TITLE:

DEPLOY Work Package 3

Software Requirements Document for a Distributed System for Attitude and Orbit Control for a Single Spacecraft

	FUNCTION	NAME	DATE
PREPARED BY	Verification Engineer	Kimmo Varpaaniemi	04.10.2011

REF: DEP-RP-SSF-R-006
ISSUE: 1.3
DATE: 04.10.2011

Document Status Sheet

Issue	Date	Modified Items / Reason for Change
1.0	31.03.2011	Initial issue of the document.
1.1	11.04.2011	The set of possible ways of overriding in Section 2.3 has been extended in order to match the intentions.
		The mode synchronization protocol in Section 4.2 has been revised because the original version can reach a deadlock or a livelock.
1.2	26.06.11	Section 2.5 has been revised in order to match the intentions.
		The document has been visually reformatted using OpenOffice.org Writer.
1.3	04.10.2011	The mode synchronization protocol in Section 4.2 has been revised again in order to match the intentions.

Table of Contents

List of Figures

1. Introduction

1.1 Purpose and scope

This Software Requirements Document (SRD) expresses the functional requirements of the Software (SW) of the DEPLOY Work Package 3 (WP3) Distributed System for Attitude and Orbit Control for a Single Spacecraft (DSAOCSS). This system is in many ways similar to the centralized Attitude and Orbit Control System (AOCS) considered by [RD1]. However, there are differences up to the extent that the systems should not be assumed to have the same baseline for requirements. The actual Attitude and Orbit Control (AOC) in DSAOCSS is centralized in conventional control-theoretical sense, so the term “distributed AOCS” is too ambiguous to be used in this context.

1.2 Glossary

1.2.1 Acronyms

Acronym	Description	Acronym	Description
AOC	Attitude and Orbit Control	AOCS	Attitude and Orbit Control System
DHSW	Data Handling Software	DSAOCSS	Distributed System for Attitude and Orbit Control for a Single Spacecraft
e.g.	exempli gratia	ES	Earth Sensor
etc.	et cetera	FDIR	Failure Detection, Isolation and Recovery
GPS	Global Positioning System	i.e.	id est
OBSW	On-Board Software	PLI	Payload Instrument
RW	Reaction Wheel	SRD	Software Requirements Document
SS	Sun Sensor	STR	Star Tracker
SW	Software	THR	Thruster
WP	Work Package	w.r.t.	with respect to

1.2.2 Definition of terms

Term	Description
actuator	The actuators in DSAOCSS are the units RW and THR.
attitude	orientation with respect to a defined frame of reference
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 DSAOCSS SW

Term	Description
reaction wheel	device that aims a spacecraft in different directions without firing rockets or jets
sensor	The sensors in DSAOCSS 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

1.3 Software overview

1.3.1 Units

The units in DSAOCSS are Earth Sensor (ES), Global Positioning System (GPS), Payload Instrument (PLI), Reaction Wheel (RW), Star Tracker (STR), Sun Sensor (SS) and Thruster (THR). ES, GPS, SS and STR are sensors, whereas RW and THR are actuators. PLI is a measurement unit but not a sensor.

1.3.2 Distributed software context

DSAOCSS SW is a part of On-Board Software (OBSW) that is distributed over several processors using a network and a protocol such that on the abstraction level of the source code, every two of these processors directly communicate with each other in both directions. DSAOCSS activities (if any) in a processor are executed by means of periodic calls by the processor's Data Handling Software (DHSW) that is not a part of DSAOCSS. Every such call is synchronous in the sense that the execution of the calling thread is blocked until the end of the called activity.

FDIR w.r.t. processors and inter-processor communications is beyond the scope of DSAOCSS and is arranged in such a way that DSAOCSS does not have to react. For example, every processor with DSAOCSS activities is shut down whenever one of such processors is shut down. (The arrangements needed for that purpose may be complicated but are beyond the scope of DSAOCSS anyway.) Then the same set of processors or some corresponding set of processors is booted.

1.3.3 Managers

DSAOCSS SW consists of one AOC manager and seven unit managers such that every manager is a routine called by DHSW. Respectively, the term "execution of a manager" means a single execution of such a routine. Every processor with DSAOCSS activities is dedicated to a fixed manager, and no two processors are dedicated to the same manager. The managers and their responsibilities of the managers are briefly listed below.

- AOC manager: responsible for

  - mode synchronization (a joint responsibility of all managers),
  - data acquisition,
  - attitude and orbit determination,
  - actuator commanding, and
  - detection and reporting of errors in data acquisition, attitude and orbit determination and actuator commanding.
- RW manager: responsible for
  - mode synchronization,
  - execution of commands from the AOC Manager,
  - decisions on branch state transitions and reconfiguration of RW,
  - performing of branch state transitions and reconfiguration of RW, and
  - detection and reporting of errors in branch state transitions of RW.
- THR manager: responsible for
  - mode synchronization,
  - execution of commands from the AOC Manager,
  - decisions on branch state transitions and reconfiguration of THR,
  - performing of branch state transitions and reconfiguration of THR, and
  - detection and reporting of errors in branch state transitions of THR.
- ES manager: responsible for
  - mode synchronization,
  - providing data to the AOC Manager,
  - decisions on branch state transitions and reconfiguration of ES,
  - performing of branch state transitions and reconfiguration of ES, and
  - detection and reporting of errors in branch state transitions of ES.
- GPS manager: responsible for
  - mode synchronization,
  - providing data to the AOC Manager,
  - decisions on branch state transitions and reconfiguration of GPS,
  - performing of branch state transitions and reconfiguration of GPS, and
  - detection and reporting of errors in branch state transitions of GPS.
- PLI manager: responsible for

  - mode synchronization,
  - providing data to the AOC Manager,
  - decisions on branch state transitions and reconfiguration of PLI,
  - performing of branch state transitions and reconfiguration of PLI, and
  - detection and reporting of errors in branch state transitions of PLI.
- SS manager: responsible for
  - mode synchronization,
  - providing data to the AOC Manager,
  - decisions on branch state transitions and reconfiguration of SS,
  - performing of branch state transitions and reconfiguration of SS, and
  - detection and reporting of errors in branch state transitions of SS.
- STR manager: responsible for
  - mode synchronization,
  - providing data to the AOC Manager,
  - decisions on branch state transitions and reconfiguration of STR,
  - performing of branch state transitions and reconfiguration of STR, and
  - detection and reporting of errors in branch state transitions of STR.

1.3.4 Inter-manager communications

The managers in DSAOCSS communicate with each other by means of permanent input and output variables. The input variables of a manager are supposed to cover the information that the manager needs from other managers. Respectively, the output variables of a manager are supposed to cover the information that other managers need from the manager. Every input or output variable of a manager is permanently dedicated to one of the other managers.

Whenever an input variable x of a manager A is dedicated to a manager B, there is a unique output variable y of B such that y is dedicated to A, and the value of x is always an as recent value of y as reasonably practicable. Respectively, whenever an output variable y of a manager B is dedicated to a manager A, there is a unique input variable x of A such that x is dedicated to B, and the value of x is always an as recent value of y as reasonably practicable.

Note that the value history of an input variable does not have to perfectly reproduce the value history of the corresponding output variable. However, if the value of an output variable remains unchanged for a predefined time, the value should get copied to the corresponding input variable within a predefined time.

The data transfers needed for ensuring the above properties are done outside DSAOCSS. Immediately after the end of a finished manager execution, the DHSW that initiated the execution initiates transfers of mappings that express the current values of the output variables of the manager. Each mapping is scoped according to the needs of the receiver. Immediately before a call to a manager, the calling DHSW goes through received new mappings and updates the input variables of the manager accordingly.

The non-DSAOCSS FDIR mentioned in Section 1.3.2 is supposed to ensure that corrupted mappings are not used for updating of input variables, and that for each output variable in the system, the value of the variable gets frequently enough copied to the corresponding input variable. So, inter-manager communications as such do not necessitate any FDIR in DSAOCSS.

1.4 References

[RD1] Kimmo Varpaaniemi. *DEPLOY WP3 Attitude and Orbit Control System Software Requirements Document*. DEP-RP-SSF-R-005, Issue 1.0, http://deploy-eprints.ecs.soton.ac.uk/266/, December 2010.

2. Some aspects of unit management

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 a processor that is dedicated to a unit manager, the nominal branch of the unit is the selected branch of the unit. A recovery procedure can cause a reconfiguration that moves the responsibilities of the unit from the nominal branch to the redundant branch. The redundant branch then becomes the selected branch. As long as the processor is not shut down, there is no way to reselect the nominal branch. Only the manager of a unit can reconfigure the unit or make decisions on reconfiguration of the unit.

2.2 States and state transitions in branches

Every branch in every unit has a software state. 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 a processor that is dedicated to a unit manager, every branch in the unit is in the state Off.

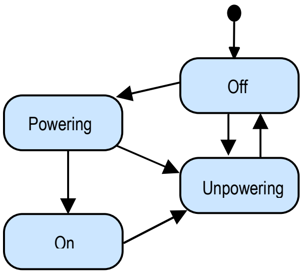

Figure 1 States and state transitions of a branch of ES, RW, SS, STR or THR

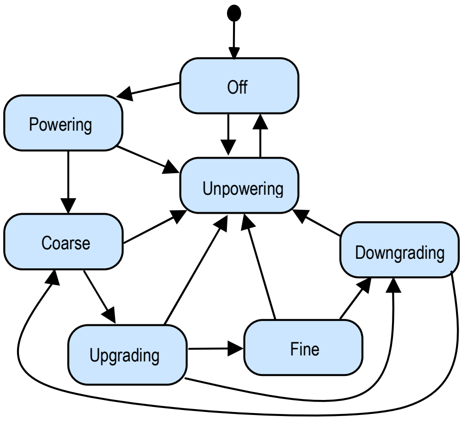

Figure 2 States and state transitions of a branch of GPS

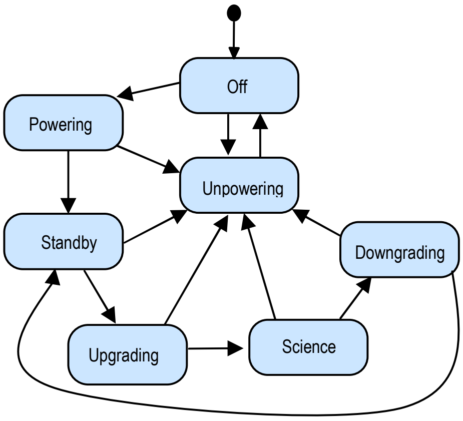

Figure 3 States and state transitions of a branch of PLI

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.

Only the manager of a unit can perform state transitions in branches of the unit or make decisions on such transitions.

2.3 Overriding a state transition

Initiation of a state transition to Unpowering overrides any ongoing state transition of the same branch of the same unit to On, Coarse, Fine, Standby or Science. For GPS, initiation of a state transition from Upgrading to Downgrading overrides any ongoing state transition of the same branch from Upgrading to Fine. There is no other way to override, cancel or abort a state transition of a branch of a unit.

2.4 Ongoing state transitions; state transition errors

Whenever a unit manager initiates a state transition to Powering, Unpowering, Upgrading or Downgrading, the transition gets completed during the same execution of the manager. Whenever a unit manager during its n^{th} execution initiates a state transition to Off, the transition gets completed during the $(n + 3)^{th}$ or $(n + 4)^{th}$ execution of the manager. Any state transition to On, Coarse, Fine, Standby or Science has a success condition such that the transition gets completed during the first execution where the manager of the unit observes the condition to hold. However, any state transition to On, Coarse, Fine, Standby or Science fails and causes a state transition error if the manager of the unit does not observe the associated success condition to hold within a predefined number of executions of the manager. There is no other way to cause a state transition error.

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 is due to an error in a state transition of the nominal branch of the unit, the reconfiguration drives the redundant branch of the unit to the target state of the transition. Any other 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. 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 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 a processor that is dedicated to a unit manager, every branch in the unit has the status Unlocked. A branch of a unit can have the status Locked only when the unit has no ongoing unit reconfiguration and the state of the branch is neither Off nor Powering nor Unpowering. In a unit reconfiguration, the final status of the redundant branch is the status that the nominal branch had immediately before the reconfiguration. Only the manager of a unit can update statuses in branches of the unit or make decisions on such updates.

3. Some aspects of AOC management

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.

Only the AOC manager can execute AOC algorithms. 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 a processor that is dedicated to the AOC manager, 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. Only the AOC manager can perform controller phase transitions or make decisions on such transitions.

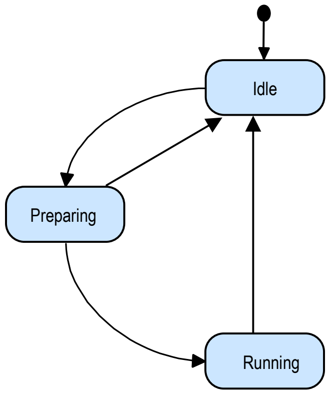

Figure 4: Phases and phase transitions of a controller

3.3 Data acquisition and actuator commanding

The AOC manager acquires data only from selected locked branches of ES, GPS, PLI SS and STR. The AOC manager commands only selected locked branches of RW and THR. A branch is locked when and only when the status of the branch is Locked.

3.4 Attitude/orbit errors

Any attitude/orbit error is initially observed by the AOC manager during an execution of an AOC algorithm. Any observation of an attitude/orbit error by any other manager is due to information received from the AOC manager.

3.5 Insufficient usability of a branch

Usability of a branch of a unit means usability for the AOC manager in data acquisition or actuator commanding. Therefore, any insufficient usability of a branch of a unit is initially observed by the AOC manager when the branch is the selected branch of the unit and has the status Locked. Any observation of insufficient branch usability by any other manager is due to information received from the AOC manager.

4. Distributed mode management

4.1 Modes and mode transitions

Modes and mode transitions in DSAOCSS are conceptually global, but every manager has its own understanding of the current mode and of the current stage of an ongoing mode transition if any.

The initial mode is Off. The other possible modes are UpToStandby, Standby, UpToSafe1, UpToSafe2, Safe, UpToNominal1, UpToNominal2, Nominal, UpToPreparation, Preparation, UpToScience, Science, DownToOff, DownToSafe1, DownToSafe2, DownToSafe3, DownToNominal1, DownToNominal2, and DownToPreparation.

The possible mode transitions and their "inherent" preconditions and actions are as follows. For any transition with several cells in the precondition column, the overall condition formed by the cells is the disjunction over the conditions in the cells. Moreover, the cells in the precondition column are such that conditions in separate cells for the same source mode are always mutually exclusive. Actions inside a cell in the actions column do not have to take place in the expressed order.

Source mode	**Target mode**	**Precondition except what is due to mode synchronization**	**Actions except what is due to mode synchronization**
Off	UpToStandby	The Standby mode has not been entered since the latest system-wide booting of DSAOCSS.	For each branch in each unit, the state is set to Unpowering, and a state transition to Off is initiated.
UpToStandby	Standby	For each branch in each unit, the state is Off.	No action.
Standby	UpToSafe1	Separation of the spacecraft from the launcher has been successfully completed.	For each selected branch in ES, RW and SS, the state is set to Powering, and a state transition to On is initiated.
UpToSafe1	UpToSafe2	For each selected branch in ES, RW and SS, the state is On. No ongoing unit reconfiguration. No state transition error in redundant branches of ES, RW and SS.	The phase of Coarse Pointing Controller is set to Preparing. For each selected branch in ES, RW and SS, the status is set to Locked.
	DownToOff	A state transition error in some of the redundant branches in ES, RW and SS.	For each unit, any ongoing unit reconfiguration is aborted. For each branch in each unit, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
UpToSafe2	Safe	A predefined time has passed from the latest moment when Preparing was not the phase of Coarse Pointing Controller.	The phase of Coarse Pointing Controller is set to Running.

Source mode	Target mode	Precondition except what is due to mode synchronization	Actions except what is due to mode synchronization
Safe	UpToNominal1	A predefined time has passed from the latest moment when Running was not the phase of Fine Pointing Controller. No ongoing unit reconfiguration. No error.	The phase of Coarse Pointing Controller is set to Idle. For each branch in ES and SS, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is inititiated. For the selected branch of GPS, the state is set to Powering, and a state transition to Coarse is initiated. For each selected branch in STR and THR, the state is set to Powering, and a state transition to On is initiated.
	DownToOff	A state transition error in some of the redundant branches in ES, RW and SS.	The phase of Coarse Pointing Controller is set to Idle. For each unit, any ongoing unit reconfiguration is aborted. For each branch in each unit, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
		An attitude/orbit error. No branch state transition error.	
		Insufficient usability of a selected redundant branch of ES, RW or SS. No branch state transition error. No attitude/orbit error.	
UpToNominal1	UpToNominal2	For each branch in ES and SS, the state is Off. For the selected branch of GPS, the state is Coarse. For each selected branch in STR and THR, the state is On. No ongoing unit reconfiguration. No state transition error in redundant branches of GPS, RW, STR and THR.	For each selected branch in GPS, STR and THR, the status is set to Locked. The phase of Fine Pointing Controller is set to Preparing.
	DownToOff	A state transition error in the redundant branch of RW.	For each unit, any ongoing unit reconfiguration is aborted. For each branch in each unit, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
	DownToSafe1	A state transition error in some of the redundant branches in GPS, STR and THR. No state transition error in the redundant branch of RW.	For each unit other than RW, any ongoing unit reconfiguration is aborted. For each branch in each unit other than RW, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
UpToNominal2	Nominal	A predefined time has passed from the latest moment when Preparing was not the phase of Fine Pointing Controller.	The phase of Fine Pointing Controller is set to Running.

Source mode	Target mode	Precondition except what is due to mode synchronization	Actions except what is due to mode synchronization
Nominal	UpToPreparation	A predefined time has passed from the latest moment when Running was not the phase of Fine Pointing Controller. No ongoing unit reconfiguration. No error.	For the selected branch of GPS, the state is set to Upgrading, and a state transition to Fine is initiated. For the selected branch of PLI, the state is set to Powering, and a state transition to Standby is initiated.
	DownToOff	A state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit, any ongoing unit reconfiguration is aborted. For each branch in each unit, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
		Insufficient usability of a selected redundant branch of RW. No branch state transition error. No attitude/orbit error.	
	DownToSafe1	A state transition error in some of the redundant branches in GPS, STR and THR. No state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit other than RW, any ongoing unit reconfiguration is aborted. For each branch in each unit other than RW, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
		An attitude/orbit error. No branch state transition error.	
		Insufficient usability of a selected redundant branch of GPS, STR or THR. No branch state transition error. No attitude/orbit error. No problem on the redundant branch of RW.	
UpToPreparation	Preparation	For the selected branch of GPS, the state is Fine. For the selected branch of PLI, the state is Standby. No ongoing unit reconfiguration. No state transition error in redundant branches of GPS, PLI, RW, STR and THR.	For the selected branch of PLI, the status is set to Locked.
	DownToOff	A state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit, any ongoing unit reconfiguration is aborted. For each branch in each unit, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
	DownToSafe1	A state transition error in some of the redundant branches in GPS, STR and THR. No state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit other than RW, any ongoing unit reconfiguration is aborted. For each branch in each unit other than RW, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
	DownToNominal1	A state transition error in the redundant branch of PLI. No state transition error in redundant branches of GPS, RW, STR and THR.	Any ongoing unit reconfiguration in PLI is aborted. For each branch in PLI, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.

Source mode	Target mode	Precondition except what is due to mode synchronization	Actions except what is due to mode synchronization
Preparation	UpToScience	A predefined time has passed from the latest moment when Preparation was not the current mode. No ongoing unit reconfiguration. No error.	For the selected branch of PLI, the state is set to Upgrading, and a state transition to Science is initiated.
	DownToOff	A state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit, any ongoing unit reconfiguration is aborted. For each branch in each unit, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
		Insufficient usability of a selected redundant branch of RW. No branch state transition error. No attitude/orbit error.	
	DownToSafe1	A state transition error in some of the redundant branches in GPS, STR and THR. No state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit other than RW, any ongoing unit reconfiguration is aborted. For each branch in each unit other than RW, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
		Insufficient usability of a selected redundant branch of GPS, STR or THR. No branch state transition error. No attitude/orbit error. No problem on the redundant branch of RW.	
	DownToNominal1	A state transition error in the redundant branch of PLI. No state transition error in redundant branches of GPS, RW, STR and THR.	Any ongoing unit reconfiguration in PLI is aborted. For each branch in PLI, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
		An attitude/orbit error. No branch state transition error.	
		Insufficient usability of a selected redundant branch of PLI. No branch state transition error. No attitude/orbit error. No problem in redundant branches of GPS, RW, STR and THR.	
UpToScience	Science	For the selected branch of PLI, the state is Science. No ongoing unit reconfiguration. No state transition error in redundant branches of GPS, PLI, RW, STR and THR.	No action.
	DownToOff	A state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit, any ongoing unit reconfiguration is aborted. For each branch in each unit, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
	DownToSafe1	A state transition error in some of the redundant branches in GPS, STR and THR. No state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit other than RW, any ongoing unit reconfiguration is aborted. For each branch in each unit other than RW, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
	DownToNominal1	A state transition error in the redundant branch of PLI. No state transition error in redundant branches of GPS, RW, STR and THR.	Any ongoing unit reconfiguration in PLI is aborted. For each branch in PLI, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.

Source mode	Target mode	Precondition except what is due to mode synchronization	Actions except what is due to mode synchronization
Science	DownToOff	A state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit, any ongoing unit reconfiguration is aborted. For each branch in each unit, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
		Insufficient usability of a selected redundant branch of RW. No branch state transition error. No attitude/orbit error.	
	DownToSafe1	A state transition error in some of the redundant branches in GPS, STR and THR. No state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit other than RW, any ongoing unit reconfiguration is aborted. For each branch in each unit other than RW, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
		Insufficient usability of a selected redundant branch of GPS, STR or THR. No branch state transition error. No attitude/orbit error. No problem on the redundant branch of RW.	
	DownToNominal1	A state transition error in the redundant branch of PLI. No state transition error in redundant branches of GPS, RW, STR and THR.	Any ongoing unit reconfiguration in PLI is aborted. For each branch in PLI, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
		Insufficient usability of a selected redundant branch of PLI. No branch state transition error. No attitude/orbit error. No problem in redundant branches of GPS, RW, STR and THR.	
	DownToPreparation	An attitude/orbit error. No branch state transition error. No ongoing unit reconfiguration.	For the selected branch of PLI, the state is set to Downgrading, and a state transition to Standby is initiated.
DownToOff	Off	For each branch in each unit, the state is Off.	No action.
DownToSafe1	DownToSafe2	For each branch in each unit other than RW, the state is Off.	For each selected branch in ES and SS, the state is set to Powering, and a state transition to On is initiated.
	DownToOff	A state transition error in the redundant branch of RW.	For each unit, any ongoing unit reconfiguration is aborted. For each branch in each unit, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
DownToSafe2	DownToSafe3	For each selected branch in ES and SS, the state is On. No ongoing unit reconfiguration. No state transition error in redundant branches of ES, RW and SS.	The phase of Coarse Pointing Controller is set to Preparing. For each selected branch in ES and SS, the status is set to Locked.
	DownToOff	A state transition error in some of the redundant branches in ES, RW and SS.	For each unit, any ongoing unit reconfiguration is aborted. For each branch in each unit, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.

Source mode	Target mode	Precondition except what is due to mode synchronization	Actions except what is due to mode synchronization
DownToSafe3	Safe	A predefined time has passed from the latest moment when Preparing was not the phase of Coarse Pointing Controller.	The phase of Coarse Pointing Controller is set to Running.
DownToNominal1	DownToNominal2	For each branch in PLI, the state is Off. For the selected branch of GPS, the state is not Coarse. No ongoing unit reconfiguration in GPS. No state transition error in redundant branches of GPS, RW, STR and THR.	For the selected branch of GPS, the state is set to Downgrading, and a state transition to Coarse is initiated.
	Nominal	For each branch in PLI, the state is Off. For the selected branch of GPS, the state is Coarse. No ongoing unit reconfiguration in GPS. No state transition error in redundant branches of GPS, RW, STR and THR.	No action.
	DownToOff	A state transition error in the redundant branch of RW.	Every controller is in the phase Idle. No ongoing unit reconfiguration. In every unit, every branch has the status Unlocked and is in the state Unpowering with an initiated state transition to Off..
	DownToSafe1	A state transition error in some of the redundant branches of GPS, STR and THR. No state transition error in the redundant branch of RW.	Every controller is in the phase Idle. No ongoing unit reconfiguration in units other than RW. In every unit other than RW, every branch has the status Unlocked and is in the state Unpowering with an initiated state transition to Off.
DownToNominal2	Nominal	For the selected branch of GPS, the state is Coarse. No ongoing unit reconfiguration. No state transition error in redundant branches of GPS, RW, STR and THR.	No action.
	DownToOff	A state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit, any ongoing unit reconfiguration is aborted. For each branch in each unit, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
	DownToSafe1	A state transition error in some of the redundant branches of GPS, STR and THR. No state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit other than RW, any ongoing unit reconfiguration is aborted. For each branch in each unit other than RW, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.

Source mode	Target mode	Precondition except what is due to mode synchronization	Actions except what is due to mode synchronization
DownToPreparation	Preparation	For the selected branch of PLI, the state is Standby. No ongoing unit reconfiguration. No state transition error in redundant branches of GPS, PLI, RW, STR and THR.	No action.
	DownToOff	A state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit, any ongoing unit reconfiguration is aborted. For each branch in each unit, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
	DownToSafe1	A state transition error in some of the redundant branches of GPS, STR and THR. No state transition error in the redundant branch of RW.	The phase of Fine Pointing Controller is set to Idle. For each unit other than RW, any ongoing unit reconfiguration is aborted. For each branch in each unit other than RW, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.
	DownToNominal1	A state transition error in the redundant branch of PLI. No state transition error in redundant branches of GPS, RW, STR and THR.	Any ongoing unit reconfiguration in PLI is aborted. For each branch in PLI, the status is set to Unlocked, the state is set to Unpowering, and a state transition to Off is initiated.

4.2 Mode synchronization

Using the communication mechanism that is described in Section 1.3.4, the managers inform each other e.g. about the current mode, about whatever is needed in evaluation of the preconditions that are expressed in Section 4.1, and about suggested mode transitions.

For each pair of managers and for each communication direction in the pair, there is a separate variable for mode transition suggestions in such a way that the variable contains at most one suggestion at a time. The variable also contains a suggestion level that is 0, 1, 2 or 3. The initial level is 0 that is equivalent to no suggestion.

A manager M suggests a mode transition x on the level 1 whenever all the information currently seen by M consistently gives an impression of the following things: the current mode is the source mode of x, the precondition expressed by Section 4.1 for x holds, there is no current suggestion on the level 2 or 3, and at least one manager (possibly though not necessarily M itself) is not currently suggesting x on the level 1. There is no other way to make a suggestion on the level 1.

The AOC manager suggests a mode transition x on the level 2 whenever all the information currently seen by the AOC manager consistently gives an impression of the following things: every manager is currently suggesting x on the level 1 or 2, and at least one manager (possibly though not necessarily the AOC manager itself) is not currently suggesting x on the level 2. There is no other way for the AOC manager make a suggestion on the level 2.

A unit manager K suggests a mode transition x on the level 2 whenever all the information currently seen by K consistently gives an impression of the following things: the AOC manager is currently suggesting x on the level 2, there is no current suggestion on the level 3, and at least one manager (possibly though not necessarily K itself) is not current suggesting anything on the level 2. There is no other way for a unit manager to make a suggestion on the level 2.

A manager M suggests a mode transition x on the level 3 whenever all the information currently seen by M consistently gives an impression of the following things: every manager is currently suggesting x on the level 2 or 3, and at least one manager (possibly though not necessarily M itself) is not currently suggesting x on the level 3. There is no other way to make a suggestion on the level 3.

A manager M locally performs a mode transition x whenever M decides to change the level of its own suggestion for x from 2 to 3. Local performing of x by M takes place within a single execution of M and covers the actions expressed by Section 4.1 for x up to the extent allowed by Sections 2 and 3. There is no other way to locally perform a mode transition.

A manager M resets the level in its own suggestions to 0 whenever all the information currently seen by M consistently gives an impression of the following things: M is currently suggesting the transition on the level 3, and any other current suggestion is on the level 0 or 3. There is no other way to erase a suggestion or to reset the suggestion level to 0.

The above arrangements are supposed to ensure the following properties:

- A mode transition can get locally performed by a manager only as a result of the transition being enabled up to the extent expressed by Section 4.1. (The precondition expressed by Section 4.1 for the transition has been true “in a sufficiently recent past” though does not necessarily hold immediately before the local performance.)
- The state transition rules in Section 2 get respected regardless of any delay between precondition evaluation and actions for a mode transition.
- A mode transition gets locally performed by some manager if the transition is long enough enabled up to the extent expressed by Section 4.1.
- A mode transition gets locally performed by every manager if the transition gets locally performed by at least one manager.
- Every complete global occurrence history of local performances of mode transitions is a sequence of effectively global performances of mode transitions.

5. Coordinated policy for unit reconfigurations

Recovery from errors in DSAOCSS is done by means of mode transitions and unit reconfigurations. Up to the extent of mode transitions, the recovery policy is expressed in detail in Section 4.1. The policy for unit reconfigurations is described below.

If the manager of a unit observes a state transition error in the nominal branch of the unit, the manager immediately starts a reconfiguration of the unit.

The manager of a unit starts a reconfiguration of the unit also whenever all the information currently seen by the manager consistently gives an impression that the following conditions hold simultaneously:

- Usability of a selected nominal branch of the unit is insufficient.
- The manager itself is currently not suggesting any mode transition beyond the suggestion level 0.
- All managers agree on the current mode.
- None of the mode transition preconditions expressed by Section 4.1 for the current mode as the source mode holds.

Beyond what is said above, there is no way to start a unit reconfiguration. Strong constraining of usability-based reconfigurations is partially due to the need to ensure that the state transition rules in Section 2 get respected regardless of circumstances. Reconfigurations due to state transition errors do not have to be similarly constrained because Section 4.1 in a certain sense takes into account all possible state transition errors in nominal branches.

6. An example of recovery

The following scenario starts from a stable situation where all managers are in the Preparation mode.

1. The AOC manager observes insufficient usability of a selected nominal branch of RW.
2. Due to information received from the AOC manager, the RW manager makes a similar observation and starts reconfiguration of RW in the mode Preparation.
3. The AOC manager observes an attitude/orbit error and therefore suggests a mode transition to DownToNominal1 on the suggestion level 1.
4. Due to information received from the AOC manager, every unit manager observes the attitude/orbit error and therefore suggests a mode transition to DownToNominal1 on the suggestion level 1.
5. The RW manager observes a state transition error in the redundant branch of RW and therefore suggests a mode transition to DownToOff on the suggestion level 1. Due to slow communication, the RW manager never sees the mode transition to DownToNominal1 having been suggested by every manager on the suggestion level 1.
6. Due to slow communication, too, the AOC manager instead sees the mode transition to DownToNominal1 being suggested by every manager on the level 1 and therefore suggests a mode transition to DownToNominal1 on the suggestion level 2.
7. Due to the rules of mode synchronization, every unit manager suggests a mode transition to DownToNominal1 on the suggestion level 2.
8. Every manager suggests a mode transition to DownToNominal1 on the suggestion level 3 and locally performs the transition, with the result that every manager is in the mode DownToNominal1.
9. Every manager resets its mode transition suggestion level to 0.
10. The RW manager re-observes the above-mentioned state transition error (that could not even possibly have disappeared) and therefore suggests a mode transition to DownToOff on the suggestion level 1. From this on, the possibilities are inevitably limited, so within a few steps every manager reaches the DownToOff mode and then the Off mode.

(End of the document)