . *BeginLandingHandler* \longrightarrow **Skip**)

end

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

process *NavigationMonitorApp* $\hat{=}$
mission : *MissionID* • **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{NavigationMonitor} \longrightarrow \\ \left(\begin{array}{l} \text{getControllingMissionCall} . \text{mission} . \text{getControllingMission}() \longrightarrow \\ \text{getControllingMissionRet} . \text{mission} . \text{getControllingMission}() ? \text{getControllingMission} \longrightarrow \end{array} \right) \\ \\ \text{var heading} : \mathbb{R} \bullet \text{heading} := \text{getHeading} \\ \text{getControllingMissionCall} . \text{mission} . \text{getControllingMission}() \longrightarrow \\ \text{getControllingMissionRet} . \text{mission} . \text{getControllingMission}() ? \text{getControllingMission} \longrightarrow \\ \\ \text{var airSpeed} : \mathbb{R} \bullet \text{airSpeed} := \text{getAirSpeed} \\ \text{getControllingMissionCall} . \text{mission} . \text{getControllingMission}() \longrightarrow \\ \text{getControllingMissionRet} . \text{mission} . \text{getControllingMission}() ? \text{getControllingMission} \longrightarrow \\ \\ \text{var altitude} : \mathbb{R} \bullet \text{altitude} := \text{getAltitude} \\ \text{Skip} \end{array} \right) ; \\ \text{handleAsyncEventRet} . \text{NavigationMonitor} \longrightarrow \\ \text{Skip}$$

Methods $\hat{=}$
(*handlerAsyncEvent*) ; *Methods*

• (*Methods*) \triangle (*end_periodic_app* . *NavigationMonitor* \longrightarrow **Skip**)

end

5.7 LandMission

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

process *LandMissionApp* $\hat{=}$
controllingMission : *MissionID* • **begin**

State
this : **ref** *LandMissionClass*

state *State*

Init
State'

this' = **new** *LandMissionClass*()

InitializePhase $\hat{=}$
 $\left(\begin{array}{l} \textit{initializeCall} . \textit{LandMission} \longrightarrow \\ \textit{register} ! \textit{GroundDistanceMonitor} ! \textit{LandMission} \longrightarrow \\ \textit{register} ! \textit{LandingGearHandlerLand} ! \textit{LandMission} \longrightarrow \\ \textit{register} ! \textit{InstrumentLandingSystemMonitor} ! \textit{LandMission} \longrightarrow \\ \textit{register} ! \textit{SafeLandingHandler} ! \textit{LandMission} \longrightarrow \\ \textit{initializeRet} . \textit{LandMission} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

CleanupPhase $\hat{=}$
 $\left(\begin{array}{l} \textit{cleanupMissionCall} . \textit{LandMission} \longrightarrow \\ \textit{cleanupMissionRet} . \textit{LandMission} ! \textbf{True} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

stowLandingGearMeth $\hat{=}$
 $\left(\begin{array}{l} \textit{stowLandingGearCall} . \textit{LandMission} \longrightarrow \\ \textit{this} . \textit{stowLandingGear}(); \\ \textit{stowLandingGearRet} . \textit{LandMission} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

isLandingGearDeployedMeth $\hat{=}$ **var** *ret* : \mathbb{B} •
 $\left(\begin{array}{l} \textit{isLandingGearDeployedCall} . \textit{LandMission} \longrightarrow \\ \textit{ret} := \textit{this} . \textit{isLandingGearDeployed}(); \\ \textit{isLandingGearDeployedRet} . \textit{LandMission} ! \textit{ret} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

getControllingMissionMeth $\hat{=}$ **var** *ret* : *MissionID* •
 $\left(\begin{array}{l} \textit{getControllingMissionCall} . \textit{LandMission} \longrightarrow \\ \textit{ret} := \textit{this} . \textit{getControllingMission}(); \\ \textit{getControllingMissionRet} . \textit{LandMission} ! \textit{ret} \longrightarrow \\ \textbf{Skip} \end{array} \right)$

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

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

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

$$\text{Methods} \hat{=} \left(\begin{array}{l} \text{InitializePhase} \\ \square \\ \text{CleanupPhase} \\ \square \\ \text{stowLandingGearMeth} \\ \square \\ \text{isLandingGearDeployedMeth} \\ \square \\ \text{getControllingMissionMeth} \\ \square \\ \text{abortMeth} \\ \square \\ \text{cleanUpMeth} \\ \square \\ \text{deployLandingGearSyncMeth} \end{array} \right) ; \text{Methods}$$

$$\bullet (\text{Init} ; \text{Methods}) \triangle (\text{end_mission_app} . \text{LandMission} \longrightarrow \mathbf{Skip})$$

end

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

state *State*

SAFE_LANDING_ALTITUDE : \mathbb{R}

abort : \mathbb{B}

landingGearDeployed : \mathbb{B}

state *State*

initial *Init*

State'

SAFE_LANDING_ALTITUDE' = 10.0

abort' = *false*

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

public *isLandingGearDeployed* $\hat{=}$ **var** *ret* : \mathbb{B} •
(*ret* := *landingGearDeployed* = **True**)

public *getControllingMission* $\hat{=}$ **var** *ret* : *MissionID* •
(*ret* := *controllingMission*)

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

public *cleanUp* $\hat{=}$ **var** *ret* : \mathbb{B} •
(**Skip**;
ret := (\neg *abort* = **True**))

• **Skip**

end

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

channel *stowLandingGearCall* : *SchedulableID*

channel *stowLandingGearRet* : *SchedulableID*

channel *isLandingGearDeployedCall* : *SchedulableID*

channel *isLandingGearDeployedRet* : *SchedulableID* \times \mathbb{B}

channel *getControllingMissionCall* : *SchedulableID*

channel *getControllingMissionRet* : *SchedulableID* \times *MissionID*

channel *abortCall* : *SchedulableID*

channel *abortRet* : *SchedulableID*

channel *cleanUpCall* : *SchedulableID*

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

channel *deployLandingGearCall* : *SchedulableID* \times *ThreadID*

channel *deployLandingGearRet* : *SchedulableID* \times *ThreadID*

5.8 Schedulables of LandMission

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

process *LandingGearHandlerLandApp* $\hat{=}$
mission : *MissionID* • **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{LandingGearHandlerLand} \longrightarrow \\ \left(\begin{array}{l} \text{Skip}; \\ \text{isLandingGearDeployedCall} . \text{mission} \longrightarrow \\ \text{isLandingGearDeployedRet} . \text{mission} ? \text{isLandingGearDeployed} \longrightarrow \\ \\ \text{var } \text{landingGearIsDeployed} : \mathbb{B} \bullet \text{landingGearIsDeployed} := \text{isLandingGearDeployed} \\ \text{if } \text{landingGearIsDeployed} = \text{True} \longrightarrow \\ \quad \left(\begin{array}{l} \text{stowLandingGearCall} . \text{mission} \longrightarrow \\ \text{stowLandingGearRet} . \text{mission} \longrightarrow \\ \text{Skip} \end{array} \right) \\ \quad \square \neg \text{landingGearIsDeployed} = \text{True} \longrightarrow \\ \quad \quad \left(\begin{array}{l} \text{deployLandingGearCall} . \text{mission} . \text{LandingGearHandlerLandThread} \longrightarrow \\ \text{deployLandingGearRet} . \text{mission} . \text{LandingGearHandlerLandThread} \longrightarrow \\ \text{Skip} \end{array} \right) \\ \text{fi} \end{array} \right) \\ \text{handleAsyncEventRet} . \text{LandingGearHandlerLand} \longrightarrow \\ \text{Skip} \end{array} \right);$$

Methods $\hat{=}$
(*handlerAsyncEvent*) ; *Methods*

• (*Methods*) \triangle (*end_aperiodic_app* . *LandingGearHandlerLand* \longrightarrow **Skip**)

end

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

process *SafeLandingHandlerApp* $\hat{=}$
landMission : *MissionID*,
threshold : *Double* • **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{SafeLandingHandler} \longrightarrow \\ \left(\begin{array}{l} \text{getControllingMissionCall} . \text{landMission} . \text{getControllingMission}() \longrightarrow \\ \text{getControllingMissionRet} . \text{landMission} . \text{getControllingMission}() ? \text{getControllingMission} \longrightarrow \end{array} \right) \\ \\ \text{var } \text{altitude} : \mathbb{R} \bullet \text{altitude} := \text{getAltitude} \\ \text{if } (\text{altitude} < \text{threshold}) \longrightarrow \\ \quad (\mathbf{Skip}) \\ \quad \square \neg (\text{altitude} < \text{threshold}) \longrightarrow \\ \quad \quad (\mathbf{Skip}) \\ \text{fi} \\ \text{handleAsyncEventRet} . \text{SafeLandingHandler} \longrightarrow \\ \mathbf{Skip} \end{array} \right) ;$$

Methods $\hat{=}$
(*handlerAsyncEvent*) ; *Methods*

• (*Methods*) \triangle (*end_aperiodic_app* . *SafeLandingHandler* \longrightarrow **Skip**)

end

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

state <i>State</i> <i>threshold</i> : \mathbb{R}
--

state *State*

initial <i>Init</i> <i>State'</i>

- **Skip**

end

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

process *GroundDistanceMonitorApp* $\hat{=}$
landMission : *MissionID* • **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{GroundDistanceMonitor} \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{getControllingMissionCall} . \text{mission} . \text{getControllingMission}() \longrightarrow \\ \text{getControllingMissionRet} . \text{mission} . \text{getControllingMission}() ? \text{getControllingMission} \longrightarrow \\ \\ \mathbf{var} \text{ distance} : \mathbb{R} \bullet \text{distance} := \text{getAltitude} \\ \mathbf{if} (\text{distance} = \text{readingOnGround}) \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{requestTerminationCall} . \text{mission} \longrightarrow \\ \text{requestTerminationRet} . \text{mission} ? \text{requestTermination} \longrightarrow \\ \mathbf{Skip} \end{array} \right) \\ \square \neg (\text{distance} = \text{readingOnGround}) \longrightarrow \mathbf{Skip} \\ \mathbf{fi}; \\ \mathbf{Skip} \end{array} \right) \\ \text{handleAsyncEventRet} . \text{GroundDistanceMonitor} \longrightarrow \\ \mathbf{Skip} \end{array} \right) ;$$

Methods $\hat{=}$
(*handlerAsyncEvent*) ; *Methods*

• (*Methods*) \triangle (*end_periodic_app* . *GroundDistanceMonitor* \longrightarrow **Skip**)

end

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

state *State*

readingOnGround : \mathbb{R}

state *State*

initial *Init*

State'

• **Skip**

end

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

process *InstrumentLandingSystemMonitorApp* $\hat{=}$
mission : *MissionID* • **begin**

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{InstrumentLandingSystemMonitor} \longrightarrow \\ (\mathbf{Skip}) ; \\ \text{handleAsyncEventRet} . \text{InstrumentLandingSystemMonitor} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

Methods $\hat{=}$
(*handlerAsyncEvent*) ; *Methods*

• (*Methods*) \triangle (*end_periodic_app* . *InstrumentLandingSystemMonitor* \longrightarrow **Skip**)

end