TITLE:

DEPLOY Work Package 3

Attitude and Orbit Control System Software Requirements Document

	FUNCTION	NAME	DATE
PREPARED BY	Verification Engineer	Kimmo Varpaaniemi	17.12.2010

REF:	DEP-RP-SSF-R-005
ISSUE:	1.0
DATE:	17.12.2010

Document Status Sheet

Issue	Date	Modified Items / Reason for Change
1.0	17.12.2010	Initial issue of the document.

Table of Contents

List of Figures

1. Introduction

1.1 Purpose

This Software Requirements Document (SRD) identifies and documents the requirements of the DEPLOY Work Package 3 (WP3) Attitude and Orbit Control System (AOCS) Software (SW). The document is mainly intended for the following categories of readers:

- The software designer – to form the basis for the design and implementation of the software.
- The software validation engineer – to form the formal requirements against which the software is validated.

1.2 Scope

This document describes the functional and non-functional requirements on the software. The requirements try to capture the spirit rather than the letter of the no longer maintained executable specification [RD1] (see also the related description in the deliverable [RD2]).

1.3 Glossary

1.3.1 Acronyms

Acronym	Description
AOC	Attitude and Orbit Control
AOCS	Attitude and Orbit Control System
FDIR	Failure Detection, Isolation and Recovery
ES	Earth Sensor
GPS	Global Positioning System
LOA	Loss of Accuracy
PLI	Payload Instrument
RW	Reaction Wheel
SRD	Software Requirements Document
SS	Sun Sensor
STR	Star Tracker
SW	Software
THR	Thruster
WP	Work Package

1.3.2 Definition of terms

Term	Description
actuator	The actuators in the AOCS are the units RW and THR.
attitude	orientation with respect to a defined frame of reference
autonomous mode transition	mode transition due to nominal behavior without any separate request
branch	See the description of "unit".
coarse pointing	directing the line-of-sight with a specified coarse accuracy
data acquisition	sampling of signals and digitization of the samples
earth sensor	device that senses orientation with respect to Earth's horizon
fine pointing	directing the line-of-sight with a specified fine accuracy
mode	global mode of the AOCS SW
reaction wheel	device that aims a spacecraft in different directions without firing rockets or jets
sensor	The sensors in the AOCS are the units ES, GPS, SS and STR.
separation	separation from a launcher
star tracker	device that measures positions of stars
sun sensor	device that senses the direction to the Sun
thruster	propulsive device used for station keeping and attitude control
unit	abstract device, consisting of two identical concrete devices that are called the nominal branch and the redundant branch
unit reconfiguration	moving the responsibilities of a unit from the nominal branch to the redundant branch
validation	confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled

The rest of this document uses the above terms with the above meaning, without any systematic re-explanation.

1.4 Software overview

1.4.1 Managers

The AOCS SW is used to determine and control the attitude of the spacecraft while in orbit. Based on input from sensors, actuators are commanded to preserve or change the attitude and/or orbit of the spacecraft. The different SW functionalities are on responsibility of the four managers:

- AOCS Manager: responsible for data acquisition, AOC (Attitude and Orbit Control) algorithm execution and actuator commanding.

- FDIR Manager: responsible for failure detection, isolation and recovery.
- Mode Manager: responsible for mode transitions.
- Unit Manager: responsible for unit-level state transitions and unit reconfigurations.

1.4.2 Execution

The execution of the AOCS SW is sequential repetition of a cycle where the above-mentioned four managers are called in the above order.

1.4.3 Units

The units in the AOCS are

- Earth Sensor (ES),
- Global Positioning System (GPS),
- Payload Instrument (PLI),
- Reaction Wheel (RW),
- Star Tracker (STR),
- Sun Sensor (SS), and
- Thruster (THR).

The sensors in the AOCS are the units ES, GPS, SS and STR. The actuators in the AOCS are the units RW and THR. The unit PLI is a measurement unit but not a sensor.

1.5 References

[RD1] Pauli Väisänen and Kimmo Varpaaniemi. *DEPLOY Satellite (an Attitude and Orbit Control System) Specification, Version 15 without statement numbering*. http://deploy-eprints.ecs.soton.ac.uk/166/, January 2010.

[RD2] DEPLOY Project. *DEPLOY Deliverable D20 D3.1 – Report on Pilot Deployment in the Space Sector*. http://www.deploy-project.eu/pdf/D20-pilot-deployment-in-the-space-sector-final-version.pdf, January 2010.

1.6 Document overview

The Unit Manager, the AOCS Manager, the Mode Manager and the FDIR Manager are described in Sections 2, 3, 4 and 5, respectively. Terminological convenience motivates this presentation order that does not reflect the execution order expressed in Section 1.4.2.

2. Unit Manager

2.1 Nominal and redundant branches

Every unit is implemented as a pair of identical devices: the nominal branch and the redundant branch. For each unit at any time, one and only one branch is the selected branch at the time. Immediately after booting of the AOCS SW, only nominal branches are selected branches. A recovery procedure can cause a unit reconfiguration that moves the responsibilities of a unit from the nominal branch to the redundant branch. The redundant branch then becomes the selected branch. Rebooting of the AOCS SW is the only way to reselect a nominal branch.

2.2 States and state transitions in branches

Every branch in every unit has a software state, appropriacy of which is a joint responsibility of the Unit Manager, the Mode Manager and the FDIR Manager. For any branch of ES, RW, SS, STR or THR, Figure 1 displays all possible states and all possible state transitions. For any branch of GPS, Figure 2 displays all possible states and all possible state transitions. For any branch of PLI, Figure 3 displays all possible states and all possible state transitions. Immediately after booting of the AOCS SW, every branch in every unit is in the state Off.

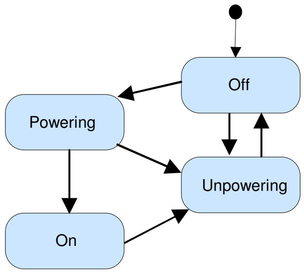

Figure 1 States and state transitions of a branch of ES, RW, SS, STR or THR

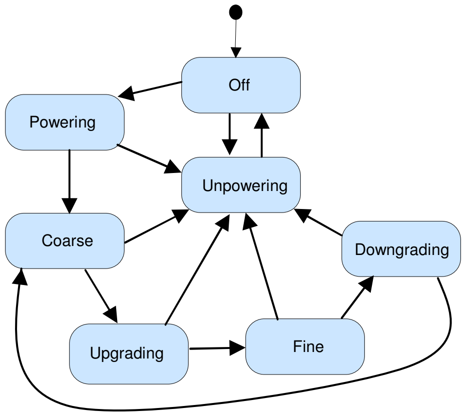

Figure 2 States and state transitions of a branch of GPS

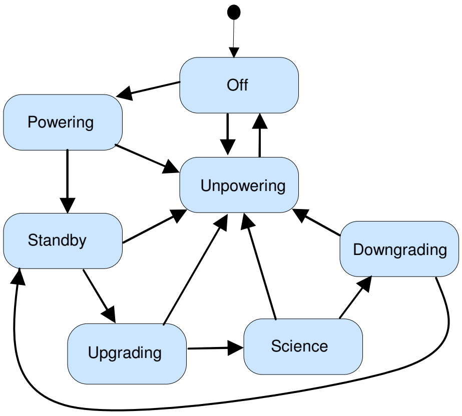

Figure 3 States and state transitions of a branch of PLI

The transitions from Off to Unpowering in the figures are needed because the software is not able to properly check the effect of power-off activities and is sometimes supposed to compensate the inability by redoing such activities.

2.3 Overriding a state transition

Any requested state transition to Unpowering overrides any ongoing state transition of the same branch of the same unit to On, Coarse, Fine, Standby or Science. There is no other way to override, cancel or abort a state transition of a branch of a unit.

2.4 State transition executions

Any state transition to Powering, Unpowering, Upgrading or Downgrading takes less than 1 AOCS cycle. Any state transition to Off takes at least 3 and at most 4 AOCS cycles. Any state transition to On, Coarse, Fine, Standby or Science has a success condition such that the transition gets completed at the first AOCS cycle where the condition is observed to hold. However, any state transition to On, Coarse, Fine, Standby or Science is overridden if the associated success condition is not observed to hold within a predefined number of AOCS cycles since the start of the transition.

2.5 State transitions in unit reconfigurations

Off and Unpowering are the only possible states for non-selected branches. If a reconfiguration of a unit starts during an ongoing mode transition or at the same AOCS cycle as a mode transition, the reconfiguration drives the redundant branch of the unit to the state that the selected branch of the unit should have at the completion of the mode transition (see Section 4.4). Otherwise any reconfiguration of a unit drives the redundant branch of the unit to the state that the nominal branch of the unit had immediately before the reconfiguration. In both cases, before any state transition of the redundant branch, the nominal branch is driven to the state Off and the redundant branch is marked as the selected branch. A branch is driven to a desired state by means of a sequence of possible state transitions.

2.6 Aborting a unit reconfiguration

Any ongoing unit reconfiguration can be aborted. Such an abort is done by overriding any associated overridable state transition (see Section 2.3) and by cancelling those associated activities that have not started yet. No reselection is involved: the selected branch immediately before the abort is the selected branch immediately after the abort.

2.7 Statuses vs. states

In addition to having a state, every branch in every unit also has a status that is either Locked or Unlocked. Immediately after booting of the AOCS SW, every branch in every unit has the status Unlocked. A branch of a unit can have the status Locked only when the unit has no ongoing reconfiguration and the state of the branch is neither Off nor Powering nor Unpowering. In a unit reconfiguration in the case of an ongoing mode transition, the final status of the redundant branch is chosen according to the needs of the target mode (see Section 4.4). In a unit reconfiguration in the case of no ongoing mode transition, the final status of the redundant branch is the status that the nominal branch had immediately before the reconfiguration.

2.8 Unit management in brief

In every AOCS cycle, the Unit Manager does the following things in the following order:

- Handling of ongoing unit reconfigurations. (This can involve generation of requests for state transitions.)
- Handling of ongoing and requested state transitions.

3. AOCS Manager

3.1 Algorithms and controllers

The AOC (Attitude and Orbit Control) algorithms are:

- Coarse Pointing Control, in order to direct the line-of-sight with a specified coarse accuracy.
- Fine Pointing Control, in order to direct the line-of-sight with a specified fine accuracy.

For conceptual convenience, the use of these algorithms is described by means of two controllers:

- Coarse Pointing Controller is responsible for the Coarse Pointing Control algorithm.
- Fine Pointing Controller is responsible for the Fine Pointing Control algorithm.

3.2 Phases and phase transitions for controllers

For a single controller, Figure 4 displays all possible phases and all possible phase transitions. Immediately after booting of the AOCS SW, every controller is in the phase Idle. An AOC algorithm is executed only when the corresponding controller is in the Running phase. At most one controller can be in a non-Idle phase at a time. The phase transitions are tightly related to the AOCS SW mode transitions and are therefore done only upon requests from the Mode Manager.

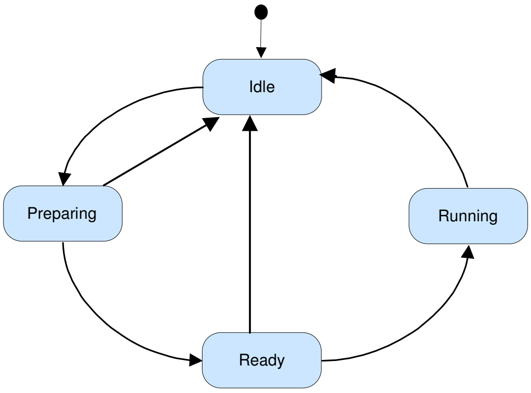

Figure 4: Phases and phase transitions of a controller

3.3 AOCS management in brief

In every AOCS cycle, the AOCS Manager does the following things in the following order:

- Data acquisition from those selected branches of ES, GPS, PLI, SS and STR that have the status Locked.
- Interpretation of measurements.
- Execution of any AOC algorithm for which the phase of the corresponding controller is Running.
- Commanding of those selected branches of RW and THR that have the status Locked.

4. Mode Manager

4.1 Overview

The Mode Manager is responsible for

- checking of mode transition preconditions,
- execution of mode transitions,
- management of controller phases (see Section 3.2), and
- (partially responsible for) management of units.

4.2 Modes and autonomous mode transitions

Figure 5 displays all possible modes and all possible autonomous mode transitions. Immediately after booting of the AOCS SW, the current mode is Off. All possible non-autonomous mode transitions are due to FDIR. Enumerative definitions of FDIR-based mode transitions are deferred to Section 5.

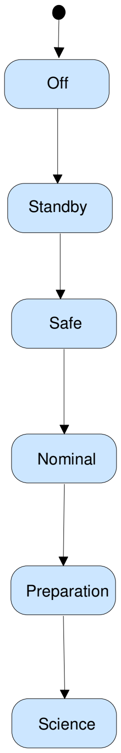

Figure 5: Modes and autonomous mode transitions

4.3 When to start an autonomous mode transition

An autonomous mode transition starts when and only when all of the following conditions hold:

- The current mode is the source mode of transition.

- There is no ongoing mode transition.
- There is no ongoing unit reconfiguration.
- Standby is not the target mode, or the Standby mode has not been entered since the latest booting of the AOCS SW.
- Safe is not the target mode, or separation of the spacecraft from the launcher has been successfully completed. (The time of the separation can be arbitrarily far in the past.)
- Nominal is not the target mode, or Running has been the phase of Coarse Pointing Controller for a predefined number of latest AOCS cycles.
- Preparation is not the target mode, or Running has been the phase of Fine Pointing Controller for a predefined number of latest AOCS cycles.
- Science is not the target mode, or Preparation has been the current mode for a predefined number of latest AOCS cycles.

4.4 Postconditions for autonomous and FDIR-based mode transitions

The following rules concern all mode transitions (autonomous and FDIR-based).

- When a mode transition gets completed: every selected branch in a state other than Off has the status Locked, and no unit reconfiguration or branch state transition or controller phase transition is going on. (Note that this rule does not justify any deviation from Section 2.7.)
- When a mode transition to Off or Standby gets completed: every branch in every unit is in the state Off, and every controller is in the phase Idle.
- When a mode transition to Safe gets completed: the selected branches of ES, RW and SS are in the state On, and otherwise every branch in every unit is in the state Off.
- When a mode transition to Safe gets completed: Coarse Pointing Controller is in the phase Running and Fine Pointing Controller is in the phase Idle.
- When a mode transition to Nominal, Preparation or Science gets completed: Coarse Pointing Controller is in the phase Idle and Fine Pointing Controller is in the phase Running.
- When a mode transition to Nominal gets completed: the selected branch of GPS is in the state Coarse, the selected branches of RW, STR and THR are in the state On, and otherwise every branch in every unit is in the state Off.
- When a mode transition to Preparation gets completed: the selected branch of GPS is in the state Fine, the selected branch of PLI is in the state Standby, the selected branches of RW, STR and THR is in the state On, and otherwise every branch in every unit is in the state Off.
- When a mode transition to Science gets completed: the selected branch of GPS is in the state Fine, the selected branch of PLI is in the state Science, the selected branches of RW, STR and THR are in the state On, and otherwise every branch in every unit is in the state Off.

4.5 Steps in autonomous and FDIR-based mode transitions

4.5.1 To the Off mode

Every mode transition to Off is FDIR-based and consists of the following steps (taken in the order of appearance):

- Any controller that is not in the phase Idle is reset to the phase Idle. Every ongoing unit reconfiguration is aborted. For each branch in each unit, the status is reset to Unlocked, and a request for a state transition to Unpowering is made if not already made as a part of the above-mentioned aborting of unit reconfigurations.
- For each branch in each unit, a request for a state transition to Off is made as soon as the branch is observed to be in the state Unpowering.
- Every branch in every unit is observed to be in the state Off. The Off mode becomes the current mode.

4.5.2 To the Standby mode

Every mode transition to Standby is autonomous and consists of the following steps (taken in the order of appearance, see also Sections 4.2 and 4.3):

- For each branch in each unit, a request for a state transition to Unpowering is made.
- For each branch in each unit, a request for a state transition to Off is made as soon as the branch is observed to be in the state Unpowering.
- Every branch in every unit is observed to be in the state Off. The Standby mode becomes the current mode. A process is started in order to check or follow the success of separation of the spacecraft from the launcher.

4.5.3 Autonomously to the Safe mode

Every autonomous mode transition to Safe consists of the following steps (taken in the order of appearance, see also Sections 4.2 and 4.3):

- The separation check/follow-up process mentioned in Section 4.5.2 is stopped. For each selected branch in ES, RW and SS, a request for a state transition to Powering is made.
- For each selected branch in ES, RW and SS, a request for a state transition to On is made as soon as the branch is observed to be in the state Powering.
- Every selected branch in ES, RW and SS is observed to be in the state On. (This also means that there is no ongoing unit reconfiguration, though reconfigurations in some or even all of these units may have taken place after the previous step.) The phase of Coarse Pointing Controller is set to Preparing.
- The phase of Coarse Pointing Controller is set to Ready after having been Preparing for a predefined number of AOCS cycles.

- The phase of Coarse Pointing Controller is set to Running. For each selected branch in ES, RW and SS, the status is set to Locked. (At this point no unit reconfiguration could even possibly be going on because there is nothing that could have caused such a reconfiguration.) The Safe mode becomes the current mode.

4.5.4 Returning to the Safe mode

Every FDIR-based mode transition to Safe consists of the following steps (taken in the order of appearance):

- Any controller that is not in the phase Idle is reset to the phase Idle. Every ongoing reconfiguration of a unit other than RW is aborted. For each branch in each unit other than RW, the status is reset to Unlocked, and a request for a state transition to Unpowering is made if not already made as a part of the above-mentioned aborting of unit reconfigurations. (The circumstances of the mode transitions being considered are such that at this point, the status of the selected branch of RW either is Locked or becomes Locked at completion of an ongoing reconfiguration.)
- For each branch in each unit other than RW, a request for a state transition to Off is made as soon as the branch is observed to be in the state Unpowering.
- Every branch in every unit other than RW is observed to be in the state Off. For each selected branch in ES and SS, a request for a state transition to Powering is made.
- For each selected branch in ES and SS, a request for a state transition to On is made as soon as the branch is observed to be in the state Powering.
- Every selected branch in ES and SS is observed to be in the state On. The selected branch of RW is observed to have the status Locked. (From these observations it follows that there is no ongoing unit reconfiguration.) The phase of Coarse Pointing Controller is set to Preparing.
- The phase of Coarse Pointing Controller is set to Ready after having been Preparing for a predefined number of AOCS cycles.
- The selected branch of RW is observed to have the status Locked. (This also means that there is no ongoing unit reconfiguration.) The phase of Coarse Pointing Controller is set to Running. For each selected branch in ES and SS, the status is set to Locked. The Safe mode becomes the current mode.

4.5.5 Autonomously to the Nominal mode

Every autonomous mode transition to Nominal consists of the following steps (taken in the order of appearance, see also Sections 4.2 and 4.3):

- Coarse Pointing Controller is reset to the phase Idle. For each branch in ES and SS, the status is reset to Unlocked, and a request for a state transition to Unpowering is made. For each selected branch in GPS, STR and THR, a request for a state transition to Powering is made.

- For each branch in ES and SS, a request for a state transition to Off is made as soon as the branch is observed to be in the state Unpowering. For each selected branch in STR and THR, a request for a state transition to On is made as soon as the branch is observed to be in the state Powering. For the selected branch of GPS, a request for a state transition to Coarse is made as soon as the branch is observed to be in the state Powering.
- Every branch in ES and SS is observed to be in the state Off. Every selected branch in STR and THR is observed to be in the state On. The selected branch of GPS is observed to be in the state Coarse. The selected branch of RW is observed to have the status Locked. (From these observations it follows that there is no ongoing unit reconfiguration.) The phase of Fine Pointing Controller is set to Preparing.
- The phase of Fine Pointing Controller is set to Ready after having been Preparing for a predefined number of AOCS cycles.
- The selected branch of RW is observed to have the status Locked. (This also means that there is no ongoing unit reconfiguration.) The phase of Fine Pointing Controller is set to Running. For each selected branch in GPS, STR and THR, the status is set to Locked. The Nominal mode becomes the current mode.

4.5.6 Returning to the Nominal mode

Every FDIR-based mode transition to Nominal consists of the following steps (taken in the order of appearance):

- Any ongoing reconfiguration of PLI is aborted. For each branch in PLI, the status is reset to Unlocked, and a request for a state transition to Unpowering is made if not already made as a part of the above-mentioned aborting of unit reconfigurations. (The circumstances of the mode transitions being considered are such that at this point, for each one of the units GPS, RW, STR and THR, the status of the selected branch of the unit either is Locked or becomes Locked at completion of an ongoing reconfiguration.)
- For each branch in PLI, a request for a state transition to Off is made as soon as the branch is observed to be in the state Unpowering.
- Every branch in PLI is observed to be in the state Off. Every selected branch in GPS, RW, STR and THR is observed to have the status Locked. (From these observations it follows that there is no ongoing unit reconfiguration.) For the selected branch of GPS, a request for a state transition to Downgrading is made if the current state of the branch is Fine. (Note that the current state of the selected branch of GPS is Coarse if the latest reconfiguration of GPS started in an AOCS cycle not earlier than the start cycle of the ongoing mode transition. The circumstances of the mode transitions being considered are such that at this point, the current state of the selected branch of GPS is either Coarse or Fine.)
- For the selected branch of GPS, a request for a state transition to Coarse is made as soon as the branch is observed to be in the state Downgrading. However, this step is skipped if no request for a state transition to Downgrading was made in the previous step.

- The selected branch of GPS is observed to be in the state Coarse. Every selected branch in GPS, RW, STR and THR is observed to have the status Locked. (From these observations it follows that there is no ongoing unit reconfiguration.) The Nominal mode becomes the current mode.

4.5.7 Autonomously to the Preparation mode

Every autonomous mode transition to Preparation consists of the following steps (taken in the order of appearance, see also Sections 4.2 and 4.3):

- For the selected branch of PLI, a request for a state transition to Powering is made. For the selected branch of GPS, a request for a state transition to Upgrading is made.
- For the selected branch of PLI, a request for a state transition to Standby is made as soon as the branch is observed to be in the state Powering. For the selected branch of GPS, a request for a state transition to Fine is made as soon as the branch is observed to be in the state Upgrading.
- The selected branch of PLI is observed to be in the state Standby. The selected branch of GPS is observed to be in the state Fine. Every selected branch in GPS, RW, STR and THR is observed to have the status Locked. (From these observations it follows that there is no ongoing unit reconfiguration.) The status of the selected branch of PLI is set to Locked. The Preparation mode becomes the current mode.

4.5.8 Returning to the Preparation mode

Every FDIR-based mode transition to Preparation consists of the following steps (taken in the order of appearance):

- Every selected branch in GPS, PLI, RW, STR and THR is observed to have the status Locked. (This also means that there is no ongoing unit reconfiguration.) For the selected branch of PLI, a request for a state transition to Downgrading is made if the current state of the branch is Science. (Note that the current state of the selected branch of PLI is Standby if the latest reconfiguration of PLI started in an AOCS cycle not earlier than the start cycle of the ongoing mode transition. The circumstances of the mode transitions being considered are such that at this point, the current state of the selected branch of PLI is either Standby or Science.)
- For the selected branch of PLI, a request for a state transition to Standby is made as soon as the branch is observed to be in the state Downgrading. However, this step is skipped if no request for a state transition to Downgrading was made in the previous step.
- The selected branch of PLI is observed to be in the state Standby. Every selected branch in GPS, PLI, RW, STR and THR is observed to have the status Locked. (From these observations it follows that there is no ongoing unit reconfiguration.) The Preparation mode becomes the current mode.

4.5.9 To the Science mode

Every mode transition to Science is autonomous and consists of the following steps (taken in the order of appearance, see also Sections 4.2 and 4.3):

- For the selected branch of PLI, a request for a state transition to Upgrading is made.
- For the selected branch of PLI, a request for a state transition to Science is made as soon as the branch is observed to be in the state Upgrading.
- The selected branch of PLI is observed to be in the state Science. Every selected branch in GPS, PLI, RW, STR and THR is observed to have the status Locked. (From these observations it follows that there is no ongoing unit reconfiguration.) The Science mode becomes the current mode.

4.5.10 Overriding a mode transition

Any requested FDIR-based mode transition overrides any ongoing mode transition. The execution of the overriding transition starts from the point where the execution of the overridden transition happens to be at the time of overriding. Any needed cleanup activity is included in the steps of the overriding transition. (Note that an overriding transition can itself get overridden and that work towards unreached goals can form even a major part of a mode change activity history.)

5. FDIR Manager

5.1 FDIR management in brief

In every AOCS cycle, the FDIR Manager does the following things in the following order:

- Handling of branch state transition errors that have been reported internally after the previous execution of the FDIR Manager.
- Handling of attitude errors that have been reported internally after the previous execution of the FDIR Manager. These errors are ignored if and only if: there is an ongoing mode transition, or at least one branch state transition error has been reported internally after the previous execution of the FDIR Manager.
- Handling of unit usability errors that have been reported internally after the previous execution of the FDIR Manager. These errors are ignored if and only if: there is an ongoing mode transition, or at least one branch state transition error or attitude error has been reported internally after the previous execution of the FDIR Manager.

Whenever any of the four managers of the AOCS SW observes an error that belongs to some of the above-mentioned three classes, the manager is in principle expected to report the error internally, together with an indicator of which of the three classes is concerned. However, there is no need to report the same error twice for a single execution of the FDIR Manager. Consequently, it is possible to design the AOCS SW in such a way that only the AOCS Manager and the Unit Manager ever need to report errors. Each one of the three error classes is considered in detail in the following subsections.

There is no “mode transition error” in the sense the term is used in [RD1] and [RD2]. Any such error would be due to a timeout in a mode transition, whereas such a timeout would always be due to timeouts in branch state transitions. Handling of branch state transition errors suffices for ensuring a decent maximum duration for every mode transition.

5.2 Branch state transition errors

A branch state transition error means that in some branch in some unit, a state transition to On, Coarse, Fine, Standby or Science gets overridden due to the timeout-based overriding rule expressed in Section 2.4. From Section 2.5 it follows that at every overridden state transition is a state transition of a selected branch at the time of overriding. From the AOCS SW execution principle expressed in Section 1.4.2 and from the error handling principles expressed in Section 5.1 it then follows that in observation, reporting and handling of branch state transition errors, it suffices to pay attention to selected branches only.

The FDIR policy for branch state transition errors is to use reconfigurations as much as possible and, if reconfigurations alone do not suffice, go to the most advanced non-Standby mode for which all branches of the no longer reconfigurable problematic units have the state Off when the mode becomes the current mode (see Section 4.4). Strictly speaking, the policy is expressed by the rules below. In all these rules, the word “error” is limited to concern errors that have been reported internally after the previous execution of the FDIR Manager.

- A branch state transition error on the redundant branch of ES, RW or SS causes a mode transition to Off.
- A branch state transition error on the redundant branch of GPS, STR or THR causes a mode transition to Safe if there is no branch state transition error on the redundant branches of ES, RW and SS.
- A branch state transition error on the redundant branch of PLI causes a mode transition to Nominal if there is no branch state transition error on the redundant branches of ES, GPS, RW, SS, STR and THR.
- A branch state transition error on the nominal branch of ES, RW or SS causes a reconfiguration of the unit if there is no branch state transition error on the redundant branches of ES, RW and SS.
- A branch state transition error on the nominal branch of GPS, PLI, STR or THR causes a reconfiguration of the unit if there is no branch state transition error on the redundant branches of ES, GPS, RW, SS, STR and THR.

Figure 6 displays every possible mode transition that is induced by the above rules. The self-loops in the figure are due to overriding of autonomous mode transitions.

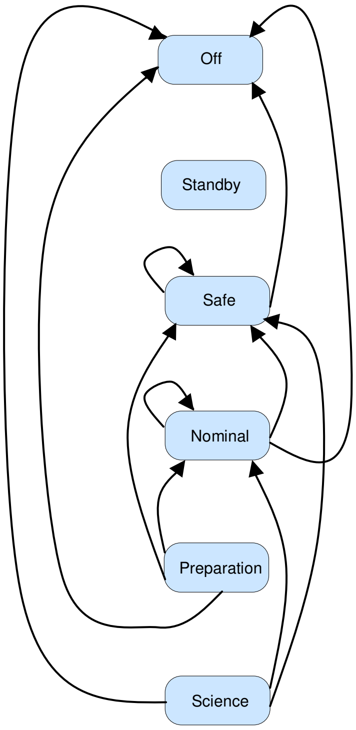

Figure 6: Mode transitions for recovery from branch state transition errors

5.3 Attitude errors

An attitude error means an error in execution of an AOC algorithm. From Section 3.3 it follows that such an error can occur only when one of the two controllers (Coarse Pointing Controller and Fine Pointing Controller) is in the phase Running.

The FDIR policy for non-ignored (see Section 5.1.) attitude errors is to go to the most advanced non-Standby mode that is less advanced than the current mode. Strictly speaking, the policy is expressed by the rules below. In all these rules, the word “error” is limited to concern errors that have been reported internally after the previous execution of the FDIR Manager.

- A non-ignored attitude error causes a mode transition to Off if the current mode is Safe.
- A non-ignored attitude error causes a mode transition to Safe if the current mode is Nominal.
- A non-ignored attitude error causes a mode transition to Nominal if the current mode is Preparation.
- A non-ignored attitude error causes a mode transition to Preparation if the current mode is Science.

Figure 7 displays every possible mode transition that is induced by the above rules.

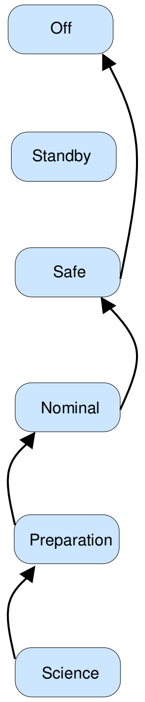

Figure 7: Mode transitions for recovery from attitude errors

5.4 Unit usability errors

A unit usability error means an error encountered by the AOCS Manager in data acquisition from ES, GPS, PLI, SS or STR or in interpretation of measurements from those units or in commanding of RW or

THR. From Section 2.7 and 3.3 it follows that any branch on which such an error occurs is a selected branch at the time of occurrence. From the AOCS SW execution principle expressed in Section 1.4.2 and from the error handling principles expressed in Section 5.1 it then follows that in observation, reporting and handling of unit usability errors, it suffices to pay attention to selected branches only.

In the considerations below, a unit usability error on a branch of PLI is is said to be standable if and only if: the error is limited to measurement accuracy, the current mode is Science, the current state of the branch is Science, and at most a predefined number of non-ignored unit usability errors on the branch have been reported internally since the latest exit from the Off state of the branch.

The FDIR policy for non-ignored (see Section 5.1.) unit usability errors is like the FDIR policy for branch state transition errors (see Section 5.2), except in the case of errors on PLI. Strictly speaking, the policy is expressed by the rules below. In all these rules, the word “error” is limited to concern errors that have been reported internally after the previous execution of the FDIR Manager.

- A non-ignored unit usability error on the redundant branch of ES, RW or SS causes a mode transition to Off.
- A non-ignored unit usability error on the redundant branch of GPS, STR or THR causes a mode transition to Safe if there is no unit usability error on the redundant branches of ES, RW and SS.
- A non-ignored unit usability error on the nominal branch of ES, RW or SS causes a reconfiguration of the unit if there is no unit usability error on the redundant branches of ES, RW and SS.
- A non-ignored unit usability error on the nominal branch of GPS, STR or THR causes a reconfiguration of the unit if there is no unit usability error on the redundant branches of ES, GPS, RW, SS, STR and THR.
- A non-standable non-ignored unit usability error on the redundant branch of PLI causes a mode transition to Nominal if there is no unit usability error on the redundant branches of ES, GPS, RW, SS, STR and THR.
- A standable non-ignored unit usability error on any branch of PLI causes a mode transition to Preparation if all unit usability errors on the branches of PLI are standable and there is no unit usability error on the redundant branches of ES, GPS, RW, SS, STR and THR.
- A non-standable non-ignored unit usability error on the nominal branch of PLI causes a reconfiguration of PLI if there is no unit usability error on the redundant branches of ES, GPS, RW, SS, STR and THR.

Figure 8 displays every possible mode transition that is induced by the above rules.

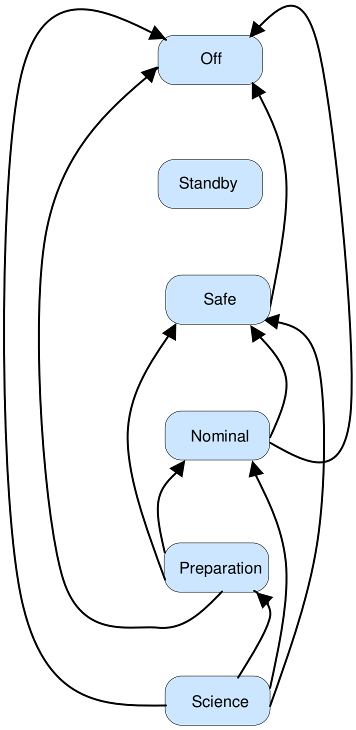

Figure 8: Mode transitions for recovery from unit usability errors

(End of the document)