

aircraft

Tight Rope v0.65

4th February 2016

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*, *MainMissionSequencerIDID*,
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

2.1 Network Channel Sets

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 . MainMission, done_mission . MainMission, done_safeletFW, done_toplevel_sequencer* }

channelset *MissionSync* ==
 {*done_safeletFW, done_toplevel_sequencer, register, signalTerminationCall, signalTerminationRet, activate_schedulables, done_schedulable, cleanupSchedulableCall, cleanupSchedulableRet* }

channelset *SchedulablesSync* ==
 {*activate_schedulables, done_safeletFW, done_toplevel_sequencer* }

channelset *ClusterSync* ==
 {*done_toplevel_sequencer, done_safeletFW* }

channelset *AppSync* ==
 {*SafeltAppSync, MissionSequencerAppSync, MissionAppSync, MTAppSync, OSEHSync, APEHSync, getSequencer, end_mission_app, end_managedThread_app, setCeilingPriority, requestTerminationCall, requestTerminationRet, terminationPendingCall, terminationPendingRet, handleAsyncEventCall, handleAsyncEventRet* }

channelset *ThreadSync* ==
 {*raise_thread_priority, lower_thread_priority, isInterruptedCall, isInterruptedRet, get_priorityLevel* }

channelset *LockingSync* ==
 {*lockAcquired, startSyncMeth, endSyncMeth, waitCall, waitRet, notify, isInterruptedCall, isInterruptedRet, interruptedCall, interruptedRet, done_toplevel_sequencer, get_priorityLevel* }

channelset *Tier0Sync* ==
 {*done_toplevel_sequencer, done_safeletFW, start_mission . TakeOffMission, done_mission . TakeOffMission, initializeRet . TakeOffMission, requestTermination . TakeOffMission . MainMissionSequencer, start_mission . CruiseMission, done_mission . CruiseMission, initializeRet . CruiseMission, requestTermination . CruiseMission . MainMissionSequencer, start_mission . LandMission, done_mission . LandMission, initializeRet . LandMission, requestTermination . LandMission . MainMissionSequencer* }

2.2 MethodCallBinder

channel *binder_setCabinPressureCall* : *MissionID* \times *SchedulableID* \times \mathbb{R}
channel *binder_setCabinPressureRet* : *MissionID* \times *SchedulableID*

setCabinPressureLocs == {*MainMission*}
setCabinPressureCallers == {*EnvironmentMonitor*}

channel *binder_setEmergencyOxygenCall* : *MissionID* \times *SchedulableID* \times \mathbb{R}
channel *binder_setEmergencyOxygenRet* : *MissionID* \times *SchedulableID*

setEmergencyOxygenLocs == {*MainMission*}
setEmergencyOxygenCallers == {*EnvironmentMonitor*}

channel *binder_setFuelRemainingCall* : *MissionID* \times *SchedulableID* \times \mathbb{R}
channel *binder_setFuelRemainingRet* : *MissionID* \times *SchedulableID*

setFuelRemainingLocs == {*MainMission*}
setFuelRemainingCallers == {*EnvironmentMonitor*}

channel *binder_setAirSpeedCall* : *MissionID* \times *SchedulableID* \times \mathbb{R}
channel *binder_setAirSpeedRet* : *MissionID* \times *SchedulableID*

setAirSpeedLocs == {*MainMission*}
setAirSpeedCallers == {*FlightSensorsMonitor*}

channel *binder_setAltitudeCall* : *MissionID* \times *SchedulableID* \times \mathbb{R}
channel *binder_setAltitudeRet* : *MissionID* \times *SchedulableID*

setAltitudeLocs == {*MainMission*}
setAltitudeCallers == {*FlightSensorsMonitor*}

channel *binder_setHeadingCall* : *MissionID* \times *SchedulableID* \times \mathbb{R}
channel *binder_setHeadingRet* : *MissionID* \times *SchedulableID*

setHeadingLocs == {*MainMission*}
setHeadingCallers == {*FlightSensorsMonitor*}

channel *binder_isLandingGearDeployedCall* : *MissionID* \times *SchedulableID*
channel *binder_isLandingGearDeployedRet* : *MissionID* \times *SchedulableID* \times \mathbb{B}

isLandingGearDeployedLocs == {*TakeOffMission*}
isLandingGearDeployedCallers == {*LandingGearHandlerTakeOff*}

channel *binder_stowLandingGearCall* : *MissionID* \times *SchedulableID*
channel *binder_stowLandingGearRet* : *MissionID* \times *SchedulableID*

stowLandingGearLocs == { *TakeOffMission* }
stowLandingGearCallers == { *LandingGearHandlerTakeOff* }

channel *binder_deployLandingGearCall* : *MissionID* × *SchedulableID*
channel *binder_deployLandingGearRet* : *MissionID* × *SchedulableID*

deployLandingGearLocs == { *TakeOffMission* }
deployLandingGearCallers == { *LandingGearHandlerTakeOff* }

channel *binder_getAltitudeCall* : *MissionID* × *SchedulableID*
channel *binder_getAltitudeRet* : *MissionID* × *SchedulableID* × ℝ

getAltitudeLocs == { *MainMission* }
getAltitudeCallers == { *GroundDistanceMonitor*, *SafeLandingHandler*, *TakeOffMonitor*, *NavigationMonitor* }

channel *binder_getAirSpeedCall* : *MissionID* × *SchedulableID*
channel *binder_getAirSpeedRet* : *MissionID* × *SchedulableID* × ℝ

getAirSpeedLocs == { *MainMission* }
getAirSpeedCallers == { *NavigationMonitor*, *TakeOffFailureHandler* }

channel *binder_abortCall* : *MissionID* × *SchedulableID*
channel *binder_abortRet* : *MissionID* × *SchedulableID*

abortLocs == { *TakeOffMission* }
abortCallers == { *TakeOffFailureHandler* }

channel *binder_getHeadingCall* : *MissionID* × *SchedulableID*
channel *binder_getHeadingRet* : *MissionID* × *SchedulableID* × ℝ

getHeadingLocs == { *MainMission* }
getHeadingCallers == { *NavigationMonitor* }

channel *binder_getAirSpeedCall* : *MissionID* × *SchedulableID*
channel *binder_getAirSpeedRet* : *MissionID* × *SchedulableID* × ℝ

getAirSpeedLocs == { *MainMission* }
getAirSpeedCallers == { *NavigationMonitor*, *TakeOffFailureHandler* }

channel *binder_getAltitudeCall* : *MissionID* × *SchedulableID*
channel *binder_getAltitudeRet* : *MissionID* × *SchedulableID* × ℝ

getAltitudeLocs == { *MainMission* }
getAltitudeCallers == { *GroundDistanceMonitor*, *SafeLandingHandler*, *TakeOffMonitor*, *NavigationMonitor* }

channel *binder_getAltitudeCall* : *MissionID* \times *SchedulableID*
channel *binder_getAltitudeRet* : *MissionID* \times *SchedulableID* $\times \mathbb{R}$

getAltitudeLocs == { *MainMission* }
getAltitudeCallers == { *GroundDistanceMonitor*, *SafeLandingHandler*, *TakeOffMonitor*, *NavigationMonitor* }

channel *binder_isLandingGearDeployedCall* : *MissionID* \times *SchedulableID*
channel *binder_isLandingGearDeployedRet* : *MissionID* \times *SchedulableID* $\times \mathbb{B}$

isLandingGearDeployedLocs == { *LandMission* }
isLandingGearDeployedCallers == { *LandingGearHandlerLand* }

channel *binder_stowLandingGearCall* : *MissionID* \times *SchedulableID*
channel *binder_stowLandingGearRet* : *MissionID* \times *SchedulableID*

stowLandingGearLocs == { *LandMission* }
stowLandingGearCallers == { *LandingGearHandlerLand* }

channel *binder_deployLandingGearCall* : *MissionID* \times *SchedulableID*
channel *binder_deployLandingGearRet* : *MissionID* \times *SchedulableID*

deployLandingGearLocs == { *LandMission* }
deployLandingGearCallers == { *LandingGearHandlerLand* }

channel *binder_getAltitudeCall* : *MissionID* \times *SchedulableID*
channel *binder_getAltitudeRet* : *MissionID* \times *SchedulableID* $\times \mathbb{R}$

getAltitudeLocs == { *MainMission* }
getAltitudeCallers == { *GroundDistanceMonitor*, *SafeLandingHandler*, *TakeOffMonitor*, *NavigationMonitor* }

channelset *MethodCallBinderSync* == { *done_toplevel_sequencer*, *binder_setCabinPressureCall*, *binder_setCabinPressureRet*,
binder_setEmergencyOxygenCall, *binder_setEmergencyOxygenRet*,
binder_setFuelRemainingCall, *binder_setFuelRemainingRet*,
binder_setAirSpeedCall, *binder_setAirSpeedRet*,
binder_setAltitudeCall, *binder_setAltitudeRet*,
binder_setHeadingCall, *binder_setHeadingRet*,
binder_isLandingGearDeployedCall, *binder_isLandingGearDeployedRet*,
binder_stowLandingGearCall, *binder_stowLandingGearRet*,
binder_deployLandingGearCall, *binder_deployLandingGearRet*,
binder_getAltitudeCall, *binder_getAltitudeRet*,
binder_getAirSpeedCall, *binder_getAirSpeedRet*,
binder_abortCall, *binder_abortRet*,
binder_getHeadingCall, *binder_getHeadingRet*,
binder_getAirSpeedCall, *binder_getAirSpeedRet*,
binder_getAltitudeCall, *binder_getAltitudeRet*,
binder_getAltitudeCall, *binder_getAltitudeRet*,
binder_isLandingGearDeployedCall, *binder_isLandingGearDeployedRet*,
binder_stowLandingGearCall, *binder_stowLandingGearRet*,
binder_deployLandingGearCall, *binder_deployLandingGearRet*,
binder_getAltitudeCall, *binder_getAltitudeRet* }

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

$$\text{setCabinPressure_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_setCabinPressureCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{setCabinPressureLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{setCabinPressureCallers}) \times \mathbb{R} \longrightarrow \\ \text{setCabinPressureCall} . \text{loc} . \text{caller} \times \mathbb{R} \longrightarrow \\ \text{setCabinPressureRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{binder_setCabinPressureRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{setCabinPressure_MethodBinder} \end{array} \right)$$

$$\text{setEmergencyOxygen_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_setEmergencyOxygenCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{setEmergencyOxygenLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{setEmergencyOxygenCallers}) \times \mathbb{R} \longrightarrow \\ \text{setEmergencyOxygenCall} . \text{loc} . \text{caller} \times \mathbb{R} \longrightarrow \\ \text{setEmergencyOxygenRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{binder_setEmergencyOxygenRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{setEmergencyOxygen_MethodBinder} \end{array} \right)$$

$$\text{setFuelRemaining_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_setFuelRemainingCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{setFuelRemainingLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{setFuelRemainingCallers}) \times \mathbb{R} \longrightarrow \\ \text{setFuelRemainingCall} . \text{loc} . \text{caller} \times \mathbb{R} \longrightarrow \\ \text{setFuelRemainingRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{binder_setFuelRemainingRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{setFuelRemaining_MethodBinder} \end{array} \right)$$

$$\text{setAirSpeed_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_setAirSpeedCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{setAirSpeedLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{setAirSpeedCallers}) \times \mathbb{R} \longrightarrow \\ \text{setAirSpeedCall} . \text{loc} . \text{caller} \times \mathbb{R} \longrightarrow \\ \text{setAirSpeedRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{binder_setAirSpeedRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{setAirSpeed_MethodBinder} \end{array} \right)$$

$$\text{setAltitude_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_setAltitudeCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{setAltitudeLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{setAltitudeCallers}) \times \mathbb{R} \longrightarrow \\ \text{setAltitudeCall} . \text{loc} . \text{caller} \times \mathbb{R} \longrightarrow \\ \text{setAltitudeRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{binder_setAltitudeRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{setAltitude_MethodBinder} \end{array} \right)$$

$$\text{setHeading_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_setHeadingCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{setHeadingLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{setHeadingCallers}) \times \mathbb{R} \longrightarrow \\ \text{setHeadingCall} . \text{loc} . \text{caller} \times \mathbb{R} \longrightarrow \\ \text{setHeadingRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{binder_setHeadingRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{setHeading_MethodBinder} \end{array} \right)$$

$$isLandingGearDeployed_MethodBinder \hat{=} \left(\begin{array}{l} binder_isLandingGearDeployedCall \\ ? loc : (loc \in isLandingGearDeployedLocs) \\ ? caller : (caller \in isLandingGearDeployedCallers) \longrightarrow \\ isLandingGearDeployedCall . loc . caller \longrightarrow \\ isLandingGearDeployedRet . loc . caller ? ret \longrightarrow \\ binder_isLandingGearDeployedRet . loc . caller ! ret \longrightarrow \\ isLandingGearDeployed_MethodBinder \end{array} \right)$$

$$stowLandingGear_MethodBinder \hat{=} \left(\begin{array}{l} binder_stowLandingGearCall \\ ? loc : (loc \in stowLandingGearLocs) \\ ? caller : (caller \in stowLandingGearCallers) \longrightarrow \\ stowLandingGearCall . loc . caller \longrightarrow \\ stowLandingGearRet . loc . caller \longrightarrow \\ binder_stowLandingGearRet . loc . caller \longrightarrow \\ stowLandingGear_MethodBinder \end{array} \right)$$

$$deployLandingGear_MethodBinder \hat{=} \left(\begin{array}{l} binder_deployLandingGearCall \\ ? loc : (loc \in deployLandingGearLocs) \\ ? caller : (caller \in deployLandingGearCallers) \longrightarrow \\ deployLandingGearCall . loc . caller \longrightarrow \\ deployLandingGearRet . loc . caller \longrightarrow \\ binder_deployLandingGearRet . loc . caller \longrightarrow \\ deployLandingGear_MethodBinder \end{array} \right)$$

$$getAltitude_MethodBinder \hat{=} \left(\begin{array}{l} binder_getAltitudeCall \\ ? loc : (loc \in getAltitudeLocs) \\ ? caller : (caller \in getAltitudeCallers) \longrightarrow \\ getAltitudeCall . loc . caller \longrightarrow \\ getAltitudeRet . loc . caller ? ret \longrightarrow \\ binder_getAltitudeRet . loc . caller ! ret \longrightarrow \\ getAltitude_MethodBinder \end{array} \right)$$

$$getAirSpeed_MethodBinder \hat{=} \left(\begin{array}{l} binder_getAirSpeedCall \\ ? loc : (loc \in getAirSpeedLocs) \\ ? caller : (caller \in getAirSpeedCallers) \longrightarrow \\ getAirSpeedCall . loc . caller \longrightarrow \\ getAirSpeedRet . loc . caller ? ret \longrightarrow \\ binder_getAirSpeedRet . loc . caller ! ret \longrightarrow \\ getAirSpeed_MethodBinder \end{array} \right)$$

$$abort_MethodBinder \hat{=} \left(\begin{array}{l} binder_abortCall \\ ? loc : (loc \in abortLocs) \\ ? caller : (caller \in abortCallers) \longrightarrow \\ abortCall . loc . caller \longrightarrow \\ abortRet . loc . caller \longrightarrow \\ binder_abortRet . loc . caller \longrightarrow \\ abort_MethodBinder \end{array} \right)$$

$$\text{getHeading_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_getHeadingCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{getHeadingLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{getHeadingCallers}) \longrightarrow \\ \text{getHeadingCall} . \text{loc} . \text{caller} \longrightarrow \\ \text{getHeadingRet} . \text{loc} . \text{caller} ? \text{ret} \longrightarrow \\ \text{binder_getHeadingRet} . \text{loc} . \text{caller} ! \text{ret} \longrightarrow \\ \text{getHeading_MethodBinder} \end{array} \right)$$

$$\text{getAirSpeed_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_getAirSpeedCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{getAirSpeedLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{getAirSpeedCallers}) \longrightarrow \\ \text{getAirSpeedCall} . \text{loc} . \text{caller} \longrightarrow \\ \text{getAirSpeedRet} . \text{loc} . \text{caller} ? \text{ret} \longrightarrow \\ \text{binder_getAirSpeedRet} . \text{loc} . \text{caller} ! \text{ret} \longrightarrow \\ \text{getAirSpeed_MethodBinder} \end{array} \right)$$

$$\text{getAltitude_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_getAltitudeCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{getAltitudeLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{getAltitudeCallers}) \longrightarrow \\ \text{getAltitudeCall} . \text{loc} . \text{caller} \longrightarrow \\ \text{getAltitudeRet} . \text{loc} . \text{caller} ? \text{ret} \longrightarrow \\ \text{binder_getAltitudeRet} . \text{loc} . \text{caller} ! \text{ret} \longrightarrow \\ \text{getAltitude_MethodBinder} \end{array} \right)$$

$$\text{getAltitude_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_getAltitudeCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{getAltitudeLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{getAltitudeCallers}) \longrightarrow \\ \text{getAltitudeCall} . \text{loc} . \text{caller} \longrightarrow \\ \text{getAltitudeRet} . \text{loc} . \text{caller} ? \text{ret} \longrightarrow \\ \text{binder_getAltitudeRet} . \text{loc} . \text{caller} ! \text{ret} \longrightarrow \\ \text{getAltitude_MethodBinder} \end{array} \right)$$

$$\text{isLandingGearDeployed_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_isLandingGearDeployedCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{isLandingGearDeployedLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{isLandingGearDeployedCallers}) \longrightarrow \\ \text{isLandingGearDeployedCall} . \text{loc} . \text{caller} \longrightarrow \\ \text{isLandingGearDeployedRet} . \text{loc} . \text{caller} ? \text{ret} \longrightarrow \\ \text{binder_isLandingGearDeployedRet} . \text{loc} . \text{caller} ! \text{ret} \longrightarrow \\ \text{isLandingGearDeployed_MethodBinder} \end{array} \right)$$

$$\text{stowLandingGear_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_stowLandingGearCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{stowLandingGearLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{stowLandingGearCallers}) \longrightarrow \\ \text{stowLandingGearCall} . \text{loc} . \text{caller} \longrightarrow \\ \text{stowLandingGearRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{binder_stowLandingGearRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{stowLandingGear_MethodBinder} \end{array} \right)$$

$$\text{deployLandingGear_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_deployLandingGearCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{deployLandingGearLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{deployLandingGearCallers}) \longrightarrow \\ \text{deployLandingGearCall} . \text{loc} . \text{caller} \longrightarrow \\ \text{deployLandingGearRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{binder_deployLandingGearRet} . \text{loc} . \text{caller} \longrightarrow \\ \text{deployLandingGear_MethodBinder} \end{array} \right)$$

$$\text{getAltitude_MethodBinder} \hat{=} \left(\begin{array}{l} \text{binder_getAltitudeCall} \\ \quad ? \text{loc} : (\text{loc} \in \text{getAltitudeLocs}) \\ \quad ? \text{caller} : (\text{caller} \in \text{getAltitudeCallers}) \longrightarrow \\ \text{getAltitudeCall} . \text{loc} . \text{caller} \longrightarrow \\ \text{getAltitudeRet} . \text{loc} . \text{caller} ? \text{ret} \longrightarrow \\ \text{binder_getAltitudeRet} . \text{loc} . \text{caller} ! \text{ret} \longrightarrow \\ \text{getAltitude_MethodBinder} \end{array} \right)$$

$$\text{BinderActions} \hat{=} \left(\begin{array}{l} \text{setCabinPressure_MethodBinder} \\ ||| \\ \text{setEmergencyOxygen_MethodBinder} \\ ||| \\ \text{setFuelRemaining_MethodBinder} \\ ||| \\ \text{setAirSpeed_MethodBinder} \\ ||| \\ \text{setAltitude_MethodBinder} \\ ||| \\ \text{setHeading_MethodBinder} \\ ||| \\ \text{isLandingGearDeployed_MethodBinder} \\ ||| \\ \text{stowLandingGear_MethodBinder} \\ ||| \\ \text{deployLandingGear_MethodBinder} \\ ||| \\ \text{getAltitude_MethodBinder} \\ ||| \\ \text{getAirSpeed_MethodBinder} \\ ||| \\ \text{abort_MethodBinder} \\ ||| \\ \text{getHeading_MethodBinder} \\ ||| \\ \text{getAirSpeed_MethodBinder} \\ ||| \\ \text{getAltitude_MethodBinder} \\ ||| \\ \text{getAltitude_MethodBinder} \\ ||| \\ \text{isLandingGearDeployed_MethodBinder} \\ ||| \\ \text{stowLandingGear_MethodBinder} \\ ||| \\ \text{deployLandingGear_MethodBinder} \\ ||| \\ \text{getAltitude_MethodBinder} \end{array} \right)$$

- $\text{BinderActions} \triangle (\text{done_toplevel_sequencer} \longrightarrow \mathbf{Skip})$

end

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

2.3 Locking

process *Threads* $\hat{=}$

$$\left(\begin{array}{l} \textit{ThreadFW}(\textit{SafeLandingHandlerThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{ACModeChangerThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{TakeOffFailureHandlerThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{InstrumentLandingSystemMonitorThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{FlightSensorsMonitorThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{TakeOffMonitorThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{AperiodicSimulatorThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{LandingGearHandlerLandThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{LandingGearHandlerTakeOffThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{GroundDistanceMonitorThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{ControlHandlerThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{CommunicationsHandlerThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{BeginLandingHandlerThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{NavigationMonitorThreadID}, 5) \\ ||| \\ \textit{ThreadFW}(\textit{EnvironmentMonitorThreadID}, 5) \end{array} \right)$$

process *Objects* $\hat{=}$

$$\left(\begin{array}{l} \text{ObjectFW}(\text{ACSafeletObjectID}) \\ ||| \\ \text{ObjectFW}(\text{MainMissionObjectID}) \\ ||| \\ \text{ObjectFW}(\text{ACModeChangerObjectID}) \\ ||| \\ \text{ObjectFW}(\text{EnvironmentMonitorObjectID}) \\ ||| \\ \text{ObjectFW}(\text{ControlHandlerObjectID}) \\ ||| \\ \text{ObjectFW}(\text{FlightSensorsMonitorObjectID}) \\ ||| \\ \text{ObjectFW}(\text{CommunicationsHandlerObjectID}) \\ ||| \\ \text{ObjectFW}(\text{AperiodicSimulatorObjectID}) \\ ||| \\ \text{ObjectFW}(\text{TakeOffMissionObjectID}) \\ ||| \\ \text{ObjectFW}(\text{LandingGearHandlerTakeOffObjectID}) \\ ||| \\ \text{ObjectFW}(\text{TakeOffMonitorObjectID}) \\ ||| \\ \text{ObjectFW}(\text{TakeOffFailureHandlerObjectID}) \\ ||| \\ \text{ObjectFW}(\text{CruiseMissionObjectID}) \\ ||| \\ \text{ObjectFW}(\text{BeginLandingHandlerObjectID}) \\ ||| \\ \text{ObjectFW}(\text{NavigationMonitorObjectID}) \\ ||| \\ \text{ObjectFW}(\text{LandMissionObjectID}) \\ ||| \\ \text{ObjectFW}(\text{GroundDistanceMonitorObjectID}) \\ ||| \\ \text{ObjectFW}(\text{LandingGearHandlerLandObjectID}) \\ ||| \\ \text{ObjectFW}(\text{InstrumentLandingSystemMonitorObjectID}) \\ ||| \\ \text{ObjectFW}(\text{SafeLandingHandlerObjectID}) \end{array} \right)$$

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

2.4 Program

section *Program* **parents** *scj_prelude, MissionId, MissionIds, SchedulableId, SchedulableIds, MissionChan, SchedulableMethChan, MissionFW, SafeletFW, TopLevelMissionSequencerFW, NetworkChannels, ManagedThreadFW, SchedulableMissionSequencerFW, PeriodicEventHandlerFW, OneShotEventHandlerFW, AperiodicEventHandlerFW, ObjectFW, ThreadFW, ACSafeletApp, MainMissionSequencerApp, MainMissionApp, 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* $\hat{=}$

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

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 \end{array} \right) \\ \text{AperiodicEventHandlerFW}(\text{TakeOffFailureHandlerID}, (\text{NULL}, \text{nullSchedulableId})) \\ \llbracket \text{SchedulablesSync} \rrbracket \end{array} \right) \\ \text{PeriodicEventHandlerFW}(\text{TakeOffMonitorID}, (\text{time}(0, 0), \text{time}(500, 0), \text{NULL}, \text{nullSchedulableId})) \\ \llbracket \text{ClusterSync} \rrbracket \end{array} \right) \\ \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 \end{array} \right) \\ \text{PeriodicEventHandlerFW}(\text{NavigationMonitorID}, (\text{time}(0, 0), \text{time}(10, 0), \text{NULL}, \text{nullSchedulableId})) \\ \llbracket \text{ClusterSync} \rrbracket \end{array} \right) \\ \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 \end{array} \right) \\ \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)$$

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

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

$$\text{process Program} \triangleq (\text{Framework} \llbracket \text{AppSync} \rrbracket \text{ApplicationB}) \llbracket \text{LockingSync} \rrbracket \text{Locking}$$

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

immortalMemorySizeMeth $\hat{=}$ **var** *ret* : \mathbb{Z} •
 $\left(\begin{array}{l} \textit{immortalMemorySizeCall} . \textit{ACSafelet} \longrightarrow \\ (\textit{ret} := \textit{Const.IMMORTAL_MEM_DEFAULT}) ; \\ \textit{immortalMemorySizeRet} . \textit{ACSafelet} ! \textit{ret} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$

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

• (*Methods*) \triangle (*end_safelet_app* \longrightarrow **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 $\hat{=}$
(*GetNextMission*) ; *Methods*

• (*Init* ; *Methods*) \triangle (*end_sequencer_app* . *MainMissionSequencer* \longrightarrow **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* •

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

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

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

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

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

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

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

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

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

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

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

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

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

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*

controllingMission : *MainMission*
modesLeft : \mathbb{Z}

state *State*

initial *Init*

State'

modesLeft' = 3

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

$\left(\begin{array}{l} \text{if } (modesLeft = 3) \longrightarrow \\ \quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ ret := TakeOffMission \end{array} \right) \\ \parallel (modesLeft = 3) \longrightarrow \\ \quad \text{if } (modesLeft = 2) \longrightarrow \\ \quad \quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ ret := CruiseMission \end{array} \right) \\ \parallel (modesLeft = 2) \longrightarrow \\ \quad \text{if } (modesLeft = 1) \longrightarrow \\ \quad \quad \left(\begin{array}{l} modesLeft := modesLeft - 1; \\ ret := LandMission \end{array} \right) \\ \parallel (modesLeft = 1) \longrightarrow \\ \quad (ret := nullMissionId) \\ \text{fi} \\ \text{fi} \\ \text{fi} \end{array} \right)$

• **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 $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{EnvironmentMonitor} \longrightarrow \\ \quad \left(\begin{array}{l} \mathbf{Skip}; \\ \text{binder_setCabinPressureCall} . \text{controllingMission} . \text{EnvironmentMonitor} ! 0 \longrightarrow \text{binder_setCabinPressureRet} . \text{contro} \\ \text{binder_setEmergencyOxygenCall} . \text{controllingMission} . \text{EnvironmentMonitor} ! 0 \longrightarrow \text{binder_setEmergencyOxygenRet} \\ \text{binder_setFuelRemainingCall} . \text{controllingMission} . \text{EnvironmentMonitor} ! 0 \longrightarrow \text{binder_setFuelRemainingRet} . \text{contro} \end{array} \right) \\ \text{handleAsyncEventRet} . \text{EnvironmentMonitor} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

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

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

end

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

state *State*

controllingMission : *MainMission*

state *State*

initial *Init*

State'

• **Skip**

end

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

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

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{FlightSensorsMonitor} \longrightarrow \\ \quad \left(\begin{array}{l} \mathbf{Skip}; \\ \text{binder_setAirSpeedCall} . \text{controllingMission} . \text{FlightSensorsMonitor} ! 0 \longrightarrow \text{binder_setAirSpeedRet} . \text{controllingMission} \\ \text{binder_setAltitudeCall} . \text{controllingMission} . \text{FlightSensorsMonitor} ! 0 \longrightarrow \text{binder_setAltitudeRet} . \text{controllingMission} \\ \text{binder_setHeadingCall} . \text{controllingMission} . \text{FlightSensorsMonitor} ! 0 \longrightarrow \text{binder_setHeadingRet} . \text{controllingMission} \end{array} \right) \\ \text{handleAsyncEventRet} . \text{FlightSensorsMonitor} \longrightarrow \\ \mathbf{Skip} \end{array} \right)$$

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

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

end

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

state *State*

controllingMission : *MainMission*

state *State*

initial *Init*

State'

• **Skip**

end

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

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

handlerAsyncEvent $\hat{=}$

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

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

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

end

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

state *State*

event : *AperiodicEventHandler*

state *State*

initial *Init*

State'

• **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}
controllingMission : *MainMission*
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* : *MissionID* \times *SchedulableID*
channel *abortRet* : *MissionID* \times *SchedulableID*

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

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

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

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

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

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

5.4 Schedulables of TakeOffMission

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

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

handlerAsyncEvent $\hat{=}$

$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{LandingGearHandlerTakeOff} \longrightarrow \\ \quad \left(\begin{array}{l} \text{Skip}; \\ \text{binder_isLandingGearDeployedCall} . \text{mission} . \text{LandingGearHandlerTakeOff} \longrightarrow \text{binder_isLandingGearDeployedRet} \\ \quad \text{var landingGearIsDeployed} : \mathbb{B} \bullet \text{landingGearIsDeployed} := \text{isLandingGearDeployed} \quad \text{if } \text{landingGearIsDeployed} = \text{True} \\ \quad \quad (\text{binder_stowLandingGearCall} . \text{mission} . \text{LandingGearHandlerTakeOff} \longrightarrow \text{binder_stowLandingGearRet} . \text{mission}) \\ \quad \quad \parallel \text{landingGearIsDeployed} = \text{True} \longrightarrow \\ \quad \quad \quad (\text{binder_deployLandingGearCall} . \text{mission} . \text{LandingGearHandlerTakeOff} . \text{LandingGearHandlerTakeOffThreadID}) \\ \quad \quad \text{fi} \end{array} \right) \\ \text{handleAsyncEventRet} . \text{LandingGearHandlerTakeOff} \longrightarrow \\ \text{Skip} \end{array} \right)$

Methods $\hat{=}$

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

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

end

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

state *State*

mission : *TakeOffMission*

state *State*

initial *Init*

State'

• **Skip**

end

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

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

handlerAsyncEvent $\hat{=}$
 $\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{TakeOffFailureHandler} \longrightarrow \\ \left(\begin{array}{l} \text{binder_getAirSpeedCall} . \text{mainMission} . \text{TakeOffFailureHandler} \longrightarrow \text{binder_getAirSpeedRet} . \text{mainMission} . \text{TakeOffFailureHandler} \\ \text{var } \text{currentSpeed} : \mathbb{R} \bullet \text{currentSpeed} := \text{getAirSpeed} \quad \text{if } (\text{currentSpeed} < \text{threshold}) \longrightarrow \\ \quad \left(\begin{array}{l} \text{Skip}; \\ \text{binder_abortCall} . \text{takeoffMission} . \text{TakeOffFailureHandler} \longrightarrow \text{binder_abortRet} . \text{takeoffMission} . \text{TakeOffFailureHandler} \\ \text{requestTerminationCall} . \text{takeoffMission} . \text{TakeOffFailureHandler} \longrightarrow \text{requestTerminationRet} . \text{takeoffMission} . \text{TakeOffFailureHandler} \end{array} \right) \\ \parallel (\text{currentSpeed} < \text{threshold}) \longrightarrow \\ \quad (\text{Skip}) \end{array} \right) \\ \text{fi Skip} \end{array} \right) \\ \text{handleAsyncEventRet} . \text{TakeOffFailureHandler} \longrightarrow \\ \text{Skip} \end{array} \right)$

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

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

end

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

state *State*

mainMission : *MainMission*
takeoffMission : *TakeOffMission*
threshold : \mathbb{R}

state *State*

initial *Init*

State'

• **Skip**

end

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

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

handlerAsyncEvent $\hat{=}$
 $\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{TakeOffMonitor} \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{binder_getAltitudeCall} . \text{mainMission} . \text{TakeOffMonitor} \longrightarrow \text{binder_getAltitudeRet} . \text{mainMission} . \text{TakeOffMonitor} ? \text{re} \\ \mathbf{var} \text{altitude} : \mathbb{R} \bullet \text{altitude} := \text{getAltitude} \quad \mathbf{if} \text{ (altitude > takeOffAltitude)} \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{releaseCall} . \text{landingGearHandler} . \text{TakeOffMonitor} \longrightarrow \text{releaseRet} . \text{landingGearHandler} . \text{TakeOffMonitor} ? \text{re} \\ \parallel (\text{altitude} > \text{takeOffAltitude}) \longrightarrow \mathbf{Skip} \end{array} \right) \\ \mathbf{fi}; \\ \mathbf{Skip} \end{array} \right) \\ \text{handleAsyncEventRet} . \text{TakeOffMonitor} \longrightarrow \\ \mathbf{Skip} \end{array} \right.$

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

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

end

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

state *State*

mainMission : *MainMission*

takeoffMission : *TakeOffMission*

takeOffAltitude : \mathbb{R}

landingGearHandler : *AperiodicEventHandler*

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

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

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

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**

state *State*

controllingMission : *MainMission*

state *State*

initial *Init*

State'

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 $\hat{=}$

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

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

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

end

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

state *State*

controllingMission : *Mission*

state *State*

initial *Init*

State'

• **Skip**

end

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

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

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{NavigationMonitor} \longrightarrow \\ \left(\begin{array}{l} \text{binder_getHeadingCall} . \text{mainMission} . \text{NavigationMonitor} \longrightarrow \text{binder_getHeadingRet} . \text{mainMission} . \text{NavigationMo} \\ \text{var heading} : \mathbb{R} \bullet \text{heading} := \text{getHeading} \text{ binder_getAirSpeedCall} . \text{mainMission} . \text{NavigationMonitor} \longrightarrow \text{binder_g} \\ \text{var airSpeed} : \mathbb{R} \bullet \text{airSpeed} := \text{getAirSpeed} \text{ binder_getAltitudeCall} . \text{mainMission} . \text{NavigationMonitor} \longrightarrow \text{binder} \\ \text{var altitude} : \mathbb{R} \bullet \text{altitude} := \text{getAltitude} \text{ Skip} \end{array} \right) \\ \text{handleAsyncEventRet} . \text{NavigationMonitor} \longrightarrow \\ \text{Skip} \end{array} \right)$$

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

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

end

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

state *State*

mainMission : *MainMission*

state *State*

initial *Init*

State'

• **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*

controllingMission : *MainMission*
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* : *MissionID* \times *SchedulableID*

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

channel *isLandingGearDeployedCall* : *MissionID* \times *SchedulableID*

channel *isLandingGearDeployedRet* : *MissionID* \times *SchedulableID* \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 *SchedulableID* \times *ThreadID*

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

5.8 Schedulables of LandMission

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

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

handlerAsyncEvent $\hat{=}$

$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{LandingGearHandlerLand} \longrightarrow \\ \quad \left(\begin{array}{l} \text{Skip}; \\ \text{binder_isLandingGearDeployedCall} . \text{mission} . \text{LandingGearHandlerLand} \longrightarrow \text{binder_isLandingGearDeployedRet} . m \\ \quad \text{var landingGearIsDeployed} : \mathbb{B} \bullet \text{landingGearIsDeployed} := \text{isLandingGearDeployed} \quad \text{if } \text{landingGearIsDeployed} = \text{True} \\ \quad \left(\text{binder_stowLandingGearCall} . \text{mission} . \text{LandingGearHandlerLand} \longrightarrow \text{binder_stowLandingGearRet} . \text{mission} . \\ \quad \parallel \text{landingGearIsDeployed} = \text{True} \longrightarrow \\ \quad \quad \left(\text{binder_deployLandingGearCall} . \text{mission} . \text{LandingGearHandlerLand} . \text{LandingGearHandlerLandThreadID} \longrightarrow \right. \\ \quad \quad \text{fi} \\ \text{handleAsyncEventRet} . \text{LandingGearHandlerLand} \longrightarrow \\ \text{Skip} \end{array} \right. \end{array} \right.$

Methods $\hat{=}$

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

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

end

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

state *State*

mission : *LandMission*

state *State*

initial *Init*

State'

• **Skip**

end

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

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

handlerAsyncEvent $\hat{=}$

$$\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{SafeLandingHandler} \longrightarrow \\ \left(\begin{array}{l} \text{binder_getAltitudeCall} . \text{mainMission} . \text{SafeLandingHandler} \longrightarrow \text{binder_getAltitudeRet} . \text{mainMission} . \text{SafeLandingHandler} \\ \text{var altitude} : \mathbb{R} \bullet \text{altitude} := \text{getAltitude} \quad \text{if } (\text{altitude} < \text{threshold}) \longrightarrow \\ \quad (\text{Skip}) \\ \parallel (\text{altitude} < \text{threshold}) \longrightarrow \\ \quad (\text{Skip}) \end{array} \right. \\ \text{fi} \\ \text{handleAsyncEventRet} . \text{SafeLandingHandler} \longrightarrow \\ \text{Skip} \end{array} \right.$$

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

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

end

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

state *State*

mainMission : *MainMission*

threshold : \mathbb{R}

state *State*

initial *Init*

State'

• **Skip**

end

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

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

handlerAsyncEvent $\hat{=}$
 $\left(\begin{array}{l} \text{handleAsyncEventCall} . \text{GroundDistanceMonitor} \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{binder_getAltitudeCall} . \text{mainMission} . \text{GroundDistanceMonitor} \longrightarrow \text{binder_getAltitudeRet} . \text{mainMission} . \text{GroundD} \\ \mathbf{var} \text{ distance} : \mathbb{R} \bullet \text{distance} := \text{getAltitude} \quad \mathbf{if} (\text{distance} = \text{readingOnGround}) \longrightarrow \\ \left(\begin{array}{l} \mathbf{Skip}; \\ \text{requestTerminationCall} . \text{mainMission} . \text{GroundDistanceMonitor} \longrightarrow \text{requestTerminationRet} . \text{mainMission} . G \\ \parallel (\text{distance} = \text{readingOnGround}) \longrightarrow \mathbf{Skip} \\ \mathbf{fi}; \\ \mathbf{Skip} \end{array} \right) \end{array} \right) \\ \text{handleAsyncEventRet} . \text{GroundDistanceMonitor} \longrightarrow \\ \mathbf{Skip} \end{array} \right.$

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

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

end

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

state *State*

mainMission : *MainMission*

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

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

state *State*

mission : *LandMission*

state *State*

initial *Init*

State'

• **Skip**

end