Safety-Driven Model-Based System Engineering Methodology Part II:

Application of the Methodology to an Outer Planet Exploration Mission*

December 16, 2007

Prepared by:

Brandon D. Owens, MIT
Margaret Stringfellow Herring, MIT
Dr. Nancy G. Leveson, MIT

Dr. Mitch D. Ingham, JPL
Dr. Kathryn Anne Weiss, JPL

* This research was supported by JPL University Subcontract 1297013

Table of Contents

List of Figures 3
List of Tables 4
Acknowledgements 5
1 Introduction 6
2 Outer Planet Explorer (OPE) Intent Specification 8
3 Derivation of Basic High-Gain Antenna (HGA) Boom Configurations for OPE 82
4 Safety-Related Trade Study of HGA Boom Design Options for OPE 86
5 Traceability Analysis of OPE Intent Specification 107
6 Functional Analysis of OPE 110

List of Figures

Figure 1. Derivation of the basic HGA boom configuration (part 1 of 11). 82
Figure 2. Derivation of the basic HGA boom configuration (part 2 of 11). 82
Figure 3. Derivation of the basic HGA boom configuration (part 3 of 11). 82
Figure 4. Derivation of the basic HGA boom configuration (part 4 of 11). 83
Figure 5. Derivation of the basic HGA boom configuration (part 5 of 11). 83
Figure 6. Derivation of the basic HGA boom configuration (part 6 of 11). 83
Figure 7. Derivation of the basic HGA boom configuration (part 7 of 11). 84
Figure 8. Derivation of the basic HGA boom configuration (part 8 of 11). 84
Figure 9. Derivation of the basic HGA boom configuration (part 9 of 11). 84
Figure 10. Derivation of the basic HGA boom configuration (part 10 of 11). 85
Figure 11. Derivation of the basic HGA boom configuration (part 11 of 11). 85
Figure 12. The HGA boom in the stowed and deployed configurations. 92
Figure 13. Traceability Structure of the OPE Intent Specification (Graphical Representation). 108
Figure 14. The Traceability Structure of the OPE Intent Specification (Matrix Representation). 109
Figure 15. Clustered Design Structure Matrix for the Spacecraft-Level Functional Decomposition. 112
Figure 16. Clustered Design Structure Matrix for the A&AC-Level Functional Decomposition. 114

List of Tables

Table 1. Acronyms used in the application of the methodology to the OPE. 7
Table 2. OPE Intent Specification Item Labeling Notation 7
Table 3. Design options considered in this study for HGA Boom Joint Rotation. 93
Table 4. The initial spacecraft functions identified and the design decisions, constraints, and/or requirements from which they originated. 111
Table 5. The identified A&AC functions and the design decisions, constraints, and/or requirements from which they originated. 113

Acknowledgements

The authors would like to thank Brad Burt, Karla Clark, Bharat Chudasama, Jeffrey Estefan, Cecilia Guiar, Peter Kahn, Steven Larsen, Cin-Young Lee, Robert Lock, Kenneth Meyer, David Nichols, Robert Rasmussen, Henry Stone, Robert Vargo, and Stephen Wall at the Jet Propulsion Laboratory for their support of this study.

This research was performed at the Massachusetts Institute of Technology (supported through JPL University Subcontract 1297013), and at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

1 Introduction

In the first part of this report, we presented a safety-driven model-based system engineering methodology. In this part of the report, we apply this methodology to a hypothetical mission, Outer Planet Explorer (OPE), to explore an icy moon of an outer planet of the solar system. This part of the report includes the following items:

- **OPE Intent Specification:** Intent specifications are a primary product of the methodology. For OPE, the intent specification is a top-down specification and analysis of a deep space exploration mission system with a "deep dive" into the area of communications antenna pointing. The specification encompasses all aspects of the mission system (i.e., spacecraft, launch vehicle, ground communications network, etc.) that influence the deep dive area.

- **Derivation of Basic High-Gain Antenna (HGA) Boom Configurations for OPE:** The derivation of the basic high-gain antenna (HGA) is shown through a narrated "walk-through of portions of the intent specification directly related to HGA Boom design.

- **Safety-Related Trade Study of HGA Boom Design Options for OPE:** Because many design options are available to engineers at virtually every step of the safety-driven methodology, a trade study of design options is presented.

- **Traceability Analysis of the OPE Intent Specification:** Given the importance of traceability, it worth noting how traceability is captured in the products generated from the methodology. Thus, an analysis of the traceability characteristics of the Outer Planet Explorer Intent Specification is provided.

- **Functional Analysis of OPE:** As per the methodology, a functional decomposition of Outer Planet Explorer was performed using Design Structure Matrices (DSMs). These DSMs are provided in this part of the report along with a list of the identified functions and the requirements, constraints, and design decisions from which they were derived.

In the application of the methodology to OPE, a number of acronyms and labeling conventions were used. While these specific acronyms and numbering conventions do not represent a universal standard for intent specification, they should be useful in understanding the material provided in this part of the report.

The acronyms are provided in Table 1, while the OPE Intent Specification item labeling conventions are defined in Table 2. Of special note is that the refinements of specification items are labeled through the addition of a numerical digit (e.g., item A&AC-2.1 is refined by A&AC-2.1.1, A&AC-2.1.2, etc.) or by the definition of a new subsystem/functional element (e.g., S/C-2.3 is refined by A&AC-2.1).

A&AC	Attitude and Articulation Control
AC&DH	A&AC Command and Data Handling
AC	Spacecraft Attitude Controller
AEP	A&AC Electrical Power
C&DH	Command and Data Handling
COM	Communications
DSN	Deep Space Network
DSM	Design Structure Matrix
EP	Electrical Power
GN	Ground Network
HA&T	HGA Attitude and Translation
HGA	High Gain Antenna
LV	Launch Vehicle
MOC	Mission Operations Center
S/C	Spacecraft
SCI	Science Data Collection
TC	Spacecraft Translation Controller

Table 1. Acronyms used in the application of the methodology to the OPE.

2.#	High-Level Design Decision Number
A#	Assumption Number
ACC#	Accident Number
DC#	Customer Design Constraint Number
EA#	Environmental Assumption Number
EC#	Environmental Constraint Number
G#	System Goal Number
H#	High-Level Hazard Number
HLR#	High-Level Requirements Number
PC#	Customer Programmatic Constraint Number
PR#	Project Programmatic Risk Number
SED#	State Effects Diagram Number
SC#	High-Level Safety Constraint Number
SV-#	State Variable Number
X#	Functional Element/Subsystem X Sub-Element Definition Number
X-2.#	Functional Element/Subsystem X Design Decision Number
X-A#	Functional Element/Subsystem X Assumption Number
X-C#	Functional Element/Subsystem Design Constraint Number
X-G#	Functional Element/Subsystem X Goal Number
X-R#	Functional Element/Subsystem X Requirement Number
X-SC#	Functional Element/Subsystem X Safety-Related Design Constraint Number

Table 2. OPE Intent Specification Item Labeling Notation

2 Outer Planet Explorer (OPE) Intent Specification

Level 0: Program Management Information

Project Programmatic Risks

PR1. Mission costs exceed TBD dollars total and/or TBD for any given fiscal year. (↓PC2)

Accident Definition

ACC1. Humans and/or human assets on earth are killed/damaged. (↓PC1, H5, SV-77, SV-78, SV-79)

ACC2. Humans and/or human assets off of the earth are killed/damaged. (↓PC1, H6, SV-77, SV-78, SV-79)

ACC3. Organisms on any of the moons of the outer planet (if they exist) are killed or mutated by biological agents of Earth Origin. (↓H4)

ACC4. The scientific data corresponding to the mission goals are not collected. (↓G1, G2, G3, G4, G5, G6, G7, H1, SV-80)

ACC5. The scientific data corresponding to the mission goals is rendered unusable (i.e., deleted and/or corrupted) before it can be fully investigated. (↓G1, G2, G3, G4, G5, G6, G7, H2, H3, SV-80)

ACC6. Organisms of Earth origin are mistaken for organisms indigenous to any of the moons of the outer planet in future missions to study the outer planet's moon. (↓H4)

ACC7. An incident during this mission directly causes another mission to fail to collect, return, and/or use the scientific data corresponding to its mission goals. (↓PC1, H7, SV-81)

Level 1: System-Level Goals, Requirements, and Constraints

System Goals

G1. Characterize the presence of a subsurface ocean on an icy moon of an outer planet (Clark, 2007)[1]. (↑ACC4, ACC5), (→HLR3, HLR4), (↓SV-81)

G2. Characterize the three-dimensional configuration of the icy crust of the icy moon of an outer planet, including possible zones of liquid (Clark, 2007). (↑ACC4, ACC5), (→HLR1, HLR2, HLR3)

G3. Map organic and inorganic surface compositions of the icy moon of an outer planet, especially as related to astrobiology (Clark, 2007). (↑ACC4, ACC5), (→HLR2, HLR3)

G4. Characterize surface features of the icy moon of an outer planet and identify candidate sites for future exploration (Clark, 2007). (↑ACC4, ACC5), (→HLR1, HLR2, HLR3)

G5. Characterize the magnetic field and radiation environment of the icy moon of an outer planet (Clark, 2007). (↑ACC4, ACC5), (→HLR4, HLR5)

G6. Understand the heat source(s) and time history of any ocean that may exist on the icy moon of an outer planet (Clark, 2007).), (↑ACC4, ACC5), (→HLR2, HLR3)

G7. To make additional characterizations and mappings of the kind described in G1 through G6 of the icy moon of an outer planet, other moons of the outer planet, and the outer planet itself as opportunities arise. (↑ACC4, ACC5), (→S/C-G2)

Introduction

This intent specification describes the design of the Outer Planets Explorer mission, a hypothetical mission to explore the icy moon of an outer planet. In order to achieve the system goals while avoiding the project risks and accidents listed above, it is necessary to build upon prior work in deep space exploration and understand the system's operating environment. Also, it is necessary to design the mission in accordance with basic customer expectations of the mission. In the sections below, prior work in deep space exploration, the system's operation environment, and customer constraints on the design are briefly described and specified.

Historical Information

There is an extensive record of outer planet exploration missions conducted by spacecraft (e.g., the Pioneer missions, the Voyager Missions, Galileo, Cassini, etc.). Through these and other spacecraft missions, an organizational and physical infrastructure exists to support outer planet exploration. This infrastructure includes numerous launch vehicle designs, launch facilities, a ground antenna network (known as the Deep Space Network or DSN) for deep space communications, a ground antenna network (known as GN) for LEO communications, and mission operation facilities. Additionally, while there is no standard spacecraft design for outer planet exploration, there are many component and subsystem designs and technologies that can be used in a custom-built spacecraft for outer planet exploration.

Environment

Velocity: The object of study (an icy moon of an outer planet) translates and rotates with respect to the Sun and the outer planet. All objects that will be in the vicinity of object will not necessarily have this velocity.

Atmosphere: The atmosphere of the icy moon of the outer planet (if indeed one exists) is much thinner than the atmosphere of Earth.

---

[1] Karla Clark, "Europa Explorer—An Exceptional Mission Using Existing Technology," *2007 IEEE Aerospace Conference Proceedings*, Big Sky, MT, March 3–10, 2007.

Vacuum: The space between the orbits of the outer planet and Earth is almost a perfect vacuum.

Gravitational Effects: The gravitational field surrounding the icy outer planet moon to be studied is poorly understood and perturbed by the outer planet and its other moons.

Particle Radiation: The particle radiation environment around the icy moon of the outer planet to be studied is poorly understood and more extreme than the radiation environment in Low Earth Orbit.

Thermal Radiation: The intensity of thermal radiation from the Sun decreases as distance from the Sun increases. Additionally, thermal radiation from the Sun can be blocked and/or reflected by planets and moons (each of which emit their own infrared radiation).

Magnetic Flux: The magnetic field surrounding the icy outer planet moon to be studied is poorly understood and different from the magnetic field in Low Earth Orbit.

Communications Occulting: Data transfer between any two points cannot occur if a planetary body obstructs the line of site between two points (e.g., a spacecraft on the side of a moon furthest from Earth cannot directly communicate with Earth).

Environment Assumptions

EA1. The translation and rotation of the object of study (i.e., a planetoid) with respect to the Sun and relevant outer planet will be relatively stable over the mission and thus predictable.

Environmental Constraints

EC1. The mission elements that reach the orbit of the outer planet moon must withstand a solar flux of TBD Watts/m^2, the solar flux in the orbit of the outer planet moon. (↓SV-1, SV-83)

Assumptions

A1. Technology for Earth-based observation of outer planets and their moons is inadequate to achieve the mission goals. (↓2.1)

A2. Technology for Low Earth Orbit based observation of outer planets and their moons is inadequate to achieve the mission goals. (↓2.1)

A3. Spacecraft automation technology is insufficient for completely autonomous operation of a spacecraft. (→S/C-C4), (↓2.4),

A4. Contamination of an icy outer planet moon with biological agents of Earth origin could have catastrophically adverse effects on any biological agents indigenous to the icy outer planet moon. (→H4)

A5. Contamination of a moon of an outer planet with biological agents of Earth origin could lead to a situation in which a future mission discovers the biological agents and falsely concludes that they are indigenous to the moon of the outer planet. (→H4)

Customer Design Constraints

DC1. The mission must be carried out with existing technologies and space exploration infrastructures as needed (i.e., technologies rated at Technology Readiness Level TBD as defined by NASA). (↓2.1)
Rationale: While technology development is expected to be an ongoing activity of NASA, it is assumed to be beyond the mandate of the mission.

DC1.1. The mission must utilize the Deep Space Network (DSN) for any communications beyond earth orbit. (→S/C-R5, S/C-R6), (↓2.3)

Rationale: The DSN is a proven resource for ground communication with spacecraft operating beyond earth orbit. The capabilities that it provides were created at great expense and funding will not be provided to duplicate them.

DC1.2. The mission must utilize existing launch vehicles for the launch of any equipment into Earth orbit and beyond. (→S/C-C1, S/C-C2), (↓2.2)
Rationale: The capabilities provided by existing launch vehicles were created at great expense and funding will not be provided to duplicate them.

DC1.3. The mission must utilize the GN for any communications within earth orbit. (→S/C-R3, S/C-R4), (↓2.5)
Rationale: The GN is a proven resource for ground communication with the Launch Vehicle.

Customer Programmatic Constraints

PC1. Whenever the mission utilizes space exploration infrastructure that other space exploration missions make use of, it must do so without directly interfering with the successful completion of those missions. (↑ACC1, ACC2, ACC7), (→S/C-C3)
Rationale: It is possible for this mission to interfere with the completion of other missions through denying the other mission access to the space exploration infrastructure (e.g., over-use of limited DSN resources, damage to launch pad during this mission results another mission missing its launch window, etc.)

PC2. The mission must not cost more than TBD dollars total and/or TBD dollars for any given fiscal year. (↑PR1)

Description

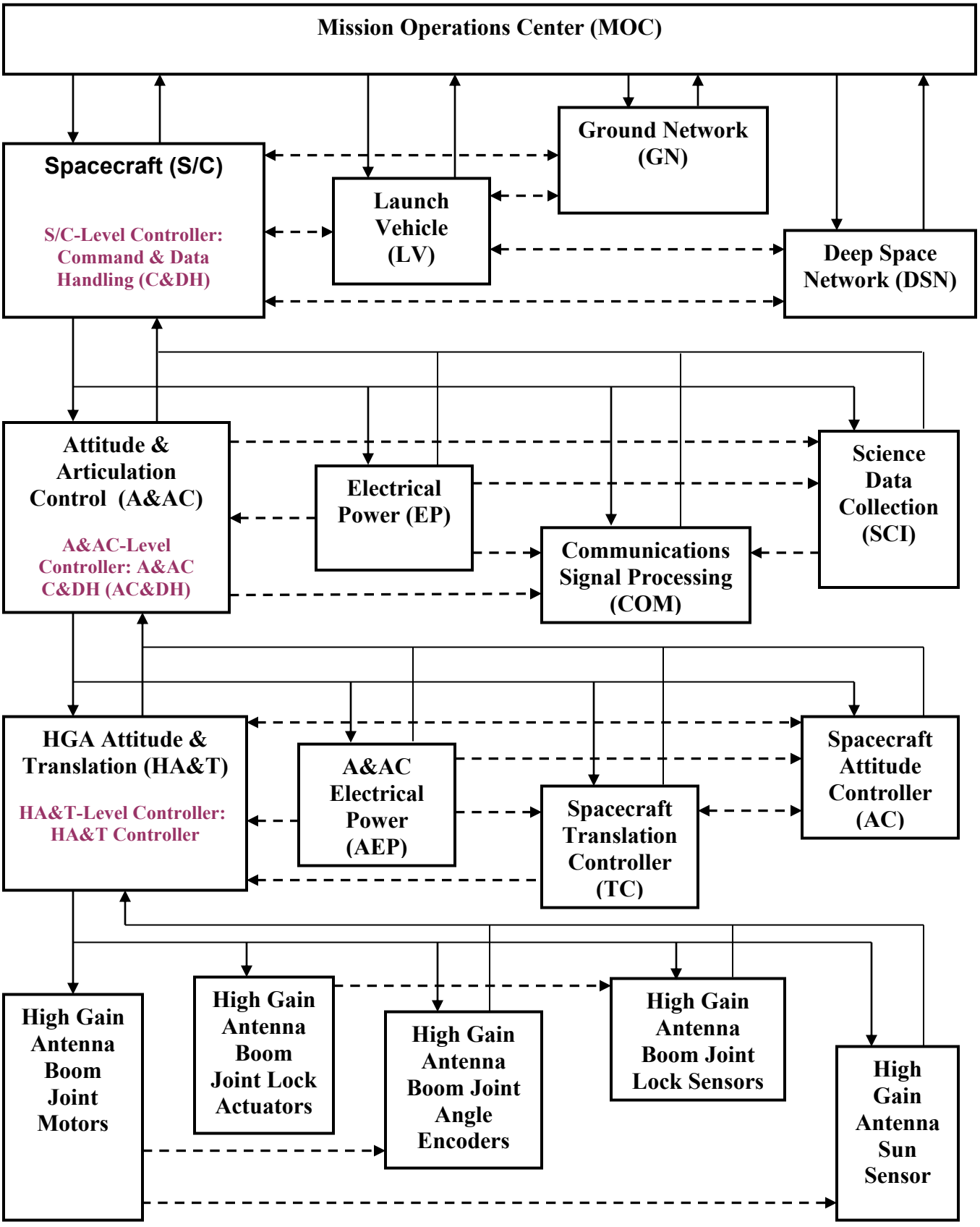
As of this iteration of the intent specification, the components, functional elements, and control structure of this system have been defined through three separate decomposition iterations. In the first iteration, the five major system elements (i.e., spacecraft, launch vehicle, Deep Space Network, Ground Network, and Mission Operations Center) were identified from mission constraints and assumptions about the technology available for the mission. These five elements place interfacing constraints on each other and because most of them are already in existence (i.e., launch vehicle, Deep Space Network, Ground Network), it was possible to immediately identify a number of detailed functions that must be performed by the elements developed specifically for this mission (i.e., spacecraft). In the second iteration of system decomposition, the energy, information, and material interactions necessary for the identified functions for the spacecraft were encoded in a Design Structure Matrix (DSM) and clustered through manual manipulation of the matrix rows and columns (the DSM for the second iteration can be found in Figure 15 of Section 6). This clustering of the functional interactions aided the assignment of the functions to functional elements so that energy, information, and material interactions across the elements would be minimized (i.e., to decouple the functional elements). This process was repeated in the third iteration of system decomposition after a new set of required functions for spacecraft attitude and articulation control were identified (the DSM for the third iteration can be found in Figure 16 of Section 6)

The control structure of the system was designed in a hierarchical fashion in order to manage the interactions across functional elements that could not be decoupled.

System Control Structure:

The control structure of the system is described in the diagram below (the graphical notation of the diagram is also described below in the Control Structure Legend). The highest-level controller is the Mission Operations Center functional element, which includes the humans (operator, scientists, managers, etc.) interfacing with the spacecraft, launch vehicle, Deep Space Network, and Ground Network. The individuals in the Mission Operations Center are responsible for issuing directives to lower-level elements for all work that the elements are to do regarding the Outer Planet Explorer mission. The next level includes those functional elements receiving directives directly from the MOC. Included in this level is the Spacecraft, which has a Command and Data Handling (C&DH) functional element that it uses to control

the major spacecraft functional elements as it executes the directives from the MOC. These major functional elements of the spacecraft comprise the third level of the control structure (though the major functional elements of the launch vehicle, Deep Space Network, and GN would also reside at this level of the control structure in the full specification of the system, they have been omitted from this diagram as specification of these elements fell beyond the scope of this study). The third level of control includes the functional elements of the spacecraft that receive directives directly from the C&DH. One of these functional elements, the Attitude and Articulation Control (A&AC) functional element uses an A&AC Command and Data Handling (AC&DH) to control all of its sub-elements in the execution of directives from the C&DH. These sub-elements are on the fourth-level of the diagram (once again, sub-elements of the other major spacecraft functional elements not included in the diagram as their specification is beyond the scope of this study). One of these sub-element of the A&AC, the High Gain Antenna Attitude and Translation Controller (HA&T) issues commands to and receives measurements from several actuators and sensors. These actuators and sensors comprise the final level of the diagram.


Mission Operations Center (MOC)
Spacecraft (S/C)
S/C-Level Controller: Command & Data Handling (C&DH)
Launch Vehicle (LV)
Ground Network (GN)
Deep Space Network (DSN)
Attitude & Articulation Control (A&AC)
A&AC-Level Controller: A&AC C&DH (AC&DH)
Electrical Power (EP)
Communications Signal Processing (COM)
Science Data Collection (SCI)
HGA Attitude & Translation (HA&T)
HA&T-Level Controller: HA&T Controller
A&AC Electrical Power (AEP)
Spacecraft Translation Controller (TC)
Spacecraft Attitude Controller (AC)
High Gain Antenna Boom Joint Motors
High Gain Antenna Boom Joint Lock Actuators
High Gain Antenna Boom Joint Angle Encoders
High Gain Antenna Boom Joint Lock Sensors
High Gain Antenna Sun Sensor

Control Structure Legend	
Diagram Item:	**Description:**
	Control in the form of Directive(s) or Command(s)
	Control Feedback in the form of State Information or Sensor Measurements
	Physical and Informational Interaction other than Control and Control Feedback Interactions
Functional Element Name Functional Element-Level Controller (if applicable)	Functional Element with the controller of its internal interactions (i.e., the functional element-level interactions)

Functional Elements and Components:

1. Spacecraft (S/C) (←A1, A2, DC1), (↓2.1, SV-5, SV-19)

S/C1. Spacecraft Command and Data Handling (C&DH) functional element (↓S/C-2.1)
Functions Performed: Health & Status Data Collection, Storage, Retrieval from storage, Evaluation, and Packetization; Interface management between spacecraft functional elements; Spacecraft MOC Directive Storage and Execution; etc.

S/C2. Electrical Power (EP) functional element (↓S/C-2.2)
Functions Performed: Spacecraft Power Generation, Spacecraft Power Distribution, etc.

S/C3. Attitude and Articulation Control (A&AC) functional element (↓S/C-2.3)
Functions Performed: Spacecraft Pointing, Spacecraft Translation, Antenna Deployment, Antenna Pointing, etc.

A&AC1. High Gain Antenna Boom (↓A&AC-2.2.1)

A&AC1.1. High Gain Antenna Boom Rotation Joints (↓A&AC-2.2.1, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17)

A&AC1.1.1. High Gain Antenna Boom Rotation Joint Motors (↓A&AC-2.2.1, SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)

A&AC1.1.2 High Gain Antenna Boom Rotation Joint Locks (↓A&AC-2.2.1.4, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

A&AC1.1.3 High Gain Antenna Boom Rotation Joint Angle Encoders (↓A&AC-2.2.1.5)

A&AC1.1.4 High Gain Antenna Boom Rotation Joint Lock Sensors (↓A&AC-2.2.1.12)

A&AC1.1.5 High Gain Antenna Sun Sensor (↓A&AC-2.2.1.11)

A&AC1.2 High Gain Antenna Boom Segments (↓A&AC-2.2.1, SV-6, SV-10)

A&AC1.3. HA&T Control (H&AT) Functional Element (↓A&AC-2.4)
Functions Performed: HGA Boom Shoulder Joint Roll Rotation, HGA Boom Joint Elbow Roll Rotation, HGA Boom Wrist Joint Roll Rotation, HGA Boom Joint Shoulder Pitch Rotation, HGA Boom Joint Elbow Pitch Rotation, HGA Boom Joint Wrist Pitch Rotation, HGA Boom Joint Shoulder Roll Data Collection, HGA Boom Joint Elbow Roll Data Collection, HGA Boom Joint Wrist Roll Data Collection, HGA Boom Joint Shoulder Pitch Data Collection, HGA Boom Joint Elbow Pitch Data Collection, HGA Boom Joint Wrist Roll Pitch Data Collection, HGA Restraint, HGA Boom Joint Elbow Translation, HGA Boom Joint Wrist Translation, HGA Deployment, etc..

A&AC2. A&AC C&DH (AC&DH) (↓A&AC-2.3)
Functions Performed: A&AC C&DH Directive Reception, A&AC C&DH Directive Storage, A&AC H&S Data Evaluation, HGA Pointing State Information Transfer to C&DH, HGA Translation State Information Transfer to C&DH, HGA Translation State Determination, HGA Pointing State Determination, A&AC C&DH Directive Execution, etc.

A&AC3. Spacecraft Attitude Controller (AC) Functional Element (↓A&AC-2.5)
Functions Performed: Spacecraft Pointing, etc.

A&AC4. Spacecraft Translation Controller (TC) Functional Element (↓A&AC-2.6)
Functions Performed: Spacecraft Velocity Changes, etc.

A&AC5. A&AC Electrical Power (AEP) Functional Element (↓A&AC-2.7)
Functions Performed: A&AC Electrical Power Reception from EP, A&AC Power Distribution, etc.

S/C4. Science Data Collection (SCI) functional element (↓S/C-2.4)
Functions Performed: Spacecraft Science Data Collection, Storage, Retrieval from storage, Packetization, etc.

S/C5. Communications Signal Processing (COM) functional element (↓S/C-2.5)
Functions Performed: Spacecraft Data Modulation, Spacecraft MOC Directive Demodulation, RF Transmission/Reception of Data, etc.

COM1. High Gain Antenna (↓COM-2.1, SV-14, SV-24)
Functions Performed: RF Transmission/Reception of Data, etc.

2. Deep Space Network (DSN) (←DC1.1), (↓2.3, SV-20)
3. Launch Vehicle (L/V) (←DC1.2), (↓2.2, SV-21)
4. Mission Operations Center (MOC) (←DC1, A3), (↓2.4, SV-22)

5. NASA Ground Network (GN) (←DC1, DC1.3), (↓2.5, SV-23)

Hazard Analysis
List of Inadequate Control Actions and Control Flaws

Inadequate Control Actions and Control Flaws	Relevant High-Level Hazard(s)	Associated Design Principle	Resulting Safety Constraint(s) or Requirements
C&DH-ICA1. The C&DH executes and/or delegates MOC Directives that are wrong. (→S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC5, S/C-SC7)	H1, H2, H4, H5, H6, H7	C&DH-2.1	
C&DH-CF1.1. A change in the state of the spacecraft or spacecraft environment that invalidates assumptions of directives occurs during the time delay between DSN transmittal of the directives and S/C reception of directives. (↓SV-2)			C&DH-SC1
C&DH-ICA2. The C&DH does not receive an initial set of MOC Directives and/or updates. (→S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC5, S/C-SC7)	H1, H2, H4, H5, H6, H7	C&DH-2.1	
C&DH-CF2.1. The C&DH does not initiate the proper functionality for reception of MOC Directives.			C&DH-SC2
C&DH-ICA3. The C&DH does not send Spacecraft H&S Data to the COM functional element when necessary. (→S/C-SC2)	H2	C&DH-2.1.2	
C&DH-CF3.1. The communication path to the COM functional element is broken, obstructed, or non-existent.			C&DH-SC3
C&DH-CF3.2. The MOC Directives become obsolete (i.e., expire) and no baseline functionality is provided to transmit spacecraft H&S Data.			C&DH-SC4
C&DH-ICA4. The C&DH does not send the 'Send Science Data to COM' directive to the SCI functional element when necessary. (→S/C-SC2)	H2	C&DH-2.1.3	
C&DH-CF4.1. The communication path to the SCI functional element is broken, obstructed, or non-existent.			C&DH-SC5

Inadequate Control Actions and Control Flaws (cont'd)	Relevant High-Level Hazard(s) (cont'd)	Associated Design Principle (cont'd)	Resulting Safety Constraint(s) or Requirements (cont'd)
C&DH-ICA5. The 'Power Up COM Transmit' directive is not sent to the EP when necessary. (→S/C-SC2, C&DH-SC4)	H2	C&DH-2.1.4	
C&DH-CF5.1. The communication path to the EP subsystem is broken, obstructed, or non-existent.			C&DH-SC6
C&DH-CF5.2. The MOC Directives become obsolete (i.e., expire) and no baseline functionality is provided to power up the COM transmit function.			C&DH-SC7
C&DH-ICA6. The 'Power Up COM Transmit' Directive is sent at the wrong time. (→S/C-SC2, C&DH-SC1)	H2	C&DH-2.1.4	
C&DH-CF6.1. 'The Power Up COM Transmit' directive is sent to the COM functional element after the Send Science Data to COM directive is sent to the SCI functional element. *Rationale: If the Power Up COM Transmit directive is sent after the Send Data to COM directive, the COM functional element will not be able to receive the data from the SCI functional element.*			C&DH-SC8
C&DH-ICA7. The Power Down COM command is sent too soon. (→S/C-SC2, C&DH-SC1)	H2	C&DH-2.1.4	
C&DH-CF7.1. The MOC Directives input includes a 'Power Down COM Transmit' directive to be sent during a period of data transmittal.			C&DH-SC9
C&DH-ICA8. The C&DH determines the wrong directives for the A&AC when considering the HGA Pointing State Information Input. (→S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC5, S/C-SC7)	H1, H2, H4, H5, H6, H7	C&DH2.1.6.1	
C&DH-CF8.1. The C&DH does not account for constraints on antenna pointing relative to the main spacecraft structure in determining directives for the A&AC directives.			A&AC-SC3, C&DH-SC10

Inadequate Control Actions and Control Flaws (cont'd)	Relevant High-Level Hazard(s) (cont'd)	Associated Design Principle (cont'd)	Resulting Safety Constraint(s) or Requirements (cont'd)
C&DH-ICA9. The C&DH determines the wrong directives for the A&AC when considering the HGA Translation State Information input. (→S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC5, S/C-SC7)	H1, H2, H4, H5, H6, H7	C&DH-2.1.6.2	
C&DH-CF9.1. The C&DH does not account for the antenna articulation constraints in determining directives for the A&AC functional element.			A&AC-SC3, C&DH-SC10
C&DH-ICA10. The C&DH determines the wrong directives for the A&AC when considering the Science Data Collection State Information. (→S/C-SC1, S/C-SC2)	H1, H2	C&DH-2.1.6.3	
C&DH-CF10.1. During periods of simultaneous data communication with the DSN or GN and science data collection, the C&DH issues directives for the A&AC that degrades one of the two functions.			C&DH-SC11
A&AC-ICA1. The HGA rotates relative to the spacecraft at the wrong time. (→S/C-SC1, S/C-SC2, S/C-SC5, S/C-SC7)	H1, H2, H5, H6, H7	A&AC-2.1	
A&AC-CF1.1. The HGA rotates relative to the spacecraft while the spacecraft is within the payload fairing. *Rationale: Because space is constrained within the payload fairing, articulation of the HGA relative to the spacecraft could cause damage to the HGA, launch vehicle, and/or other parts of the spacecraft. The effects of such damage could range from degradation in HGA functionality to partial break up of the spacecraft and launch vehicle.*			A&AC-SC1

Inadequate Control Actions and Control Flaws (cont'd)	Relevant High-Level Hazard(s) (cont'd)	Associated Design Principle (cont'd)	Resulting Safety Constraint(s) or Requirements (cont'd)
A&AC-ICA2. The HGA rotates too quickly or too much with respect to the spacecraft. (→S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC5, S/C-SC7)	H1, H2, H4, H5, H6, H7	A&AC-2.1	
A&AC-CF2.1. HGA articulation with respect to the spacecraft couples dramatically with spacecraft velocity changes.			A&AC-SC2
A&AC-CF2.2. Other parts of the spacecraft are within the allowable range of HGA rotation and signal radiation.			A&AC-SC3
A&AC-CF2.3. An unidentified mechanical disturbance induces rotational oscillation of the HGA about its desired rotation setpoint. (↓SV-3, SV-5, SV-6, SV-10, SV-14) *Rationale: Mechanical disturbances include interactions with the spacecraft's environment (e.g., micrometeorite impacts, atmospheric drag, etc.) as well as vibrations created by processes performed by the spacecraft's other functional elements (e.g., power generation, etc.)*			A&AC-SC7
A&AC-ICA3. The HGA translates relative to the main spacecraft structure at the wrong time. (→S/C-SC1, S/C-SC2, S/C-SC5, S/C-SC7)	H1, H2, H5, H6, H7	A&AC-2.2	
A&AC-CF3.1. The HGA translates relative to the main spacecraft structure while the spacecraft is within the payload fairing. (↓SV-21)			A&AC-SC1

Inadequate Control Actions and Control Flaws (cont'd)	Relevant High-Level Hazard(s) (cont'd)	Associated Design Principle (cont'd)	Resulting Safety Constraint(s) or Requirements (cont'd)
A&AC-ICA4. The HGA translates relative to the main spacecraft structure too much or too quickly. (→S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC5, S/C-SC7)	H1, H2, H4, H5, H6, H7	A&AC-2.2	
A&AC-CF4.1. HGA translation with respect to the main spacecraft structure couples dramatically with spacecraft velocity changes.			A&AC-SC2
A&AC-CF4.2. Other parts of the spacecraft are within the allowable range of HGA translation and signal radiation.			A&AC-SC3
A&AC-CF4.3. An unidentified mechanical disturbance induces translational oscillation of the HGA about its desired translation setpoint. (↓SV-3, SV-5, SV-6, SV-10, SV-14) *Rationale: Mechanical disturbances include interactions with the spacecraft's environment (e.g., micrometeorite impacts, atmospheric drag, etc.) as well as vibrations created by processes performed by the spacecraft's other functional elements (e.g., power generation, etc.)*			A&AC-SC7
A&AC-ICA5. The A&AC functional element does not send the HGA Pointing State Information input to the C&DH. (→S/C-SC2)	H2	A&AC-2.1.2	
A&AC-CF5.1. The communications path to the C&DH is broken, obstructed, or non-existent.			A&AC-SC4
A&AC-ICA6. The A&AC functional element sends the HGA Pointing State Information inputs at the wrong time. (→S/C-SC2)	H2	A&AC-2.1.2	
A&AC-CF6.1. There is an unacceptable delay in the A&AC functional element's transfer of the HGA Pointing State Information to the C&DH.			A&AC-SC5
A&AC-CF6.2. The HGA Pointing State Information input is not updated frequently enough for the C&DH to provide accurate directives to the A&AC.			A&AC-SC6

Inadequate Control Actions and Control Flaws (cont'd)	Relevant High-Level Hazard(s) (cont'd)	Associated Design Principle (cont'd)	Resulting Safety Constraint(s) or Requirements (cont'd)
A&AC-ICA7. The A&AC functional element does not send the HGA Translation State Information inputs to the C&DH. (→S/C-SC2)	H2	A&AC-2.2.2	
A&AC-CF7.1. The communications path to the C&DH is broken, obstructed, or non-existent.			A&AC-SC4
A&AC-ICA8. The A&AC functional element sends the HGA Translation State Information inputs at the wrong time. (→S/C-SC2)	H2	A&AC-2.2.2	
A&AC-CF8.1. There is an unacceptable delay in the A&AC's transfer of the HGA Translation State Information to the C&DH.			A&AC-SC5
A&AC-CF8.2. The HGA Translation State Information input is not updated frequently enough for the C&DH to provide accurate setpoints to the A&AC.			A&AC-SC6
A&AC-ICA9. The HGA boom rotation joints do not rotate along the appropriate degrees of freedom at the required times. (→S/C-SC2), (↓SV-8, SV-9, SV-12, SV-13, SV-16, SV-17)	H2	A&AC-2.2.1.4, A&AC-2.2.1.8	
A&AC-CF9.1. The lock controller does not command the locks to disengage at the appropriate times. (↓SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)			A&AC-SC8
A&AC-CF9.2. Power is not provided to disengage the locks. (↓SV-43, SV-44, SV-45, SV-46, SV-47, SV-48)			A&AC-SC9
A&AC-CF9.3. The locks do not receive or act on a command to disengage. (↓SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)			A&AC-SC10
A&AC-CF9.4. Power is not provided to the motor on the degree of freedom. (↓SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)			A&AC-SC12
A&AC-CF9.5. Torque is not transferred from the motor to the joint due to slippage. (↓SV-25, SV-26, SV-27, SV-28, SV-29, SV-30)			A&AC-SC13
A&AC-CF9.6. The joint jams along the degree of freedom.			A&AC-SC11

Inadequate Control Actions and Control Flaws (cont'd)	Relevant High-Level Hazard(s) (cont'd)	Associated Design Principle (cont'd)	Resulting Safety Constraint(s) or Requirements (cont'd)
A&AC-ICA10. The HGA Boom Rotation Joints rotate too little, too slowly, or too much along the HGA Boom Rotation Joint degrees of freedom when the locks are disengaged. (→A&AC-SC3, A&AC-SC7), (↓SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)	H1, H2, H4, H5, H6, H7	A&AC-2.2.1.5, A&AC-2.2.1.8	
A&AC-CF10.1. The process model of the motor controller incorrectly accounts for spacecraft velocity changes.			A&AC-SC14
A&AC-CF10.2. Spacecraft velocity changes create inertial loads exceeding the torque capacity of the motor. (↓SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)			A&AC-SC15
A&AC-CF10.3. The process model of the motor controller does not account for time delay in motor actuation. (↓SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)			A&AC-SC14
A&AC-CF10.4. The process model of the motor controller does not account for joint friction, slippage, partial disengagement of the lock, or other physical effects. (↓SV-31, SV-32, SV-33, SV-34, SV-35, SV-36, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)			A&AC-SC14
A&AC-CF10.5. The process model of the motor controller does not account for changes in joint friction, slippage, rotation joint angle measurement errors, or other physical effects. (↓SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)			A&AC-SC14, A&AC-SC19
A&AC-CF10.6. The motor controller receives a control input (or goal) that would violate minimum separation between the HGA boom, HGA, or HGA radiation and the rest of the spacecraft.			A&AC-SC16

A&AC-CF10.7. Power is not provided to the HGA Boom Rotation Joint Motors. *Rationale: If no power is provided to a joint motor while the locks are disengaged, the only resistance to rotational disturbances along the affected degree of freedom will be the rotational inertia of the joint and all HGA Boom Assembly mass downstream of it. Thus, if the disturbance is large enough, oscillation can occur about the desired pointing vector or, worse yet, minimum separation between the HGA, HGA boom, or HGA radiation and other parts of the spacecraft could be violated.*			A&AC-SC12
A&AC-CF10.8. The motor controller does not receive up-to-date feedback on the HGA Boom Rotation Joint Angles.			A&AC-SC18
A&AC-ICA11. The locks on the degrees of freedom in the joints of the HGA boom disengage (i.e., allow rotation) at the wrong time. (→A&AC-SC1, A&AC-SC3), (↑A&AC-2.2.1.8), (↓SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)	H1, H2, H4, H5, H6, H7	A&AC-2.2.1.8	
A&AC-CF11.1. The lock controller commands the locks to disengage while the HGA is in the payload fairing. (↓SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)			A&AC-SC8
A&AC-CF11.2. The joint(s) receive a mechanical disturbance greater than the designed capacity of the lock. (↓SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)			A&AC-SC17
A&AC-CF11.3. The locks receive and act upon the command to disengage with an unaccounted-for delay. (↓SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)			A&AC-SC10

Hazard List and Hazard Log

H1. Inability of Mission to collect data. (↓SV-85)

System Element: Spacecraft (C&DH, SCI, EP, and A&AC), Launch Vehicle, and Mission Operations Center

Operation/Phase: Pre-Launch, Post-Launch/Pre-Icy Moon Orbit, Icy Moon Orbit, Disposal

Causal Factors:

Spacecraft loses functionality to collect data,
(←C&DH-CF1.1, C&DH-CF2.1, C&DH-CF8.1, C&DH-CF9.1, C&DH-CF10.1, A&AC-CF1.1, A&AC-CF2.1, A&AC-CF2.2, A&AC-CF2.3, A&AC-CF3.1, A&AC-CF4.1, A&AC-CF4.2, A&AC-CF4.3, A&AC-CF10.1, A&AC-CF10.2, A&AC-CF10.3, A&AC-CF10.4, A&AC-CF10.5, A&AC-CF10.6, A&AC-CF10.7, A&AC-10.8, A&AC-CF11.1, A&AC-CF11.2, A&AC-CF11.3)

Level and Effect: Potential loss of data collection opportunities (↑ACC4)

Safety Constraints:

The mission must have the necessary functionality for data acquisition at the required times. (→SC1),

The spacecraft must have the necessary functionality for data acquisition at the required times. (→S/C-SC1),

The C&DH must validate the time and state dependent assumptions of directives generated by the MOC. (→C&DH-SC1),

In the absence of valid MOC Directives, the C&DH must initiate the proper functionality for reception of MOC Directives. (→C&DH-SC2),

The C&DH must provide directives to the A&AC that do not place the direction of Earth outside of the HGA's allowable range of articulation and translation. (→C&DH-SC10),

During times of simultaneous communication with the DSN or GN and science data collection, the C&DH must provide directives to the A&AC that do not degrade either function. (→C&DH-SC11),

The HGA must not rotate or translate with respect to the main spacecraft structure while the spacecraft is inside the payload fairing of the launch vehicle. (→A&AC-SC1),

HGA translation and rotation with respect to the main spacecraft structure must be restrained during periods of spacecraft velocity changes so that the HGA does not deform and/or detach from the spacecraft due to inertial loads. (→A&AC-SC2),

While translating and/or rotating, the HGA and the radiation that it emits must maintain minimum separation from other parts of the spacecraft. (→A&AC-SC3),

Mechanical disturbances to the HGA must not create rotational or translational oscillations of the HGA that are large enough to prevent data return.
(→A&AC-SC7)

A command must be sent to disengage the HGA Boom Joint Rotation Locks at the desired HGA Boom deployment time (i.e., after separation of the launch vehicle payload fairing) or any time in which rotation of a locked degree of freedom is desired. (→A&AC-SC8)

The HGA Boom Joint Rotation Locks must receive and respond to a disengagement command within TBD milliseconds. (→A&AC-SC10)

The power supply to the HGA Boom Rotation Joint Motors must not be interrupted for greater than a TBD second interval unless the HGA Boom Rotation Joint Locks engage within TBD seconds. (→A&AC-SC12)

The process model of the controller of the HGA Boom Rotation Joint Motors must explicitly or implicitly account for time delays in the motor actuation, joint friction, slippage, partial disengagement of the joint rotation locks, inertial loads from spacecraft velocity changes, other physical effects on joint rotation, and changes thereof. (→A&AC-SC14)

The spacecraft velocity must not change by more than TBD m/s^2 along an axis perpendicular to the axis of the deployed boom and TBD m/s^2 along an axis parallel to the axis of the deployed boom unless all rotation can be locked along all HGA Boom rotational degrees of freedom. (→A&AC-SC15)

The HGA Boom Rotation Joint motor controller must not receive a control input (goal) that would violate minimum separation between the HGA boom, HGA, or HGA radiation and the rest of the spacecraft. (→A&AC-SC16)

The HGA Boom Rotation Joint Locks must be able to counteract all torques on the rotation joints when they are engaged. (→A&AC-SC17)

The HGA Boom Angle Encoders must provide HGA Boom Rotation Joint angles to the HGA Boom Rotation Joint Motors every TBD seconds. (→A&AC-SC18)

The HGA Boom Rotation Joint Motor controllers must account for HGA Boom Rotation Joint Angle Encoder measurement errors. (→A&AC-SC19)

Analyses Performed:
Actions Taken:
Status:
Verification:
Final Disposal (Closeout Status):
Responsible Engineer:
Remarks: Data includes spacecraft health and status data, science data, and science instrument calibration data (if applicable)

H2. Inability of Mission to return collected data. (↓SV-86)

System Element: Spacecraft (C&DH, COM, and A&AC), DSN, and GN
Operation/Phase: Pre-Launch, Post-Launch/Pre-Icy Moon Orbit, Icy Moon Orbit, Disposal
Causal Factors:
Spacecraft loses functionality to return data,
(←C&DH-CF1.1, C&DH-CF2.1, C&DH-CF3.1, C&DH-CF3.2, C&DH-CF4.1, C&DH-CF5.1, C&DH-CF5.2, C&DH-CF6.1, C&DH-CF7.1, C&DH-CF8.1, C&DH-CF9.1, C&DH-CF10.1, A&AC-CF1.1, A&AC-CF2.1, A&AC-CF2.2, A&AC-CF2.3, A&AC-CF3.1, A&AC-CF4.1, A&AC-CF4.2, A&AC-CF4.3, A&AC-CF5.1, A&AC-CF6.1, A&AC-CF6.2, A&AC-CF7.1, A&AC-CF8.1, A&AC-CF8.2, A&AC-CF9.1, A&AC-CF9.2, A&AC-CF9.3, A&AC-CF9.4, A&AC-CF9.5, A&AC-CF9.6, A&AC-CF10.1, A&AC-CF10.2, A&AC-CF10.3, A&AC-CF10.4, A&AC-CF10.5, A&AC-CF10.6, A&AC-CF10.7, A&AC-CF10.8, A&AC-CF11.1, A&AC-CF11.2, A&AC-CF11.3)
Level and Effect: Potential loss of collected data (↑ACC5)
Safety Constraints:
The mission must be able to return data at the required times. (→SC2),

The spacecraft must be able to return data at the required times. (→S/C-SC2),

The C&DH must validate the time and state dependent assumptions of directives generated by the MOC. (→C&DH-SC1),

In the absence of valid MOC Directives, the C&DH must initiate the proper functionality for reception of MOC Directives. (→C&DH-SC2),

The communications path between the C&DH and COM functional elements for the transfer of Spacecraft H&S Data must not become broken or obstructed. (→C&DH-SC3),

The C&DH must be able to initiate communications with the GN or DSN in the event that the MOC Directives become obsolete. (→C&DH-SC4),

The communications path between the C&DH and SCI functional elements for transmission of the 'Send Science Data to COM' directive must not become broken or obstructed. (→C&DH-SC5),

The communications path between the C&DH and EP for transmission of the 'Power Up COM Transmit' directive must not become broken or obstructed. (→C&DH-SC6),

The C&DH must be able to initiate power transfer between the EP and COM functional elements in the events that the COM Transmit function has been powered down and/or the MOC Directives become obsolete. (→C&DH-SC7),

The C&DH must not attempt to initiate data transfer between the SCI and COM functional elements before power transfer has been initiated between the EP and COM Transmit elements. (→C&DH-SC8),

The C&DH must not terminate power transfer between the EP and COM Transmit functional elements during a period of data transmission unless other safety considerations make such an action necessary. (→C&DH-SC9),

The C&DH must provide directives to the A&AC that do not place the direction of Earth outside of the HGA's allowable range of articulation and translation. (→C&DH-SC10),

During times of simultaneous communication with the DSN or GN and science data collection, the C&DH must provide directives to the A&AC that do not degrade either function. (→C&DH-SC11),

The HGA must not rotate or translate with respect to the main spacecraft structure while the spacecraft is inside the payload fairing of the launch vehicle. (→A&AC-SC1),

HGA translation and rotation with respect to the main spacecraft structure must be restrained during periods of spacecraft velocity changes so that the HGA does not deform and/or detach from the spacecraft due to inertial loads. (→A&AC-SC2),

While translating and/or rotating, the HGA and the radiation that it emits must maintain minimum separation from other parts of the spacecraft. (→A&AC-SC3),

The communications paths between the A&AC functional element and the C&DH for transfer of the HGA Pointing State Information and HGA Translation State Information inputs must not become broken or obstructed. (→A&AC-SC4),

Transfer of the HGA Pointing State Information and HGA Translation State Information between the A&AC and C&DH must take no longer than TBD micro-seconds. (→A&AC-SC5),

The HGA Pointing State Information and HGA Translation State Information inputs to the C&DH must be updated every TBD seconds. (→A&AC-SC6),

Mechanical disturbances to the HGA must not create rotational or translational oscillations of the HGA that are large enough to prevent data return.
(→A&AC-SC7),

A command must be sent to disengage the HGA Boom Joint Rotation Locks at the desired HGA Boom deployment time (i.e., after separation of the launch vehicle payload fairing) or any time in which rotation of a locked degree of freedom is desired. (→A&AC-SC8),

Power must be provided to all HGA Boom Joint Rotation Locks at the desired times of lock disengagement. (→A&AC-SC9),

The HGA Boom Joint Rotation Locks must receive and respond to a disengagement command within TBD milliseconds. (→A&AC-SC10),

All rotation joints must not jam along a rotational degree of freedom. (→A&AC-SC11),

The power supply to the HGA Boom Rotation Joint Motors must not be interrupted for greater than a TBD second interval unless the HGA Boom Rotation Joint Locks engage within TBD seconds. (→A&AC-SC12),

The HGA Boom Rotation Joint Motors must not slip more than TBD radians/revolution with respect to the joints. (→A&AC-SC13),

The process model of the controller of the HGA Boom Rotation Joint Motors must explicitly or implicitly account for time delays in the motor actuation, joint friction, slippage, partial disengagement of the joint rotation locks, inertial loads from spacecraft velocity changes, other physical effects on joint rotation, and changes thereof. (→A&AC-SC14),

The spacecraft velocity must not change by more than TBD m/s^2 along an axis perpendicular to the axis of the deployed boom and TBD m/s^2 along an axis parallel to the axis of the deployed boom unless all rotation can be locked along all HGA Boom rotational degrees of freedom. (→A&AC-SC15),

The HGA Boom Rotation Joint motor controller must not receive a control input (goal) that would violate minimum separation between the HGA boom, HGA, or HGA radiation and the rest of the spacecraft. (→A&AC-SC16),

The HGA Boom Rotation Joint Locks must be able to counteract all torques on the rotation joints when they are engaged. (→A&AC-SC17),

The HGA Boom Angle Encoders must provide HGA Boom Rotation Joint angles to the HGA Boom Rotation Joint Motors every TBD seconds. (→A&AC-SC18),

The HGA Boom Rotation Joint Motor controllers must account for HGA Boom Rotation Joint Angle Encoder measurement errors. (→A&AC-SC19)

Analyses Performed:
Actions Taken:
Status:
Verification:
Final Disposal (Closeout Status):
Responsible Engineer:
Remarks:

H3. Inability of mission scientific investigators to use returned data. (↓SV-87, SV-88)

System Element: Mission Operations Center
Operation/Phase: Pre-Launch, Post-Launch/Pre-Icy Moon Orbit, Icy Moon Orbit, Disposal, Post Disposal
Causal Factors:
MOC corrupts or deletes returned data before transfer to scientific investigators (e.g., the MOC provides science data without calibration data)
Level and Effect: Potential loss of returned data and failure to establish scientific return from the mission. (↑ACC5)
Safety Constraints:
Mission scientific investigators must be able to use the data from the mission at the required times. (→SC3)
Analyses Performed:
Actions Taken:
Status:

Verification:
Final Disposal (Closeout Status):
Responsible Engineer:
Remarks: This hazard may or may not apply to the Pre-Launch phases depending on the requirements for calibration data.

H4. Contamination of Outer Planet Moon with biological agents of Earth origin on mission hardware. (←A4, A5), (↓SV-1, SV-89)

System Element: Spacecraft (C&DH, EP, and A&AC)
Operation/Phase: Post-Launch/Pre-Icy Moon Orbit, Icy Moon Orbit, Disposal
Causal Factors:
Physical elements of the spacecraft unintentionally move along a collision course with an outer planet moon,
Non-sterile physical elements of the spacecraft are intentionally impacted into an outer planet moon,
(←C&DH-CF1.1, C&DH-CF2.1, C&DH-CF8.1, C&DH-CF9.1, A&AC-CF2.1, A&AC-CF2.2, A&AC-CF2.3, A&AC-CF4.1, A&AC-CF4.2, A&AC-CF4.3, A&AC-CF8.1, A&AC-CF10.1, A&AC-CF10.2, A&AC-CF10.3, A&AC-CF10.4, A&AC-CF10.5, A&AC-CF10.6, A&AC-CF10.7, A&AC-CF10.8, A&AC-CF11.1, A&AC-CF11.2, A&AC-CF11.3)
Level and Effect: Potential destruction and/or mutation of organism populations indigenous to the Outer Planet Moon. (↑ACC3) Additionally, in the event of contamination of the outer planet moon, there is the potential for future missions to mistakenly conclude that the organisms are indigenous to the outer planet moon. (↑ACC6)
Safety Constraints:
All physical elements of the mission must not unintentionally move along a collision course with an outer planet moon. (→SC4),

All physical elements of the mission that intentionally collide with an outer planet moon must be sterile. (→SC5),

All physical elements of the spacecraft must not unintentionally move along a collision course with an outer planet moon. (→S/C-SC3),

All physical elements of the spacecraft that intentionally collide with an outer planet moon must be sterile. (→S/C-SC4),

The C&DH must validate the time and state dependent assumptions of directives generated by the MOC. (→C&DH-SC1),

In the absence of valid MOC Directives, the C&DH must initiate the proper functionality for reception of MOC Directives. (→C&DH-SC2),

The C&DH must provide directives to the A&AC that do not place the direction of Earth outside of the HGA's allowable range of articulation and translation. (→C&DH-SC10),

HGA translation and rotation with respect to the main spacecraft structure must be restrained during periods of spacecraft velocity changes so that the HGA does not deform and/or detach from the spacecraft due to inertial loads. (→A&AC-SC2),

While translating and/or rotating, the HGA and the radiation that it emits must maintain minimum separation from other parts of the spacecraft. (→A&AC-SC3),

Mechanical disturbances to the HGA must not create rotational or translational oscillations of the HGA that are large enough to prevent data return.
(→A&AC-SC7),

A command must be sent to disengage the HGA Boom Joint Rotation Locks at the desired HGA Boom deployment time (i.e., after separation of the launch vehicle payload fairing) or any time in which rotation of a locked degree of freedom is desired. (→A&AC-SC8),

The HGA Boom Joint Rotation Locks must receive and respond to a disengagement command within TBD milliseconds. (→A&AC-SC10),

The power supply to the HGA Boom Rotation Joint Motors must not be interrupted for greater than a TBD second interval unless the HGA Boom Rotation Joint Locks engage within TBD seconds. (→A&AC-SC12),

The process model of the controller of the HGA Boom Rotation Joint Motors must explicitly or implicitly account for time delays in the motor actuation, joint friction, slippage, partial disengagement of the joint rotation locks, inertial loads from spacecraft velocity changes, other physical effects on joint rotation, and changes thereof. (→A&AC-SC14),

The spacecraft velocity must not change by more than TBD m/s^2 along an axis perpendicular to the axis of the deployed boom and TBD m/s^2 along an axis parallel to the axis of the deployed boom unless all rotation can be locked along all HGA Boom rotational degrees of freedom. (→A&AC-SC15),

The HGA Boom Rotation Joint motor controller must not receive a control input (goal) that would violate minimum separation between the HGA boom, HGA, or HGA radiation and the rest of the spacecraft. (→A&AC-SC16),

The HGA Boom Rotation Joint Locks must be able to counteract all torques on the rotation joints when they are engaged. (→A&AC-SC17),

The HGA Boom Angle Encoders must provide HGA Boom Rotation Joint angles to the HGA Boom Rotation Joint Motors every TBD seconds. (→A&AC-SC18),

The HGA Boom Rotation Joint Motor controllers must account for HGA Boom Rotation Joint Angle Encoder measurement errors. (→A&AC-SC19)

Analyses Performed:
Actions Taken:
Status:
Verification:
Final Disposal (Closeout Status):
Responsible Engineer:
Remarks:

H5. Exposure of Earth life or human assets on Earth to toxic, radioactive, and/or energetic elements of mission hardware. (↓SV-2, SV-90, SV-91, SV-92, SV-93, SV-94, SV-95)

System Element: Spacecraft (C&DH, EP, and A&AC), Launch Vehicle, DSN, GN, Mission Operations Center
Operation/Phase: Pre-Launch, Post-Launch/Pre-Icy Moon Orbit, Icy Moon Orbit, Disposal
Causal Factors:
The spacecraft unintentionally moves along a collision course with Earth,
Physical elements of the spacecraft unintentionally detach from the main spacecraft structure,
Toxic, radioactive, and/or energetic elements of the spacecraft that are intentionally collided with earth survive re-entry and land in inhabited areas,

(←C&DH-CF1.1, C&DH-CF2.1, C&DH-CF8.1, C&DH-CF9.1, A&AC-CF1.1, A&AC-CF2.1, A&AC-CF2.2, A&AC-CF2.3, A&AC-CF3.1, A&AC-CF4.1, A&AC-CF4.2, A&AC-CF4.3, A&AC-CF8.1, A&AC-CF10.1, A&AC-CF10.2, A&AC-CF10.3, A&AC-CF10.4, A&AC-CF10.5, A&AC-CF10.6, A&AC-CF10.7, A&AC-CF10.8, A&AC-CF11.1, A&AC-CF11.2, A&AC-CF11.3)
Level and Effect: Potential for immediate death and injury of humans, damage to human assets, and delayed adverse health effects on a human and wildlife populations. (↑ACC1). Potential for failure of another mission to collect, return, and/or use data in accordance with its mission goals. (↑ACC7)
Safety Constraints:
All physical elements of the mission must not unintentionally move along a collision course with Earth. (→SC6),

All physical elements of the mission that intentionally collide with the Earth must not cause damage to humans or human assets. (→SC7),

All physical elements of the spacecraft must not unintentionally move along a collision course with Earth. (→S/C-SC5),

All physical elements of the spacecraft that intentionally collide with the Earth must not cause damage to humans or human assets. (→S/C-SC6),

The C&DH must validate the time and state dependent assumptions of directives generated by the MOC. (→C&DH-SC1),

In the absence of valid MOC Directives, the C&DH must initiate the proper functionality for reception of MOC Directives. (→C&DH-SC2),

The C&DH must provide directives to the A&AC that do not place the direction of Earth outside of the HGA's allowable range of articulation and translation. (→C&DH-SC10),

The HGA must not rotate or translate with respect to the main spacecraft structure while the spacecraft is inside the payload fairing of the launch vehicle.
(→A&AC-SC1),

HGA translation and rotation with respect to the main spacecraft structure must be restrained during periods of spacecraft velocity changes so that the HGA does not deform and/or detach from the spacecraft due to inertial loads. (→A&AC-SC2),

While translating and/or rotating, the HGA and the radiation that it emits must maintain minimum separation from other parts of the spacecraft. (→A&AC-SC3),

Mechanical disturbances to the HGA must not create rotational or translational oscillations of the HGA that are large enough to prevent data return.
(→A&AC-SC7),

A command must be sent to disengage the HGA Boom Joint Rotation Locks at the desired HGA Boom deployment time (i.e., after separation of the launch vehicle payload fairing) or any time in which rotation of a locked degree of freedom is desired. (→A&AC-SC8),

The HGA Boom Joint Rotation Locks must receive and respond to a disengagement command within TBD milliseconds. (→A&AC-SC10),

The power supply to the HGA Boom Rotation Joint Motors must not be interrupted for greater than a TBD second interval unless the HGA Boom Rotation Joint Locks engage within TBD seconds. (→A&AC-SC12),

The process model of the controller of the HGA Boom Rotation Joint Motors must explicitly or implicitly account for time delays in the motor actuation, joint friction, slippage, partial disengagement of the joint rotation locks, inertial loads from spacecraft velocity changes, other physical effects on joint rotation, and changes thereof. (→A&AC-SC14),

The spacecraft velocity must not change by more than TBD m/s^2 along an axis perpendicular to the axis of the deployed boom and TBD m/s^2 along an axis parallel to the axis of the deployed boom unless all rotation can be locked along all HGA Boom rotational degrees of freedom. (→A&AC-SC15),

The HGA Boom Rotation Joint motor controller must not receive a control input (goal) that would violate minimum separation between the HGA boom, HGA, or HGA radiation and the rest of the spacecraft. (→A&AC-SC16),

The HGA Boom Rotation Joint Locks must be able to counteract all torques on the rotation joints when they are engaged. (→A&AC-SC17),

The HGA Boom Angle Encoders must provide HGA Boom Rotation Joint angles to the HGA Boom Rotation Joint Motors every TBD seconds. (→A&AC-SC18),

The HGA Boom Rotation Joint Motor controllers must account for HGA Boom Rotation Joint Angle Encoder measurement errors. (→A&AC-SC19)

Analyses Performed:
Actions Taken:
Status:
Verification:
Final Disposal (Closeout Status):
Responsible Engineer:
Remarks:

H6. Exposure of Earth life or human assets off Earth to toxic, radioactive, and/or energetic elements of mission hardware. (↓SV-2, SV-90, SV-91, SV-92, SV-93, SV-94, SV-95)

System Element: Spacecraft (C&DH, EP, and A&AC) and Launch Vehicle
Operation/Phase: Post-Launch/Pre-Icy Moon Orbit
Causal Factors:
The spacecraft unintentionally moves along a collision course with Earth
Physical elements of the spacecraft unintentionally detach from the main spacecraft,
Toxic, radioactive, and/or energetic elements of the spacecraft that are intentionally collided with earth survive re-entry and land in inhabited areas,
(←C&DH-CF1.1, C&DH-CF2.1, C&DH-CF8.1, C&DH-CF9.1, A&AC-CF1.1, A&AC-CF2.1, A&AC-CF2.2, A&AC-CF2.3, A&AC-CF3.1, A&AC-CF4.1, A&AC-CF4.2, A&AC-CF4.3, A&AC-CF8.1, A&AC-CF10.1, A&AC-CF10.2, A&AC-CF10.3, A&AC-CF10.4, A&AC-CF10.5, A&AC-CF10.6, A&AC-CF10.7, A&AC-CF10.8, A&AC-CF11.1, A&AC-CF11.2, A&AC-CF11.3)
Level and Effect: Potential for immediate death and injury of humans off earth; damage, destruction, and/or abandonment of crewed space stations, damage, destruction, and/or abandonment of crewed lunar stations, and damage or destruction of uncrewed spacecraft. (↑ACC2). Potential for failure of another mission to collect, return, and/or use data in accordance with its mission goals. (↑ACC7)

Safety Constraints:
All physical elements of the mission must not unintentionally move along a collision course with humans or human assets that are off of Earth (e.g., International Space Station). (→SC8),

All physical elements of the spacecraft must not unintentionally move along a collision course with Earth life or human assets that are off of Earth (e.g., International Space Station). (→S/C-SC7),

The C&DH must validate the time and state dependent assumptions of directives generated by the MOC. (→C&DH-SC1),

In the absence of valid MOC Directives, the C&DH must initiate the proper functionality for reception of MOC Directives. (→C&DH-SC2),

The C&DH must provide directives to the A&AC that do not place the direction of Earth outside of the HGA's allowable range of articulation and translation. (→C&DH-SC10),

The HGA must not rotate or translate with respect to the main spacecraft structure while the spacecraft is inside the payload fairing of the launch vehicle. (→A&AC-SC1),

HGA translation and rotation with respect to the main spacecraft structure must be restrained during periods of spacecraft velocity changes so that the HGA does not deform and/or detach from the spacecraft due to inertial loads. (→A&AC-SC2),

While translating and/or rotating, the HGA and the radiation that it emits must maintain minimum separation from other parts of the spacecraft. (→A&AC-SC3),

Mechanical disturbances to the HGA must not create rotational or translational oscillations of the HGA that are large enough to prevent data return.
(→A&AC-SC7),

A command must be sent to disengage the HGA Boom Joint Rotation Locks at the desired HGA Boom deployment time (i.e., after separation of the launch vehicle payload fairing) or any time in which rotation of a locked degree of freedom is desired. (→A&AC-SC8),

The HGA Boom Joint Rotation Locks must receive and respond to a disengagement command within TBD milliseconds. (→A&AC-SC10),

The power supply to the HGA Boom Rotation Joint Motors must not be interrupted for greater than a TBD second interval unless the HGA Boom Rotation Joint Locks engage within TBD seconds. (→A&AC-SC12),

The process model of the controller of the HGA Boom Rotation Joint Motors must explicitly or implicitly account for time delays in the motor actuation, joint friction, slippage, partial disengagement of the joint rotation locks, inertial loads from spacecraft velocity changes, other physical effects on joint rotation, and changes thereof. (→A&AC-SC14),

The spacecraft velocity must not change by more than TBD m/s^2 along an axis perpendicular to the axis of the deployed boom and TBD m/s^2 along an axis parallel to the axis of the deployed boom unless all rotation can be locked along all HGA Boom rotational degrees of freedom. (→A&AC-SC15),

The HGA Boom Rotation Joint motor controller must not receive a control input (goal) that would violate minimum separation between the HGA boom, HGA, or HGA radiation and the rest of the spacecraft. (→A&AC-SC16),

The HGA Boom Rotation Joint Locks must be able to counteract all torques on the rotation joints when they are engaged. (→A&AC-SC17),

The HGA Boom Angle Encoders must provide HGA Boom Rotation Joint angles to the HGA Boom Rotation Joint Motors every TBD seconds. (→A&AC-SC18),

The HGA Boom Rotation Joint Motor controllers must account for HGA Boom Rotation Joint Angle Encoder measurement errors. (→A&AC-SC19)

Analyses Performed:
Actions Taken:
Status:
Verification:
Final Disposal (Closeout Status):
Responsible Engineer:
Remarks:

H7. Inability of other space exploration missions to use shared space exploration infrastructure to collect, return, and/or use data.

System Element: Spacecraft (C&DH, EP, and A&AC), DSN, GN, Mission Operations Center
Operation/Phase: Pre-Launch, Post-Launch/Pre-Icy Moon Orbit, Icy Moon Orbit, Disposal, Post-Disposal
Causal Factors:
The Mission unnecessarily denies use of space exploration infrastructure to another mission,
The spacecraft unintentionally moves along a collision course with Earth,
Physical elements of the spacecraft unintentionally detach from the main spacecraft structure,
Toxic, radioactive, and/or energetic elements of the spacecraft that are intentionally collided with earth survive re-entry and land in inhabited areas,
(←C&DH-CF1.1, C&DH-CF2.1, C&DH-CF8.1, C&DH-CF9.1, A&AC-CF1.1, A&AC-CF2.1, A&AC-CF2.2, A&AC-CF2.3, A&AC-CF3.1, A&AC-CF4.1, A&AC-CF4.2, A&AC-CF4.3, A&AC-CF10.1, A&AC-CF10.2, A&AC-CF10.3, A&AC-CF10.4, A&AC-CF10.5, A&AC-CF10.6, A&AC-CF10.7, A&AC-CF10.8, A&AC-CF11.1, A&AC-CF11.2, A&AC-CF11.3)
Level and Effect: Potential for failure of another mission to collect, return, and/or use data in accordance with its mission goals. (↑ACC7)
Safety Constraints:
All physical elements of the mission must not unintentionally move along a collision course with Earth. (→SC6),

All physical elements of the mission that intentionally collide with the Earth must not cause damage to humans or human assets. (→SC7),

All physical elements of the mission must not unintentionally move along a collision course with humans or human assets that are off of Earth (e.g., International Space Station). (→SC8),

The Mission must not deny usage of shared space exploration infrastructure to another mission if such a denial would jeopardize that mission's goals (This constraint does not necessarily apply if the Mission's goals are similarly or more severely jeopardized). (→SC9),

All physical elements of the spacecraft must not unintentionally move along a collision course with Earth. (→S/C-SC5),

All physical elements of the spacecraft that intentionally collide with the Earth must not cause damage to humans or human assets. (→S/C-SC6),

All physical elements of the spacecraft must not unintentionally move along a collision course with Earth life or human assets that are off of Earth (e.g., International Space Station). (→S/C-SC7),

The C&DH must validate the time and state dependent assumptions of directives generated by the MOC. (→C&DH-SC1),

In the absence of valid MOC Directives, the C&DH must initiate the proper functionality for reception of MOC Directives. (→C&DH-SC2),

The C&DH must provide directives to the A&AC that do not place the direction of Earth outside of the HGA's allowable range of articulation and translation. (→C&DH-SC10),

The HGA must not rotate or translate with respect to the main spacecraft structure while the spacecraft is inside the payload fairing of the launch vehicle. (→A&AC-SC1),

HGA translation and rotation with respect to the main spacecraft structure must be restrained during periods of spacecraft velocity changes so that the HGA does not deform and/or detach from the spacecraft due to inertial loads. (→A&AC-SC2),

While translating and/or rotating, the HGA and the radiation that it emits must maintain minimum separation from other parts of the spacecraft. (→A&AC-SC3),

Mechanical disturbances to the HGA must not create rotational or translational oscillations of the HGA that are large enough to prevent data return.
(→A&AC-SC7),

A command must be sent to disengage the HGA Boom Joint Rotation Locks at the desired HGA Boom deployment time (i.e., after separation of the launch vehicle payload fairing) or any time in which rotation of a locked degree of freedom is desired. (→A&AC-SC8),

The HGA Boom Joint Rotation Locks must receive and respond to a disengagement command within TBD milliseconds. (→A&AC-SC10),

The power supply to the HGA Boom Rotation Joint Motors must not be interrupted for greater than a TBD second interval unless the HGA Boom Rotation Joint Locks engage within TBD seconds. (→A&AC-SC12),

The process model of the controller of the HGA Boom Rotation Joint Motors must explicitly or implicitly account for time delays in the motor actuation, joint friction, slippage, partial disengagement of the joint rotation locks, inertial loads from spacecraft velocity changes, other physical effects on joint rotation, and changes thereof. (→A&AC-SC14),

The spacecraft velocity must not change by more than TBD m/s^2 along an axis perpendicular to the axis of the deployed boom and TBD m/s^2 along an axis parallel to the axis of the deployed boom unless all rotation can be locked along all HGA Boom rotational degrees of freedom. (→A&AC-SC15),

The HGA Boom Rotation Joint motor controller must not receive a control input (goal) that would violate minimum separation between the HGA boom, HGA, or HGA radiation and the rest of the spacecraft. (→A&AC-SC16),

The HGA Boom Rotation Joint Locks must be able to counteract all torques on the rotation joints when they are engaged. (→A&AC-SC17),

The HGA Boom Angle Encoders must provide HGA Boom Rotation Joint angles to the HGA Boom Rotation Joint Motors every TBD seconds. (→A&AC-SC18),

The HGA Boom Rotation Joint Motor controllers must account for HGA Boom Rotation Joint Angle Encoder measurement errors. (→A&AC-SC19)

Analyses Performed:
Actions Taken:
Status:
Verification:
Final Disposal (Closeout Status):
Responsible Engineer:
Remarks:

High-Level Safety Constraints

SC1. The mission must have the necessary functionality for data acquisition at the required times. (←H1), (↓2.1, 2.2, 2.4, SV-85), (→MOC-G1, MOC-G2, MOC-G3, MOC-G4)

SC2. The mission must be able to return data at the required times. (←H2), (↓2.1, 2.3, 2.4, 2.5, SV-86), (→MOC-G1, MOC-G2, MOC-G3, MOC-G4)

SC3. Mission scientific investigators must be able to use the data from the mission at the required times. (←H3), (↓2.1, 2.3, 2.4, 2.5, SV-87, SV-88), (→MOC-G1, MOC-G2, MOC-G3, MOC-G4)

SC4. All physical elements of the mission must not unintentionally move along a collision course with an outer planet moon. (←H4), (↓2.1, 2.4, SV-1, SV-89), (→MOC-G1, MOC-G2, MOC-G3, MOC-G4)

SC5. All physical elements of the mission that intentionally collide with an outer planet moon must be sterile. (←H4), (↓2.1, 2.4, SV-2, SV-89), (→MOC-G1, MOC-G2, MOC-G3, MOC-G4)

SC6. All physical elements of the mission must not unintentionally move along a collision course with Earth. (←H5, H7), (↓2.1, 2.2, 2.4, SV-2, SV-92), (→MOC-G1, MOC-G2, MOC-G3, MOC-G4)

SC7. All physical elements of the mission that intentionally collide with the Earth must not cause damage to humans or human assets. (←H5, H7), (↓2.1, 2.2, 2.4, SV-2, SV-90, SV-91, SV-92, SV-93, SV-94, SV-95), (→MOC-G1, MOC-G2, MOC-G3, MOC-G4)

SC8. All physical elements of the mission must not unintentionally move along a collision course with humans or human assets that are off of Earth (e.g., International Space Station). (←H6, H7), (↓2.1, 2.2, 2.4, SV-2, SV-92), (→MOC-G1, MOC-G2, MOC-G3, MOC-G4)

SC9. The Mission must not deny usage of shared space exploration infrastructure to another mission if such a denial would jeopardize that mission's goals (This constraint does not necessarily apply if the Mission's goals are similarly or more severely jeopardized). (←H7), (↓2.1, 2.2, 2.3, 2.4, 2.5, SV-96), (→MOC-G1, MOC-G2, MOC-G3, MOC-G4)

High-Level Requirements

HLR1. The mission shall image TBD% of the surface of the icy moon of the outer planet in the visual spectrum to a resolution of TBD meters. (←G2, G4), (→S/C-G1, S/C-G2, S/C-R1, S/C-R2), (↓2.1, SV-1, SV-97, SV-98)
Rationale: Visual data of this resolution will is necessary for characterization of icy crust and identification of candidate sites for exploration.

HLR2. The mission shall image TBD% of the surface of the icy moon of the outer planet moon in the infrared spectrum to a resolution of TBD. (←G2, G3, G4, G6), (→S/C-G1, S/C-G2, S/C-R1, S/C-R2), (↓2.1, SV-1, SV-99, SV-100)
Rationale: The infrared radiation emitted by a mass is a function of its temperature and thermal properties. Thus, imaging the IR spectrum of surface provides insights into the physical composition of the icy moon's surface and the location of heat sources.

HLR3. The mission shall image TBD% of the surface of the icy moon of the outer planet in spectra other than visual and infrared, to a resolution of TBD. (←G1, G2, G3, G4, G6), (→S/C-G1, S/C-G2, S/C-R1, S/C-R2), (↓2.1, SV-1, SV-101, SV-102)
Rationale: The other bands of the spectrum provide insights into the chemical composition of the icy moon

HLR4. The mission shall measure the magnetic field surrounding TBD% of the icy moon of the outer planet (altitude TBD to altitude TBD). (←G1, G5), (→S/C-G1, S/C-G2, S/C-R1, S/C-R2), (↓2.1, SV-1,SV-103)
Rationale: These measurements are necessary to characterize the magnetic field of the icy moon of the outer planet. An understanding of this field provides insights in the physical composition of the moon, including the possible existence of an ocean.

HLR5. The mission shall measure the flux of radiation particles of energy levels TBD MeV to TBD MeV in TBD% of the space surrounding the icy moon of the outer planet (altitude TBD to altitude TBD). (←G5), (→S/C-G1, S/C-G2, S/C-R1, S/C-R2), (↓2.1, SV-1, SV-104, SV-105)
Rationale: These measurements are necessary to characterize the radiation environment of the icy moon of the outer planet.

Level 1.1: Spacecraft (S/C) Goals, Requirements, and Constraints

Spacecraft (S/C) Goals

S/C-G1. To collect the data specified in HLR 1 through HLR5. (←HLR1, HLR2, HLR3, HLR4, HLR5), (→S/C-R1, S/C-R2)

S/C-G2. To surpass the data collection specified HLR1 through HLR5 with additional observations of the icy moon of the outer planet, other moons of the outer planet, and the outer planet itself. (←HLR1, HLR2, HLR3, HLR4, HLR5, G7), (→S/C-C4)

Spacecraft (S/C) Requirements

S/C-R1. After release from the Launch Vehicle, the spacecraft shall enter and maintain an orbit around the icy moon of the outer planet at an inclination of greater than TBD degrees for at least 90 days. (←HLR1, HLR2, HLR3, HLR4, HLR5, S/C-G1), (↓S/C-2.3, SV-1), (→A&AC-G1)

> *Rationale: The inclination of the orbit determines the percent of the moon's surface that the spacecraft will fly over. The duration of TBD days is necessary to collect the desired data. Additional days in orbit may be necessary to initialize data collection.*

S/C-R2. The spacecraft shall collect the data specified in HLR1 through HLR5 for at least TBD days. (←HLR1, HLR2, HLR3, HLR4, HLR5, S/C-G1), (↓S/C-2.4)

S/C-R3. While in LEO orbit (distance from Earth < TBD km), the spacecraft shall packetize all data to be transmitted to Earth, modulate it onto GN operating frequencies, and radiate it in the direction of the GN. (←DC1.3), (↓S/C-2.1, S/C-2.3, S/C-2.5, SV-1), (→COM-G1)

> *Rationale: Data transferred through GN must be packetized, modulated onto GN operating frequencies, and radiated in the direction of the GN. Note that the decision to have the spacecraft interface with the GN is not final. It may be possible to conduct all LEO communications through the launch vehicle.*

S/C-R4. While in LEO orbit (distance from Earth < TBD km), the spacecraft shall demodulate data sent to it through the GN. (←DC1.3), (↓S/C-2.5, SV-2), (→COM-G2)

Rationale: Data transmitted from GN is packetized and modulated onto GN operating frequencies. Note that the decision to have the spacecraft interface with the GN is not final. It may be possible to conduct all LEO communications through the launch vehicle.

S/C-R5. While beyond LEO orbit (distance from Earth > TBD km), the spacecraft shall packetize all data to be transmitted to Earth, modulate it onto DSN operating frequencies, and radiate it in the direction of the DSN. (←DC1.1), (↓S/C-2.1, S/C-2.3, S/C-2.4, S/C-2.5, SV-2), (→COM-G3)

Rationale: Data transferred through DSN must be packetized, modulated onto DSN operating frequencies, and radiated in the direction of the DSN

S/C-R6. While beyond LEO orbit (distance from Earth < TBD km), the spacecraft shall demodulate data sent to it through the DSN. (←DC1.1), (↓S/C-2.5, SV-2), (→COM-G4)

Rationale: Data transmitted from DSN is packetized and modulated onto DSN operating frequencies.

S/C-R7. The spacecraft shall generate at least TBD kilowatts of electrical power for use in data collection, storage, transmission, and other activities. (↓S/C-2.2)

Rationale: The collection, packetization, and modulation of data requires electrical power. We also expect that more functions that would require electrical power will be identified in further iterations of the design process.

Spacecraft (S/C) Design Constraints

S/C-C1. The spacecraft must be less than TBD kg in mass. (←DC1.2), (↓2.2), (→C&DH-C3, A&AC-C6, COM-C5)

Rationale: The launch vehicle cannot place the spacecraft into the proper orbit if it is greater than TBD kg in mass

S/C-C2. The spacecraft must fit within the payload fairing of the Delta-IVH (←DC1.2), (→C&DH-C2, A&AC-C1, COM-C1), (↓2.2)

Rationale: A payload fairing encapsulates the payload of the launch vehicle in order to create acceptable aerodynamic loads for flight through the Earth's atmosphere. The Delta-IVH is the selected launch vehicle for this mission.

S/C-C3. The spacecraft must have a capability to store at least TBD minutes worth of science data. (←PC1), (↓S/C-2.4)

Rationale: Depending on the spacecraft's orbit about the icy moon and the icy moon's orbit about the outer planet, the communications path from the spacecraft to the DSN could become occulted. Additionally, because other space exploration missions will be using the DSN and GN, immediate data transmission will not always be possible.

S/C-C4. The spacecraft must have a capability to execute directives generated by the Mission Operations Center. (←A3, S/C-G2), (↓2.4, S/C-2.1), (→C&DH-G2)

Rationale: Directives generated by humans and transmitted through the GN and DSN are the human control interface to the spacecraft. Such an interface is necessary given our assumption of current state of spacecraft automation technology and the possibility of unanticipated science data collection opportunities arising during the mission.

Spacecraft (S/C) Safety-Related Design Constraints

S/C-SC1. The spacecraft must have the necessary functionality for data acquisition at the required times. (←H1), (↓S/C-2.1, S/C-2.3, S/C-2.4), (→C&DH-G1, C&DH-ICA1, C&DH-ICA2, C&DH-ICA8, C&DH-ICA9, C&DH-ICA10, A&AC-ICA1, A&AC-ICA2, A&AC-ICA3, A&AC-ICA4)

S/C-SC2. The spacecraft must be able to return data at the required times. (←H2), (↓S/C-2.1, S/C-2.3, S/C-2.5, C&DH-2.1.2, C&DH-2.1.3), (→C&DH-G1, C&DH-ICA1, C&DH-ICA2, C&DH-ICA3, C&DH-ICA4, C&DH-ICA5, C&DH-ICA6, C&DH-ICA7, C&DH-ICA8, C&DH-ICA9, C&DH-ICA10, A&AC-ICA1, A&AC-ICA2, A&AC-ICA3, A&AC-ICA4, A&AC-ICA5, A&AC-ICA6, A&AC-ICA7, A&AC-ICA8, A&AC-ICA9)

S/C-SC3. All physical elements of the spacecraft must not unintentionally move along a collision course with an outer planet moon. (←H4), (↓S/C-2.1, S/C-2.3, SV-2), (→C&DH-G1, C&DH-ICA1, C&DH-ICA2, C&DH-ICA8, C&DH-ICA9, A&AC-R5, A&AC-ICA2, A&AC-ICA4)

S/C-SC4. All physical elements of the spacecraft that intentionally collide with an outer planet moon must be sterile. (←H4), (↓S/C-2.1, S/C-2.3, SV-2), (→C&DH-G1, A&AC-R5)

S/C-SC5. All physical elements of the spacecraft must not unintentionally move along a collision course with Earth. (←H5, H7), (↓S/C-2.1, S/C-2.3, SV-2), (→C&DH-G1, C&DH-ICA1, C&DH-ICA2, C&DH-ICA8, C&DH-ICA9, A&AC-ICA1, A&AC-ICA2, A&AC-ICA3, A&AC-ICA4)

S/C-SC6. All physical elements of the spacecraft that intentionally collide with the Earth must not cause damage to humans or human assets. (←H5, H7), (↓S/C-2.1, S/C-2.3, SV-1), (→C&DH-G1)

S/C-SC7. All physical elements of the spacecraft must not unintentionally move along a collision course with Earth life or human assets that are off of Earth (e.g., International Space Station). (←H6, H7), (↓S/C-2.1, S/C-2.3, SV-1), (→C&DH-G1, C&DH-ICA1, C&DH-ICA2, C&DH-ICA8, C&DH-ICA9, A&AC-ICA1, A&AC-ICA2, A&AC-ICA3, A&AC-ICA4)

Level 1.1.1: Spacecraft Command & Data Handling (C&DH) Goals, Requirements, and Constraints

Spacecraft Command & Data Handling (C&DH) Goals

C&DH-G1. To monitor the health and manage the interfaces of the following spacecraft-level functional elements: Electrical Power (EP), Attitude and Articulation Control (A&AC), Science Data Collection (SCI), and Communications Signal Processing (COM). (←S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC4, S/C-SC5, S/C-SC6, S/C-SC7), (↓S/C-2.1, S/C-2.2, S/C-2.3, S/C-2.4, S/C-2.5), (→C&DH-R1, C&DH-R2, C&DH-R3, C&DH-R4, C&DH-R5, C&DH-R6, C&DH-R7, C&DH-R8, C&DH-R9)

> *Rationale: A central concept in control and systems theory is that of hierarchy. By definition, control involves the imposition of constraints from one level of the control hierarchy to a lower level (Checkland, 1981)[2]. The C&DH functional element represents control on the spacecraft-level while the functional elements mentioned in this goal all control lower-level functions and need a higher-level controller to manage their interactions with each other.*

C&DH-G2. To receive and execute directives generated by the MOC. (←S/C-C4), (→C&DH-C1)

Spacecraft Command & Data Handling (C&DH) Requirements

C&DH-R1. The C&DH shall initiate and regulate electrical power generation on the spacecraft. (←C&DH-G1)

> *Rationale: Intelligence (human and/or artificial) is required to initiate power generation on the spacecraft. Humans will not have physical access to the power generation device(s) on the spacecraft once the spacecraft leaves the launch pad.*

[2] Peter Checkland (1981), *Systems Thinking, Systems Practice*, Chichester, UK: John Wiley and Sons Ltd

C&DH-R2. The C&DH shall initiate and terminate electrical power distribution to the A&AC as needed. (←C&DH-G1), (↓C&DH-2.1.7)

C&DH-R3. The C&DH shall initiate and terminate electrical power distribution to the SCI as needed. (←C&DH-G1)

C&DH-R4. The C&DH shall initiate and terminate electrical power distribution to its Spacecraft Health & Status Data storage, retrieval, evaluation, and packetization functional elements as needed. (←C&DH-G1)

C&DH-R5. The C&DH shall initiate and terminate electrical power distribution to the COM functional element as needed. (←C&DH-G1), (↓C&DH-2.1.4, C&DH-2.1.5)

C&DH-R6. The C&DH shall provide spacecraft translation directives to the A&AC in accordance with the needs of the COM and SCI functional elements. (←C&DH-G1), (↓C&DH-2.1.6, SV-1, SV-2)

C&DH-R7. The C&DH shall provide spacecraft attitude directives to the A&AC in accordance with the needs of the COM and SCI functional elements. (←C&DH-G1), (↓C&DH-2.1.6, SV-1, SV-2)

C&DH-R8. The C&DH shall transfer of packetized spacecraft health & status data to the COM functional element as needed. (←C&DH-G1), (↓C&DH-2.1.2)

C&DH-R9. The C&DH shall initiate and terminate the transfer of packetized science data between the SCI and COM functional elements as needed. (←C&DH-G1), (↓C&DH-2.1.3)

Spacecraft Command & Data Handling (C&DH) Design Constraints

C&DH-C1. The C&DH must be able to receive, store, and execute directives generated by the MOC and transmitted through the DSN and/or GN. (←C&DH-G2), (↓C&DH-2.1, C&DH-2.1.6)

C&DH-C2. All command and data handling components must fit within TBD% of the space beneath the payload fairing of a Delta-IVH. (←S/C-C2)

Rationale: Space is a limited resource inside the payload fairing of a launch vehicle and thus, space for each component of the spacecraft must be carefully budgeted. The space allocation process involves a number of architectural tradeoffs beyond the scope of this study. Therefore, we will use a TBD% space allocation to the command and data handling functional elements.

C&DH-C3. The combined mass of the C&DH functional elements must be less than TBD kg. (←S/C-C1)

Rationale: The launch vehicle cannot place the spacecraft into the proper orbit if it is greater than TBD kg in mass. Thus, the mass of each component of the spacecraft must be carefully budgeted. The mass allocation process involves a number of architectural tradeoffs beyond the scope of this study. Therefore, we will use a TBD mass allocation to the spacecraft command and data handling functional elements.

Spacecraft Command & Data Handling (C&DH) Safety-Related Design Constraints

C&DH-SC1. The C&DH must validate the time and state dependent assumptions of directives generated by the MOC (←H1, H2, H4, H5, H6, H7), (→C&DH-ICA6, C&DH-ICA7)

C&DH-SC2. In the absence of valid MOC Directives, the C&DH must initiate the proper functionality for reception of MOC Directives (←H1, H2, H4, H5, H6, H7), (↓C&DH-2.1.5)

C&DH-SC3. The communications path between the C&DH and COM functional elements for the transfer of Spacecraft H&S Data must not become broken or obstructed. (←H2)

C&DH-SC4. The C&DH must be able to initiate communications with the GN or DSN in the event that the MOC Directives become obsolete. (←H2), (→C&DH-ICA5)

C&DH-SC5. The communications path between the C&DH and SCI functional elements for transmission of the Send Science Data to COM directive must not become broken or obstructed. (←H2)

C&DH-SC6. The communications path between the C&DH and EP for transmission of the 'Power Up COM Transmit' directive must not become broken or obstructed. (←H2)

C&DH-SC7. The C&DH must be able to initiate power transfer between the EP and COM functional elements in the events that the COM Transmit function has been powered down and/or the MOC Directives become obsolete. (←H2)

C&DH-SC8. The C&DH must not attempt to initiate data transfer between the SCI and COM functional elements before power transfer has been initiated between the EP and COM Transmit elements. (←H2)

C&DH-SC9. The C&DH must not terminate power transfer between the EP and COM Transmit functional elements during a period of data transmission unless other safety considerations make such an action necessary. (←H2)

Rationale: It may be necessary at some point to temporarily power down the COM subsystem in order to avoid long-term damage to the COM system. While in such instances, a small amount a data might be lost, the losses associated with maintaining power transfer to the COM subsystem could be much more severe.

C&DH-SC10. The C&DH must provide directives to the A&AC that do not place the direction of Earth outside of the HGA's allowable range of articulation and translation. (←H1, H2, H4, H5, H6, H7), (↓SV-2)

C&DH-SC11. During times of simultaneous communication with the DSN or GN and science data collection, the C&DH must provide directives to the A&AC that do not degrade either function. (←H1, H2), (↓A&AC-2.1, A&AC-2.2)

Level 1.1.2: Spacecraft Electrical Power (EP) Goals, Requirements, and Constraints

Further specification of this functional element is beyond the scope of this study.

Level 1.1.3: Spacecraft Attitude and Articulation Control (A&AC) Goals, Requirements, and Constraints

Spacecraft Attitude and Articulation Control (A&AC) Goals

A&AC-G1. To provide the spacecraft velocity changes necessary for orbit insertion about the icy moon of the outer planet, maintenance of/changes to that orbit, and spacecraft disposal. (←S/C-R1), (↓2.2, S/C-2.3, C&DH-2.1.6, SV-1, SV-2), (→A&AC-R1, A&AC-R2, A&AC-R3, A&AC-R4, A&AC-R5),

Rationale: Because our functional analysis has shown tight coupling between spacecraft attitude and spacecraft velocity changes, we have allocated these functions to one functional element, the A&AC. However, in order to avoid confusion, it is worth noting that traditionally, spacecraft velocity changes have been allocated to a separate "Propulsion" functional element or subsystem in JPL spacecraft.

A&AC-G2. To point the spacecraft and spacecraft elements in accordance with science data collection and communications needs for the mission. (↓S/C-2.3, C&DH-2.1.6, SV-1, SV-2), (→A&AC-R6, A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10)

Rationale: The pointing of the spacecraft and spacecraft elements are both allocated to the A&AC functional element because the rotation and translation of spacecraft elements with respect to the main spacecraft structure will affect spacecraft attitude.

Spacecraft Attitude and Articulation Control (A&AC) Assumptions

A&AC-A1. Telescoping boom segments for the HGA are not practical for this mission. (↓A&AC-2.2.1)

Rationale: While this assumption is largely a simplifying assumption, the complexity associated with telescoping boom segments for an object as massive as the HGA would warrant a trade study beyond the scope of this study if they were to be considered.

A&AC-A2. Four or more HGA boom joints are not practical for this mission. (↓A&AC-2.2.1)

Rationale: While this assumption is largely a simplifying assumption, the complexity associated with four or more boom joints would warrant a trade study beyond the scope of this study if they were to be considered.

Spacecraft Attitude and Articulation Control (A&AC) Requirements

A&AC-R1. After release from the launch vehicle, the A&AC shall provide spacecraft velocity changes for spacecraft transit from the release point to the orbit of the outer planet. (←A&AC-G1), (↓A&AC-2.6, SV-1, SV-2)

A&AC-R2. Upon arrival to the orbit of the outer planet, the A&AC shall provide spacecraft velocity changes necessary for spacecraft capture in the orbit of the outer planet. (←A&AC-G1), (↓A&AC-2.6, SV-1)

A&AC-R3. After capture in the orbit of the outer planet, the A&AC shall provide the spacecraft velocity changes necessary for orbit insertion about the icy moon of the outer planet. (←A&AC-G1), (↓A&AC-2.6, SV-1)

A&AC-R4. After orbit insertion about the icy moon, the A&AC shall provide the spacecraft velocity changes necessary for orbit maintenance for at least TBD days. (←A&AC-G1), (↓A&AC-2.6, SV-1)

A&AC-R5. At the conclusion of the mission, the A&AC shall provide the spacecraft velocity changes necessary for disposal of the spacecraft. (←A&AC-G1, S/C-SC3, S/C-SC4), (↓A&AC-2.6, SV-1)

A&AC-R6. The A&AC shall provide pointing of the main spacecraft structure to TBD degrees. (←A&AC-G2), (↓A&AC-2.5, SV-1, SV-2)

A&AC-R7. The A&AC shall articulate all necessary antennas relative to the main spacecraft structure as needed for radiation of modulated data and carrier signal to the GN. (←A&AC-G2), (↓A&AC-2.1, A&AC-2.2)

A&AC-R8. The A&AC shall articulate all necessary antennas relative to the main spacecraft structure as needed for radiation of modulated data and carrier signal to the DSN. (←A&AC-G2), (↓A&AC-2.1, A&AC-2.2)

A&AC-R9. The A&AC shall articulate all necessary antennas relative to the main spacecraft structure as needed for reception of signals radiated from the GN. (←A&AC-G2), (↓A&AC-2.1, A&AC-2.2)

A&AC-R10. The A&AC shall articulate all necessary antennas relative to the main spacecraft structure as needed for reception of signals radiated from the DSN. (←A&AC-G2), (↓A&AC-2.1, A&AC-2.2)

Spacecraft Attitude and Articulation Control (A&AC) Design Constraints

A&AC-C1. All attitude and articulation control components must fit within TBD% of the space beneath the payload fairing of a Delta-IVH. (←S/C-C2), (→AC&DH-C1), (↓A&AC-2.2.1)

Rationale: Space is a limited resource inside the payload fairing of a launch vehicle and thus, space for each component of the spacecraft must be carefully budgeted. The space allocation process involves a number of architectural tradeoffs beyond the scope of this study. Therefore, we will use a TBD% space allocation to the attitude and articulation control functional elements.

A&AC-C2. The A&AC functional element must be able to receive and execute directives from the C&DH functional element. (←A&AC-G2), (↓C&DH-2.1.6), (→AC&DH-G2)

A&AC-C3. The A&AC functional element must provide HGA Pointing State Information to the C&DH functional element as an input. (↓C&DH-2.1.6.1, A&AC-2.1.2, A&AC-2.2.1.5), (→AC&DH-G3)

A&AC-C4. The A&AC functional element must provide HGA Translation State Information to the C&DH functional element as an input. (↓C&DH-2.1.6.2, A&AC-2.2.2, A&AC-2.2.1.5), (→AC&DH-G3)

A&AC-C5. The A&AC functional element must be able to receive power from the EP functional element. (↑C&DH-2.1.7), (↓A&AC-2.7)

A&AC-C6. The combined mass of the A&AC functional elements must be less than TBD kg. (←S/C-C1), (→AC&DH-C2, HA&T-C1)

Rationale: The launch vehicle cannot place the spacecraft into the proper orbit if it is greater than TBD kg in mass. Thus, the mass of each component of the spacecraft must be carefully budgeted. The mass allocation process involves a number of architectural tradeoffs beyond the scope of this study. Therefore, we will use a TBD mass allocation to the spacecraft attitude and articulation functional elements.

Spacecraft Attitude and Articulation Control (A&AC) Safety-Related Design Constraints

A&AC-SC1. The HGA must not rotate or translate with respect to the main spacecraft structure while the spacecraft is inside the payload fairing of the launch vehicle. (←H1, H2, H5, H6, H7), (↓A&AC-2.2.1.4, A&AC-2.2.1.8, A&AC-2.3, A&AC-2.4), (→A&AC-ICA10, A&AC-ICA11, AC&DH-G1, HA&T-G1, HA&T-G2, HA&T-G3)

A&AC-SC2. HGA translation and rotation with respect to the main spacecraft structure must be restrained during periods of spacecraft velocity changes so that the HGA does not deform and/or detach from the spacecraft due to inertial loads. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.2.1.4, A&AC-2.3, A&AC-2.4), (→AC&DH-G1, HA&T-G1, HA&T-G2, HA&T-G3)

A&AC-SC3. While translating and/or rotating, the HGA and the radiation it emits must maintain minimum separation from other parts of the spacecraft. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.2.1.5, A&AC-2.3, A&AC-2.4, AC&DH-2.1.2, A&AC-2.2.1.9), (→A&AC-ICA10, A&AC-ICA11, AC&DH-G1, HA&T-G1, HA&T-G2)

A&AC-SC4. The communications paths between the A&AC functional element and the C&DH for transfer of the HGA Pointing State Information and HGA Translation State Information inputs must not become broken or obstructed. (←H2), (↓A&AC-2.3), (→AC&DH-G1, HA&T-G1, HA&T-G2)

A&AC-SC5. Transfer of the HGA Pointing State Information and HGA Translation State Information between the A&AC and C&DH must take no longer than TBD micro-seconds. (←H2), (↓A&AC-2.3, A&AC-2.4), (→AC&DH-G1, HA&T-G1, HA&T-G2)

A&AC-SC6. The HGA Pointing State Information and HGA Translation State Information inputs to the C&DH must be updated every TBD seconds. (←H2), (↓A&AC-2.2.1.5, A&AC-2.3, A&AC-2.4), (→AC&DH-G1, AC&DH-C4, HA&T-G1, HA&T-G2)

A&AC-SC7. Mechanical disturbances to the HGA must not create rotational or translational oscillations of the HGA that are large enough to prevent data return. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.3, A&AC-2.4 SV-3, SV-5, SV-6, SV-10, SV-14), (→A&AC-ICA10, AC&DH-G1, AC&DH-C4, HA&T-G1, HA&T-G2, HA&T-G3)

A&AC-SC8. A command must be sent to disengage the HGA Boom Joint Rotation Locks at the desired HGA Boom deployment time (i.e., after separation of the launch vehicle payload fairing) or any time in which rotation of a locked degree of freedom is desired. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.3, A&AC-2.4, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42), (→AC&DH-G1, HA&T-G3)

A&AC-SC9. Power must be provided to all HGA Boom Joint Rotation Locks at the desired times of lock disengagement. (←H2), (↓A&AC-2.3, A&AC-2.7, SV-43, SV-44, SV-45, SV-46, SV-47, SV-48), (→AC&DH-G1)

A&AC-SC10. The HGA Boom Joint Rotation Locks must receive and respond to a disengagement command within TBD milliseconds. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.3, A&AC-2.4, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42), (→AC&DH-G1, HA&T-G3)

A&AC-SC11. All rotation joints must not jam along a rotational degree of freedom. (←H2), (↓SV-8, SV-9, SV-12, SV-13, SV-16, SV-17)

A&AC-SC12. The power supply to the HGA Boom Rotation Joint Motors must not be interrupted for greater than a TBD second interval unless the HGA Boom Rotation Joint Locks engage within TBD seconds. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.3, A&AC-2.4, A&AC-2.7, SV-31, SV-32, SV-33, SV-34, SV-35, SV-36), (→AC&DH-G1, HA&T-G3)

Rationale: If an HGA Boom Rotation Joint Motor loses power and the lock on the corresponding degree of freedom does not engage, the only resistance to mechanical disturbances will be the rotational inertia of the joint and the HGA/HGA Boom mass downstream of it.

A&AC-SC13. The HGA Boom Rotation Joint Motors must not slip more than TBD radians/revolution with respect to the joints. (←H2), (↓SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)

A&AC-SC14. The process model of the controller of the HGA Boom Rotation Joint Motors must explicitly or implicitly account for time delays in the motor actuation, joint friction, slippage, partial disengagement of the joint rotation locks, inertial loads from spacecraft velocity changes, other physical effects on joint rotation, and changes thereof. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.3, A&AC-2.4, A&AC-2.2.1.12, SV-31, SV-32, SV-33, SV-34, SV-35, SV-36, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42), (→AC&DH-G1, HA&T-G2, HA&T-G3)

Rationale: Note that even a PID control law implicitly accounts for the effects mentioned in the constraint by altering the control effort in response to proportion, changes, and the summation of pointing error over time.

A&AC-SC15. The spacecraft velocity must not change by more than TBD m/s^2 along an axis perpendicular to the axis of the deployed boom and TBD m/s^2 along an axis parallel to the axis of the deployed boom unless all rotation can be locked along all HGA Boom rotational degrees of freedom. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.3, A&AC-2.4, A&AC-2.5, A&AC2.6, SV-1, SV-2, SV-31, SV-32, SV-33, SV-34, SV-35, SV-36, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42), (→AC&DH-G1, HA&T-G3)

Rationale: If spacecraft accelerations exceed these values, the inertial loads created at the HGA Boom joints will overpower the HGA Boom Rotation Joint Motors as they try to null them. The ensuing rotation could potentially cause a violation of minimum separation between the HGA, HGA Boom, or HGA radiation and other parts of the spacecraft.

A&AC-SC16. The HGA Boom Rotation Joint motor controller must not receive a control input (goal) that would violate minimum separation between the HGA boom, HGA, or HGA radiation and the rest of the spacecraft. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.1.2, A&AC-2.3, A&AC-2.4), (→AC&DH-G1, HA&T-G1)

A&AC-SC17. The HGA Boom Rotation Joint Locks must be able to counteract all torques on the rotation joints when they are engaged. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.2.1.10, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

A&AC-SC18. The HGA Boom Angle Encoders must provide HGA Boom Rotation Joint angles to the HGA Boom Rotation Joint Motors every TBD seconds. (←H1, H2, H4, H5, H6, H7), (→AC&DH-G1, HA&T-G1)

A&AC-SC19. The HGA Boom Rotation Joint Motor controllers must account for HGA Boom Rotation Joint Angle Encoder measurement errors. (←H1, H2, H4, H5, H6, H7), (→AC&DH-G1, HA&T-G1), (↓A&AC-2.2.1.11, AC&DH-2.1.2.3, AC&DH-2.1.2.4, AC&DH-2.1.2.5)

Level 1.1.3.1: Spacecraft Attitude and Articulation Command and Data Handling (AC&DH) Goals, Requirements, and Constraints

Spacecraft Attitude and Articulation Control C&DH (AC&DH) Goals

AC&DH-G1. To monitor the health and manage the interfaces of the following A&AC-level functional elements. HGA Attitude & Translation (HA&T) Controller, A&AC Electrical Power (AEP), Spacecraft Attitude Controller (AC), and Spacecraft Translation Controller (TC). (←A&AC-SC1, A&AC-SC2, A&AC-SC3, A&AC-SC4, A&AC-SC5, A&AC-SC6, A&AC-SC7, A&AC-SC8, A&AC-SC9, A&AC-SC10, A&AC-SC12, A&AC-SC14, A&AC-SC15, A&AC-SC16, A&AC-SC18, A&AC-SC19), (↓A&AC-2.2.1.11, A&AC-2.3, A&AC-2.4, A&AC-2.5, A&AC-2.6, A&AC-2.7), (→AC&DH-R1, AC&DH-R2, AC&DH-R3, AC&DH-R4, AC&DH-R5)

Rationale: A central concept in control and systems theory is that of hierarchy. By definition, control involves the imposition of constraints from one level of the control hierarchy to a lower level (Checkland, 1981). The AC&DH functional element represents control on the A&AC-level while the other functional elements mentioned in this design principle all control lower level functions and need a higher-level controller to manage their interactions with each other.

AC&DH-G2. To receive and execute directives from the Spacecraft C&DH. (←A&AC-C2), (→AC&DH-C3)

AC&DH-G3. To provide necessary state information to the Spacecraft C&DH (←A&AC-C3, A&AC-C4), (→AC&DH-C4)

Spacecraft Attitude and Articulation Control C&DH (AC&DH) Requirements

AC&DH-R1. The AC&DH shall initiate and terminate electrical power distribution to the HA&T as needed. (←AC&DH-G1)

AC&DH-R2. The AC&DH shall provide spacecraft attitude directives to the AC in accordance with the needs and state of the HA&T. (←AC&DH-G1), (↓SV-1, SV-2)

AC&DH-R3. The AC&DH shall provide spacecraft translation directives to the TC in accordance with the needs and state of the HA&T. (←AC&DH-G1), (↓SV-1, SV-2)

AC&DH-R4. The AC&DH shall provide HGA articulation directives to the HA&T in accordance with the needs and state of the AC. (←AC&DH-G1), (↓AC&DH-2.1.1), (→HA&T-C3)

AC&DH-R5. The AC&DH shall provide HGA articulation directives to the HA&T in accordance with the needs and state of the TC. (←AC&DH-G1), (↓AC&DH-2.1.1), (→HA&T-C3)

AC&DH-R6. The AC&DH shall derive 'Expected Sun Angles with respect to the HGA Center' and provide them to the HA&T every TBD seconds. (←AC&DH-G1), (→HA&T-C7)

Rationale: The AC&DH is the lowest-level controller with access to estimated state information on spacecraft position with respect to the Sun, spacecraft attitude, and HGA Boom Rotation Joint Angles. All of this state information is necessary to

Spacecraft Attitude and Articulation Control C&DH (AC&DH) Constraints

AC&DH-C1. All AC&DH components must fit within TBD% of the space beneath the payload fairing of a Delta-IVH. (←A&AC-C1)

Rationale: Space is a limited resource inside the payload fairing of a launch vehicle and thus, space for each component of the spacecraft must be carefully budgeted. The space allocation process involves a number of architectural tradeoffs beyond the scope of this study. Therefore, we will use a TBD% space allocation to the AC&DH functional elements.

AC&DH-C2. The combined mass of the AC&DH functional elements must be less than TBD kg. (←A&AC-C6)

Rationale: The launch vehicle cannot place the spacecraft into the proper orbit if it is greater than TBD kg in mass. Thus, the mass of each component of the spacecraft must be carefully budgeted. The mass allocation process involves a number of architectural tradeoffs beyond the scope of this study. Therefore, we will use a TBD mass allocation to the A&AC command and data handling functional elements.

AC&DH-C3. The AC&DH must be able to receive, store, evaluate, and execute directives generated by the C&DH (←AC&DH-G2), (↓AC&DH-2.1.1, AC&DH-2.1.2)

AC&DH-C4. The AC&DH must update HGA Pointing State Information and HGA Translation State Information inputs to the C&DH every TBD seconds. (←A&AC-SC6, AC&DH-G3), (→HA&T-C2), (↓AC&DH-2.1.3)

Spacecraft Attitude and Articulation Control C&DH (AC&DH) Safety-Related Design Constraints

Further specification of this functional element is beyond the scope of this study.

Level 1.1.3.2: Spacecraft HGA Attitude and Translation (HA&T) Controller Goals, Requirements, and Constraints

HGA Attitude and Translation (HA&T) Controller Goals

HA&T-G1. To infer HGA Translation and Rotation states from HGA boom joint pitch and roll encoder measurements. (←A&AC-SC1, A&AC-SC2, A&AC-SC3, A&AC-SC5, A&AC-SC6, A&AC-SC7, A&AC-SC16, A&AC-SC18, A&AC-SC19), (↓A&AC-2.2.1.5, A&AC-2.2.1.11, A&AC-2.2.1.12, A&AC-2.4), (→HA&T-R1, HA&T-C4, HA&T-C5, HA&T-C6)

HA&T-G2. To create pitch and roll rotation in the HGA boom joints (i.e., shoulder, elbow and wrist) as needed. (←A&AC-SC1, A&AC-SC2, A&AC-SC3, A&AC-SC4, A&AC-SC7, A&AC-SC14), (↓A&AC-2.2.1, A&AC-2.2.1.4, A&AC-2.4), (→HA&T-R2)

HA&T-G3. To restrain pitch and roll rotation in the HGA boom joints (i.e., shoulder, elbow, and wrist) as needed. (←A&AC-SC1, A&AC-SC2, A&AC-SC7, A&AC-SC8, A&AC-SC10, A&AC-SC12, A&AC-SC14, A&AC-SC15), (↓A&AC-2.2.1.5, A&AC-2.4), (→HA&T-R3, HA&T-R4, HA&T-R5)

HGA Attitude and Translation (HA&T) Controller Requirements

HA&T-R1. The HA&T shall infer the state of each HGA boom rotation joint degree of freedom every TBD seconds. (←HA&T-G1), (↓HA&T-2.1)

HA&T-R2. The HA&T shall direct HGA boom rotation joint motor actuation in accordance with AC&DH directives and the HA&T's inference of HGA boom rotation state. (←HA&T-G2, HA&T-R1), (↓HA&T-2.3, SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)

HA&T-R3. The HA&T shall infer the state of each HGA boom joint rotation lock every TBD seconds. (←HA&T-G3), (↓HA&T-2.2)

HA&T-R4. The HA&T shall engage/maintain engagement of the HGA boom joint rotation locks while the spacecraft is within the payload fairing of the launch vehicle and the time period between payload fairing separation and HGA deployment. (←HA&T-G3), (↓HA&T-2.3, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

HA&T-R5. The HA&T shall engage/maintain engagement of HGA boom joint rotation locks as needed during spacecraft velocity changes. (←HA&T-G3), (↓HA&T-2.3, HA&T-2.4, HA&T-2.5, SV-1, SV-2, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

HGA Attitude and Translation (HA&T) Controller Constraints

HA&T-C1. The combined mass of the HA&T functional elements must be less than TBD kg. (←A&AC-C6)

> *Rationale: The launch vehicle cannot place the spacecraft into the proper orbit if it is greater than TBD kg in mass. Thus, the mass of each component of the spacecraft must be carefully budgeted. The mass allocation process involves a number of architectural tradeoffs beyond the scope of this study. Therefore, we will use a TBD mass allocation to the HA&T functional elements.*

HA&T-C2. The HA&T must send a HGA boom joint rotation state information to the AC&DH every TBD seconds. (←AC&DH-C4), (↓AC&DH-2.1.3)

HA&T-C3. The HA&T functional element must be able to receive and execute directives from the AC&DH functional element. (←AC&DH-R4, AC&DH-R5), (↓HA&T-2.1)

HA&T-C4. The HA&T functional element must be able to receive measurements from the HGA Boom Rotation Joint Angle Encoders every TBD seconds. (←HA&T-G1), (↓HA&T-2.1)

HA&T-C5. The HA&T functional element must be able to receive measurements from the HGA Sun Sensor every TBD seconds. (←HA&T-G1)

HA&T-C6. The HA&T functional element must be able to receive measurements from the HGA Boom Rotation Joint Lock Sensors every TBD seconds. (←HA&T-G1), (↓HA&T-2.2)

HA&T-C7. The HA&T functional element must be able to receive 'Expected Sun Angles with Respect to the HGA Center' directive from the AC&DH every TBD seconds. (←AC&DH-R6, HA&T-G1)

Level 1.1.3.3: Spacecraft Attitude Controller (AC) Goals, Requirements, and Constraints

Further specification of this functional element is beyond the scope of this study.

Level 1.1.3.4: Spacecraft Translation Controller (TC) Goals, Requirements, and Constraints

Further specification of this functional element is beyond the scope of this study.

Level 1.1.3.5: Spacecraft A&AC Electrical Power (AEP) Goals, Requirements, and Constraints

Further specification of this functional element is beyond the scope of this study.

Level 1.1.4: Spacecraft Science Data Collection (SCI) Goals, Requirements, and Constraints

Further specification of this functional element is beyond the scope of this study.

Level 1.1.5: Spacecraft Communications Signal Processing (COM) Goals, Requirements, and Constraints

Spacecraft Communications Signal Processing (COM) Goals

COM-G1. To process (i.e., modulate, etc.) packetized spacecraft data to be sent to Earth onto GN operating frequencies and radiate it in the direction of the GN. (←S/C-R3), (↓S/C-2.5), (→COM-R1, COM-R5)

COM-G2. To process (i.e., demodulate, etc.) data from signals received from the GN. (←S/C-R4), (↓S/C-2.5), (→COM-R3, COM-R5)

COM-G3. To process (i.e., modulate, etc.) packetized spacecraft data to be sent to Earth onto DSN operating frequencies and radiate it in the direction of the DSN. (←S/C-R5), (↓S/C-2.5), (→COM-R2, COM-R6)

COM-G4. To process (i.e., demodulate, etc.) data from signals received from the DSN. (←S/C-R6), (↓S/C-2.5), (→COM-R4, COM-R6)

Spacecraft Communications Signal Processing (COM) Assumptions

COM-A1. The space allocation for a parabolic antenna while within the payload fairing of the launch vehicle is 3 meters diameter. (←COM-C1), (↓COM-2.1.2)

> *Rationale: Space is a limited resource inside the payload fairing of a launch vehicle and thus, space for each component of the spacecraft must be carefully budgeted. The space allocation process involves a number of architectural tradeoffs beyond the scope of this study. Therefore, we will use a maximum antenna size corresponding to the antenna size selected in (Clark, 2007).*

COM-A2. While the antenna is in the payload fairing it is not practical for this mission to stow the antenna in any shape other than its final parabolic shape. (↓COM-2.1.2)

> *Rationale: Stowing a parabolic antenna in a non-parabolic shape while it is in the launch vehicle and then deploying it to a parabolic shape will allow for a larger deployed antenna diameter. However, the effects on antenna efficiency and added risk of antenna deployment are assumed to largely outweigh the benefits derived from stowing the antenna in a non-parabolic shape. The trade study implied in this assumption is beyond the scope of this study. Thus, the assumption above is the most conservative outcome of the trade study.*

Spacecraft Communications Signal Processing (COM) Requirements

COM-R1. The COM functional element shall modulate packetized spacecraft data for transmission to the GN onto carrier frequencies ranging from TBD GHz to TBD GHz. (←COM-G1)

COM-R2. The COM functional element shall modulate packetized spacecraft data for transmission to the DSN onto carrier frequencies ranging from TBD GHz to TBD GHz. (←COM-G3)

COM-R3. The COM functional element shall demodulate data from signals sent by the GN (carrier frequencies of these signals range from TBD GHz to TBD GHz). (←COM-G2)

COM-R4. The COM functional element shall demodulate data from signals sent by the DSN (carrier frequencies of these signals range from TBD GHz to TBD GHz). (←COM-G4)

COM-R5. The COM functional element shall radiate the modulated spacecraft data at frequencies ranging from TBD GHz to TBD GHz. (←COM-G1, COM-G2), (↓COM-2.1)

COM-R6. The COM functional element shall absorb radiated signals from the DSN and/or GN and convert them into electrical signals. (←COM-G3, COM-G4), (↓COM-2.1)

Spacecraft Communications Signal Processing (COM) Design Constraints

COM-C1. All communications signal-processing components must fit within TBD% of the space beneath the payload fairing of a Delta-IVH. (←S/C-C2), (→COM-A1), (↓COM-2.1.2)

Rationale: Space is a limited resource inside the payload fairing of a launch vehicle and thus, space for each component of the spacecraft must be carefully budgeted. The space allocation process involves a number of architectural tradeoffs beyond the scope of this study. Therefore, we will use a TBD% space allocation to the communications functional elements.

COM-C2. The COM functional element must be able to receive packetized H&S data from the C&DH functional element. (↓C&DH-2.1.2)

COM-C3. The COM functional element must be able to receive power from the EP functional element. (↓C&DH-2.1.4)

COM-C4. The COM functional element must be able to receive packetized science data from the SCI functional element. (↓C&DH-2.1.3)

COM-C5. The combined mass of the COM functional elements must be less than TBD kg. (←S/C-C1)

Rationale: The launch vehicle cannot place the spacecraft into the proper orbit if it is greater than TBD kg in mass. Thus, the mass of each component of the spacecraft must be carefully budgeted. The mass allocation process involves a number of architectural tradeoffs beyond the scope of this study. Therefore, we will use a TBD mass allocation to the spacecraft communications signal processing functional elements.

Spacecraft Communications Subsystem (COM) Safety-Related Design Constraints

Further specification of this functional element is beyond the scope of this study.

Level 1.2: Deep Space Network (DSN) Goals, Requirements, and Constraints

Further specification of this functional element is beyond the scope of this study.

Level 1.3: Launch Vehicle (L/V) Goals, Requirements, and Constraints

Further specification of this functional element is beyond the scope of this study.

Level 1.4: Mission Operations Center (MOC) Goals, Requirements, and Constraints

Mission Operations Center (MOC) Goals

MOC-G1. To issue directives to the spacecraft in accordance with mission goals. (←SC1, SC2, SC3, SC4, SC5, SC6, SC7, SC8, SC9), (↓2.1, 2.4)

MOC-G2. To issue directives to the DSN in accordance with mission goals. (←SC1, SC2, SC3, SC4, SC5, SC6, SC7, SC8, SC9), (↓2.3, 2.4)

MOC-G3. To issue directives to the Launch Vehicle in accordance with mission goals. (←SC1, SC2, SC3, SC4, SC5, SC6, SC7, SC8, SC9), (↓2.2, 2.4)

MOC-G4. To issue directives to the GN in accordance with mission goals. (←SC1, SC2, SC3, SC4, SC5, SC6, SC7, SC8, SC9), (↓2.4, 2.5)

Level 1.5: NASA Ground Network (GN) Goals, Requirements, and Constraints

Further specification of this functional element is beyond the scope of this study.

Level 2: System Design

System Design Decisions

2.1. A new spacecraft will be used for data collection (↑HLR1, HLR2, HLR3, HLR4, HLR5, DC1, SC1, SC2, SC3, SC4, SC5, SC6, SC7, SC8, SC9, A1, A2, MOC-G1), (→2.2, 2.3, 2.4, 2.5, S/C-2.1, SV-1, SV-2)

Rationale: The data cannot be collected from Earth's surface or orbit. Additionally, no existing spacecraft design will be able to accomplish the mission goals

S/C-2.1. The interfaces of the spacecraft-level functional elements are monitored and managed by a spacecraft command and data handling (C&DH) functional element that translates directives generated by the MOC (after they have been transmitted through the GN or DSN and demodulated) into directives for other functional elements after evaluating if the conditions for the directives are satisfied. (↑S/C-C4, S/C-R3, S/C-R5, S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC4, S/C-SC5, S/C-SC6, S/C-SC7, C&DH-G1), (←2.1)

Rationale: A central concept in control and systems theory is that of hierarchy. By definition, control involves the imposition of constraints from one level of the control hierarchy to a lower level (Checkland, 1981). The C&DH functional element represents control on the spacecraft-level while the other functional elements mentioned in this design principle all control lower level functions and need a higher level controller to manage their interactions with each other.

C&DH-2.1. The C&DH receives MOC Directives as an input (routed through the COM functional element), evaluates them for consistency with spacecraft state, and executes the necessary tasks and/or delegates them to the appropriate functional elements. (↑C&DH-C1, C&DH-ICA1, C&DH-ICA2), (←S/C-2.1)

C&DH-2.1.1. The C&DH delegates tasks in the MOC Directives related directly to the transfer of data between the spacecraft, DSN, and GN to the COM functional elements.

C&DH-2.1.2. When spacecraft health and status data transmission to the DSN or GN is to occur, the C&DH sends Spacecraft H&S Data to the COM functional element. (↑S/C-SC2, C&DH-R8, COM-C2, C&DH-ICA3)

C&DH-2.1.3. When science data transmission to the DSN or GN is to occur, the C&DH sends the 'Send Science Data to COM' directive to the SCI functional element. (↑S/C-SC2, C&DH-R9, COM-C4, C&DH-ICA4)

C&DH-2.1.4. When Spacecraft H&S Data and Science Data transmission to the DSN or GN is to occur, the C&DH sends the 'Power Up COM Transmit' directive and 'Power Down COM Transmit' directives to the EP functional element. (↑C&DH-R5, COM-C3, C&DH-ICA5, C&DH-ICA6, C&DH-ICA7)

C&DH-2.1.5. The C&DH automatically sends the 'Power Up COM Receive' directive to the EP functional element:

1. TBD seconds after the spacecraft is deployed from the launch vehicle.
2. TBD seconds after a 'Power Down COM Receive' directive is sent to the EP functional element.
3. TBD seconds after an undirected power down of the COM Receive functional element is detected.

(↑C&DH-SC2, C&DH-R5)

Rationale: If the COM functional element's receive function is unpowered, humans (i.e., the MOC) will not be able to update MOC Directives or otherwise interface with the spacecraft until the C&DH automatically sends the 'Power Up COM Receive' directive. Note this design principle means that the COM Receive function will never be powered down for more than TBD seconds

C&DH-2.1.6. The C&DH provides attitude and translation directives to the A&AC functional element in accordance with SCI and COM subsystem needs and MOC Directives. (↑C&DH-R6, C&DH-R7, C&DH-C1, A&AC-C2), (→SV-1, SV-2)

C&DH-2.1.6.1. The C&DH receives a 'HGA Pointing' State Information input from the A&AC functional element and uses this information to update directives for the A&AC and the A&AC health and status data. (←A&AC-2.1.2, A&AC-2.2), (↑A&AC-C3, C&DH-ICA8)

C&DH-2.1.6.2. The C&DH receives a 'HGA Translation' State Information input from the A&AC functional element and uses this information to update directives for the A&AC and A&AC health and status data. (←A&AC2.2.2), (↑A&AC-C4, C&DH-ICA9)

C&DH-2.1.6.3. The C&DH receives a 'Science Data Collection' State Information input from the SCI functional element and uses this information to update directives for the A&AC and SCI health and status data. (↑C&DH-ICA10)

C&DH-2.1.7. The C&DH initiates electrical power distribution to the A&AC by sending the 'Power Up A&AC' directive to the EP functional element. (↑C&DH-R2, A&AC-C5)

S/C-2.2. An electrical power functional element on the spacecraft generates and distributes electrical power to the spacecraft functional elements. (↑S/C-R7, C&DH-G1)

S/C-2.3. An attitude and articulation control functional element on the spacecraft controls spacecraft pointing and translation and the articulation of spacecraft elements with respect to the main spacecraft structure. (↑S/C-R1, S/C-R3, S/C-R5, S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC4, S/C-SC5, S/C-SC6, S/C-SC7, C&DH-G1, A&AC-G1, A&AC-G2), (→A&AC-2.1)

Rationale: Spacecraft attitude and translation control is coupled. The orientation of translation mechanisms on the spacecraft (e.g., thrusters) affects the change in the direction of translation produced by these mechanisms. While it can be possible to rotate these mechanisms with respect to the overall spacecraft orientation, this rotation would be limited in range and thus, pointing of the spacecraft as a whole would be necessary at some point. Also, rotation and translation of spacecraft elements with respect to the main spacecraft structure will affect spacecraft attitude.

A&AC-2.1. The A&AC functional element rotates the HGA relative to the main structure of the spacecraft. (↑A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, C&DH-SC11, A&AC-ICA1, A&AC-ICA2), (→A&AC-2.2, AC&DH-2.1.2, A&AC-2.4, COM-2.1, SV-15, SV-18)

Rationale: Having the HGA articulate relative to the spacecraft decouples antenna pointing from science data collection. If the HGA were spacecraft-fixed, the spacecraft as a whole would have to rotate, possibly altering science data collection instrument pointing (which is essential to satisfactory data collection).

A&AC-2.1.1. Electrical power is used to rotate the HGA with respect to the main spacecraft structure. (→A&AC-2.2.1, SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)

Rationale: Because the spacecraft has a source of electric power (the EP), the rotation function can be provided without adding additional energy conversion processes (such as those that would be required for a hydraulic system) to spacecraft operation. Additionally, electric motor technology in spacecraft applications is mature.

A&AC-2.1.2. The A&AC functional element sends the HGA Pointing State Information input to the C&DH every TBD seconds. (↑A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, A&AC-C3, A&AC-ICA3, A&AC-ICA4), (→AC&DH-2.1.2, A&AC-2.4)

Rationale: The C&DH requires this information for determining directives for the A&AC.

A&AC-2.2. The A&AC functional element translates the HGA relative to the main spacecraft structure. (←A&AC-2.1), (↑A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, C&DH-SC11, A&AC-ICA3, A&AC-ICA4), (→SV-4, SV-7, SV-11, SV-15)

Rationale: Translating (or deploying) the HGA away from the main spacecraft structure allows for a wider range of rotation of the HGA (i.e., it distances the HGA from other parts of the spacecraft that it could collide with). It also distances the HGA from potential EMI noise sources in the main spacecraft structure.

A&AC-2.2.1. The HGA boom consists of 3 rotation joints (shoulder, elbow, and wrist) driven by TBD electric motors and connected by 2 solid (i.e., non-telescoping) boom segments. (↑A&AC-A1, A&AC-A2, A&AC-C1, HA&T-G2), (←A&AC-2.1.1)

A&AC-2.2.1.1. Each rotation joint has two rotational degrees of freedom: roll and pitch. (→A&AC-2.2.1.3, A&AC-2.2.1.5, A&AC-2.2.1.6, A&AC-2.2.1.7, A&AC-2.2.1.8, AC&DH-2.1.1.1, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17)

Rationale: Though roll has no direct effect on the translation of material downstream of the rotation joint or the HGA's beam direction, it can be coupled with pitch or yaw to create a hemispheric range of motion for beam pointing or material translation. Refer to the trade study in Section 4 for a detailed explanation for the selection of six degrees of freedom in the HGA Boom.

A&AC-2.2.1.2. The HGA boom segments are TBD meters long cylindrical shells, each TBD centimeters thick. (↑A&AC-A1, A&AC-C1)

A&AC-2.2.1.3. Translation of the HGA with respect to the main spacecraft structure is controlled through rotation of HGA boom segments. (←A&AC-2.2.1.1)

A&AC-2.2.1.4. Each HGA Boom rotation joint degree of freedom can be restrained during launch, spacecraft velocity changes, and as otherwise needed by TBD mechanical locks that can be engaged electrically. While electrical power is required to change the state of the locks (i.e., engaged, disengaged), no power is required to maintain the current state of the locks. (↑A&AC-SC1, A&AC-SC2, A&AC-ICA11, HA&T-G2), (→A&AC-2.2.1.12, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42, SV-43, SV-44, SV-45, SV-46, SV-47, SV-48)

A&AC-2.2.1.5. Each HGA boom rotation joint degree of freedom is measured every TBD seconds by an angle encoder. (↑A&AC-C3, A&AC-C4, A&AC-SC3, A&AC-SC6, A&AC-ICA10, HA&T-G1, HA&T-G3), (←A&AC 2.2.1.1), (→A&AC-2.2.1.11, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17),

(↓3.ShoulderRollMSMT, 3.ShoulderPitchMSMT, 3.ElbowRollMSMT, 3.ElbowPitchMSMT, 3.WristRollMSMT, 3.WristPitchMSMT)

A&AC-2.2.1.6. The maximum range of pitch rotation at each joint is TBD radians in the forward and reverse directions with the zero radian defined by the angle in which the boom segment (or antenna center) downstream of the joint is parallel to the boom segment upstream of the joint. (←A&AC 2.2.1.1), (→SV-9, SV-13, SV-17)

A&AC-2.2.1.7. The maximum range of roll rotation at each joint is TBD Radians in the forward and reverse directions. (←A&AC 2.2.1.1), (→SV-8, SV-12, SV-16)

A&AC-2.2.1.8. Rotation in each rotational degree of freedom is created and resisted, as needed, by an electric motor when the locks on the degree of freedom are disengaged. (←A&AC 2.2.1.1), (↑A&AC-SC1, A&AC-ICA9, A&AC-ICA10, A&AC-ICA11), (→SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-25, SV-26, SV-27, SV-28, SV-29, SV-30, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

A&AC-2.2.1.9. To the extent that it is prudent, the HGA Boom will be mounted on a part of the main spacecraft structure that reduces the overlap in its range of articulation and signal radiation with the range of articulation of other spacecraft appendages. (↑A&AC-SC3)

A&AC-2.2.1.10. The locks will be made to allow no more than TBD radians of rotation over an operational torque range of TBD to TBD Newton-meters plus TBD safety margin. (↑A&AC-SC17), (→SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

A&AC-2.2.1.11. An HGA Sun Sensor mounted on the HGA measures the angle between the HGA pointing vector (i.e., center of HGA) and the Sun every TBD seconds. (↑A&AC-SC19, HA&T-G1), (←A&AC 2.2.1.5), (↓3.SunAngleMSMT)

Rationale: Because there is the possibility of slippage between the HGA Boom Rotation Joint Angle Encoders and the HGA Boom Rotation Joints, it is beneficial to have an external reference to verify the encoders' measurements. The position of the Sun with respect to the spacecraft will be known for the purpose of spacecraft navigation. This information, coupled with spacecraft attitude information and rotation joint angles, should make it possible to derive the expected Sun angle with respect to the HGA pointing vector. Any difference between the expected Sun angle and the measured Sun angle would be an indirect indication of boom rotation angle measurement errors and/or errors in inferred spacecraft attitude and position.

A&AC-2.2.1.12. The position of the locks on the HGA Boom Rotation Joint degrees of freedom are measured every TBD seconds by HGA Boom Rotation Lock Sensors. (↑A&AC-SC14, HA&T-G1), (←A&AC-2.2.1.4), (→SV-37, SV-38, SV-39, SV-40, SV-41, SV-42), (↓3.ShoulderRollLockPositionMSMT, 3.ShoulderPitchLockPositionMSMT, 3.ElbowRollLockPositionMSMT, 3.ElbowPitchLockPositionMSMT, 3.WristRollLockPositionMSMT, 3.WristPitchLockPositionMSMT)

Rationale: Because there is the possibility of partial disengagement of the HGA Boom Rotation Joint Locks, it is beneficial to have a measurement of the joint lock positions to inform control of the motors.

A&AC-2.2.2. The A&AC functional element sends a 'HGA Translation' State Information input to the C&DH every TBD seconds. (↑A&AC-C4, A&AC-ICA7, A&AC-ICA8), (→C&DH-2.1.6.2)

Rationale: The C&DH requires this information for determining directives for the A&AC.

A&AC-2.3. The interfaces of the A&AC-level functional elements are monitored and managed by an A&AC command and data handling (AC&DH) functional element that translates directives generated by the C&DH into directives for other A&AC functional elements after evaluating if the conditions for the directives are satisfied. (↑A&AC-SC1, A&AC-SC2, A&AC-SC3, A&AC-SC4, A&AC-SC5, A&AC-SC6, A&AC-SC7, A&AC-SC8, A&AC-SC9, A&AC-SC10, A&AC-SC12, A&AC-SC14, A&AC-SC15, A&AC-SC16, AC&DH-G1), (→AC&DH-2.1)

Rationale: A central concept in control and systems theory is that of hierarchy. By definition, control involves the imposition of constraints from one level of the control hierarchy to a lower level (Checkland, 1981). The AC&DH functional element represents control on the A&AC-level while the other functional elements mentioned in this design principle all control lower-level functions and need a higher-level controller to manage their interactions with each other.

AC&DH-2.1. The A&AC C&DH (AC&DH) receives C&DH Directives as an input, sends all necessary A&AC state information to the C&DH as an output, and executes the necessary tasks and/or delegates them to the appropriate A&AC functional elements. (←A&AC-2.3, A&AC-2.1.2)

AC&DH-2.1.1. The AC&DH computes and sends the 'HGA Boom Rotation Joint Targets' directive to the HA&T. (↑AC&DH-R4, AC&DH-R5, AC&DH-C3), (→AC&DH-2.1.2)

AC&DH-2.1.1.1. The 'HGA Boom Rotation Joint Targets' directive is a vector of six values (in radians) corresponding to HGA Boom Shoulder Pitch, HGA Boom Shoulder Roll, HGA Boom Elbow Pitch, HGA Boom Elbow Roll, HGA Boom Wrist Pitch, HGA Boom Wrist Roll. (←A&AC 2.2.1.1) (→SV-8, SV-9, SV-12, SV-13, SV-16, SV-17)

AC&DH-2.1.1.2. The 'HGA Boom Rotation Joint Targets' directive is derived from C&DH directives related to spacecraft attitude and HGA pointing and the AC&DH's knowledge of the following state information: Spacecraft Position, Spacecraft Attitude, and HA&T Control Mode.

Rationale: The AC&DH is assigned this function because it is the lowest-level functional element with access to state information relating to the spacecraft's position relative to Earth, and the spacecraft's attitude. This information is necessary to define pointing vectors for HGA signal radiation.

AC&DH-2.1.2. The AC&DH defines an imaginary 3-dimensional surface referred to as the "roll-pitch mask" that marks the allowable boundary of HGA motion and signal radiation relative to the main spacecraft structure and spacecraft appendages. Any C&DH directive that produces an 'HGA Boom Rotation Joint Targets' directive that would lead to a combination of shoulder, elbow, and wrist roll and pitch rotation that causes any part of the HGA, HGA boom, and/or the HGA's radiated signals to breach the roll-pitch mask will not be authorized for execution by the AC&DH. (↑A&AC-SC3, A&AC-SC16, AC&DH-C3), (←A&AC-2.1, A&AC-2.2, AC&DH-2.1.1), (→SV-8, SV-9, SV-12, SV-13, SV-16, SV-17)

Rationale: The AC&DH is assigned this function because it is the lowest-level functional element with access to the 'HGA Boom Joint Rotation Targets' directive and state information relating to the attitude of spacecraft appendages relative to the main spacecraft structure. This information is necessary to determine HGA Boom Joint Rotation Targets that will violate the envelope of safe HGA translation and rotation.

AC&DH-2.1.2.1. The roll-pitch mask is derived from the mounting position of the HGA Boom Shoulder Joint on the main spacecraft structure, the model of the spacecraft's structural configuration, and state information inputs from the estimators of other spacecraft appendage states.

AC&DH-2.1.2.2. Whenever an 'HGA Boom Rotation Joint Targets' directive is generated that would violate the roll-pitch mask, the AC&DH transitions into the "Safe" Control Mode

Rationale: If the AC&DH must reject the 'HGA Boom Rotation Joint Targets' directive that it derives, it must revert to some baseline functionality in order to restore nominal pointing operations. This baseline functionality could include reorientation of the spacecraft or the commanding of the HA&T to hold the current boom joint rotation angles. The issue of the determining what that baseline functionality should be requires a trade study during the next iteration of the STPA, which is beyond the scope of this study.

AC&DH-2.1.2.3. The roll-pitch mask accounts for a ±TBD degree pointing error in HGA Boom Shoulder Roll and a ±TBD degree pointing error in HGA Shoulder Pitch. (↑A&AC-SC19)

AC&DH-2.1.2.4. The roll-pitch mask accounts for a ±TBD degree pointing error in HGA Boom Elbow Roll and a ±TBD degree pointing error in HGA Elbow Pitch. (↑A&AC-SC19)

AC&DH-2.1.2.5. The roll-pitch mask accounts for a ±TBD degree pointing error in HGA Boom Wrist Roll and a ±TBD degree pointing error in HGA Wrist Pitch. (↑A&AC-SC19)

AC&DH-2.1.3. The AC&DH infers HGA Translation and Rotation state from a 'HGA Boom Joint Rotation' state information input sent every TBD seconds from the HA&T. (↑AC&DH-C4, HA&T-C2)

A&AC-2.4. A HGA Attitude and Translation (HA&T) Control functional element is used for feedback control of the joint rotations necessary for HGA rotation and translation. (←A&AC-2.1, A&AC-2.2), (↑A&AC-SC1, A&AC-SC2, A&AC-SC3, A&AC-SC5, A&AC-SC6, A&AC-SC7, A&AC-SC8, A&AC-SC10, A&AC-SC12, A&AC-SC14, A&AC-SC15, A&AC-SC16, AC&DH-G1, HA&T-G1, HA&T-G2, HA&T-G3), (→HA&T-2.1, HA&T-2.2, HA&T-2.3, HA&T-2.4, HA&T-2.5)

Rationale: HGA restraint, rotation, and translation are coupled heavily due to the multiple boom segment architecture.

HA&T-2.1. The HA&T infers the rotation states (relative to the desired states) along all degrees of freedom (ShoulderRoll, ShoulderPitch, ElbowRoll, ElbowPitch, WristRoll, and WristPitch) every TBD seconds based on control inputs from the AC&DH and measurements from the angle encoders. (←A&AC-2.4), (↑HA&T-R1, HA&T-C3, HA&T-C4), (↓3.ShoulderRollMSMT, 3.ShoulderPitchMSMT, 3.ElbowRollMSMT, 3.ElbowPitchMSMT, 3.WristRollMSMT, 3.WristPitchMSMT), (→HA&T-2.4, HA&T-2.5, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17)

HA&T-2.2. The HA&T infers the rotation joint lock position states along all degrees of freedom (ShoulderRollLockPosition, ShoulderPitchLockPosition, ElbowRollLockPosition, ElbowPitchLockPosition, WristRollLockPosition, and WristPitchLockPosition) every TBD seconds based on measurements from the joint rotation lock sensors. The inferred states are:

1. Unknown if the lock position measurement is 'Obsolete'
2. Engaged if the lock position measurement is 'Engaged'
3. Disengaged if the lock position measurement is 'Disengaged'

(←A&AC-2.4), (↑HA&T-R3, HA&T-C6), (↓3.ShoulderRollLockPositionMSMT, 3.ShoulderRollLockPosition, 3.ShoulderPitchLockPositionMSMT, 3.ElbowRollLockPositionMSMT, 3.ElbowPitchLockPositionMSMT 3.WristRollLockPositionMSMT, 3.WristPitchLockPositionMSMT), (→HA&T-2.4, HA&T-2.5, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

HA&T-2.3. The HA&T has the following control modes:

1. "Safe" mode for off-nominal operations.
2. "Wrist" mode for pointing operations utilizing only the wrist pitch and wrist roll degrees of freedom.
3. "Elbow_Wrist" mode for pointing operations utilizing the wrist pitch and elbow roll degrees of freedom or the wrist roll and elbow pitch degrees of freedom.
4. "Shoulder_Wrist" mode for pointing operations utilizing the wrist pitch and shoulder roll degrees of freedom or the wrist roll and shoulder pitch degrees of freedom.
5. "Shoulder_Elbow" mode for the pointing operations utilizing the elbow pitch and shoulder roll degrees of freedom or the elbow roll and shoulder pitch degrees of freedom.
6. "Pre_Deploy" mode for operations prior to HGA boom deployment.
7. "Deploy" mode for HGA boom deployment operations.
8. "Lock" mode for planned locking of all HGA boom degrees of freedom after HGA boom deployment.

(←A&AC-2.4), (↑HA&T-R2, HA&T-R4, HA&T-R5), (↓3.HA&T Control), (→HA&T-2.4, HA&T-2.5, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-25, SV-26, SV-27, SV-28, SV-29, SV-30, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

Rationale: These control modes are a preliminary set to capture the types of functionality that the HA&T controller will require. Because the elbow and shoulder joint motors are further from the HGA than the wrist joint motors, their effectiveness in controlling the orientation of the HGA (in

terms of pointing precision, minimization of control effort, and pointing stability) will be less than that of the wrist joint motors (assuming that the same type of motor is used on all joints). Thus, the primary pointing mode will be the "Wrist" mode. Note that these mode definitions are subject to a trade study and hazard analysis of their transition conditions.

HA&T-2.4. The HA&T sends the 'EngageShoulderRollLockCMD', 'EngageShoulderPitchLockCMD', 'EngageElbowRollLockCMD', 'EngageElbowPitchLockCMD', 'EngageWristRollLockCMD', and 'EngageWristPitchLockCMD' to the Shoulder, Elbow, and Wrist Roll and Pitch Locks in accordance with HA&T Control Modes, rotation state inferences along all HGA boom degrees of freedom, and HGA boom rotation joint lock state inferences in order to engage the HGA boom rotation joint locks at the appropriate times.
(←A&AC-2.4, HA&T-2.1, HA&T-2.2, HA&T-2.3), (↑HA&T-R5), (↓3.EngageShoulderRollLockCMD), (→SV-1, SV-2, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

HA&T-2.5. The HA&T sends the 'DisengageShoulderRollLockCMD', 'DisengageShoulderPitchLockCMD', 'DisengageElbowRollLockCMD', 'DisengageElbowPitchLockCMD', 'DisengageWristRollLockCMD', and 'DisengageWristPitchLockCMD' to the Shoulder, Elbow, and Wrist Roll and Pitch Locks in accordance with HA&T Control Modes, rotation state inferences along all HGA boom degrees of freedom, and HGA boom rotation joint lock state inferences in order to engage the HGA boom rotation joint locks at the appropriate times.
(←A&AC-2.4, HA&T-2.1, HA&T-2.2, HA&T-2.3), (↑HA&T-R5), (↓3.DisengageShoulderRollLockCMD), (→SV-1, SV-2, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

A&AC-2.5. A Spacecraft Attitude Controller (AC) functional element is used for feedback control of spacecraft pointing. (↑A&AC-R6, A&AC-SC15, AC&DH-G1), (→SV-1, SV-2)

A&AC-2.6. A Spacecraft Translation Controller (TC) functional element is used for feedback control of spacecraft translation. (↑A&AC-R1, A&AC-R2, A&AC-R3, A&AC-R4, A&AC-R5, A&AC-SC16, AC&DH-G1), (→SV-1, SV-2)

A&AC-2.7. An A&AC Electrical Power (AEP) functional element receives and distributes electrical power from the EP to the A&AC functional elements. (↑A&AC- C5, A&AC-SC9, A&AC-SC12, AC&DH-G1)

S/C-2.4. A science data collection functional element on the spacecraft collects, stores, retrieves, and packetizes the scientific data to be gathered in fulfillment of the mission high-level requirements and goals. (↑S/C-R2, S/C-R5, S/C-C3, S/C-G2, S/C-SC1, C&DH-G1)

S/C-2.5. A communications functional element on the spacecraft modulates spacecraft data to be transmitted through the DSN or GN, radiates it in the direction of the DSN or GN, and demodulates data from signals received from the DSN and GN. (↑S/C-R3, S/C-R4, S/C-R5, S/C-R6, S/C-SC2, C&DH-G1, COM-G1, COM-G2, COM-G3, COM-G4)

COM-2.1. A passive (i.e., no electrical power is required to convert the processed electrical signal to radiation) High Gain Antenna (HGA) is deployed on the spacecraft for bi-directional communication over the DSN and GN operating frequencies. (↑COM-R5, COM-R6), (←A&AC-2.1)

COM-2.1.1. The antenna converts the processed electrical signal modulated with packetized data into focused electromagnetic radiation on DSN and GN operating frequencies. Similarly, the antenna converts received electromagnetic radiation into electrical signals.

COM-2.1.2. The High Gain Antenna (HGA) is composed of a 3-meter parabolic dish which efficiently increases the Signal to Noise Ratio of the communications link by utilizing a directional radiation pattern. (↑COM-A1, COM-A2, COM-C1)

Rationale: Antenna geometry is a major factor in strength of a communications link. A parabolic shape focuses the power of the radiated signal in a specific direction, thereby increasing the

strength of the signal when it is ultimately received. Due to the assumed detrimental effects of stowing the HGA in a non-parabolic shape while it is in the launch vehicle, the HGA will be a stowed in a parabolic shape and thus can be no larger than 3 meters in diameter.

2.2. A Delta-IVH launch vehicle is used insert the spacecraft into LEO (↑DC1.2, SC1, SC6, SC7, SC8, SC9, S/C-C1, S/C-C2, MOC-G3, A&AC-G1), (←2.1), (→SV-2)

Rationale: The Delta-IVH provides the largest mass to LEO capability of any U.S. expendable launch vehicle. (www.astronautix.com)

2.3. The NASA Deep Space Network (DSN) is be used for wireless communication between the spacecraft and Earth while the spacecraft is beyond Earth orbit (↑DC1.1, SC2, SC3, SC9, MOC-G2), (←2.1), (→SV-2)

2.4. A facility on earth, the Mission Operations Center (MOC), provides human operators with the capability to issue directives to the spacecraft and monitor telemetry that it transmits back to Earth. (↑A3, DC1, SC1, SC2, SC3, SC4, SC5, SC6, SC7, SC8, SC9, S/C-C4, MOC-G1, MOC-G2, MOC-G3, MOC-G4), (←2.1)

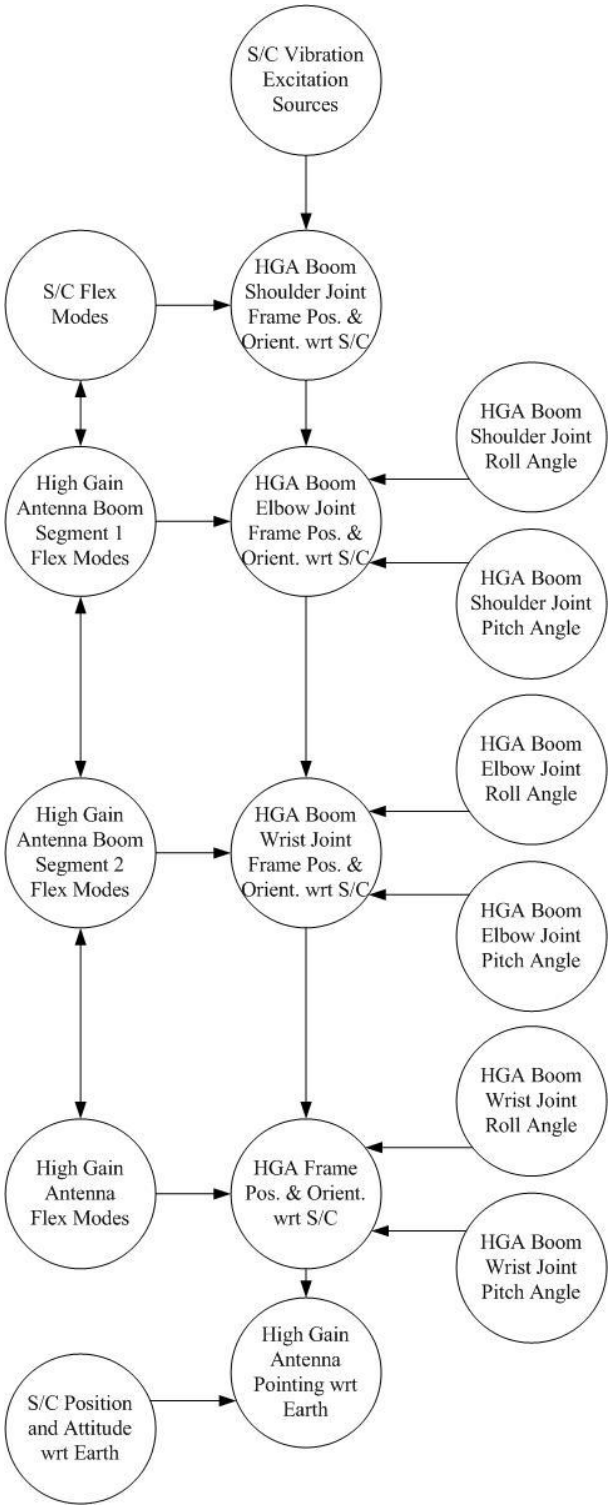
Rationale: It is assumed that complete autonomy of the spacecraft will not be possible (it also may not be desirable as new scientific goals may emerge throughout mission operations). Thus, there must be a human control interface to the spacecraft.

2.5. The NASA Ground Network (GN) is used for wireless communication between the Launch Vehicle and Spacecraft (if necessary) and Earth while the spacecraft is in Low Earth Orbit. (↑DC1.3, SC2, SC3, SC9, MOC-G4), (←2.1, 2.2), (→SV-2)

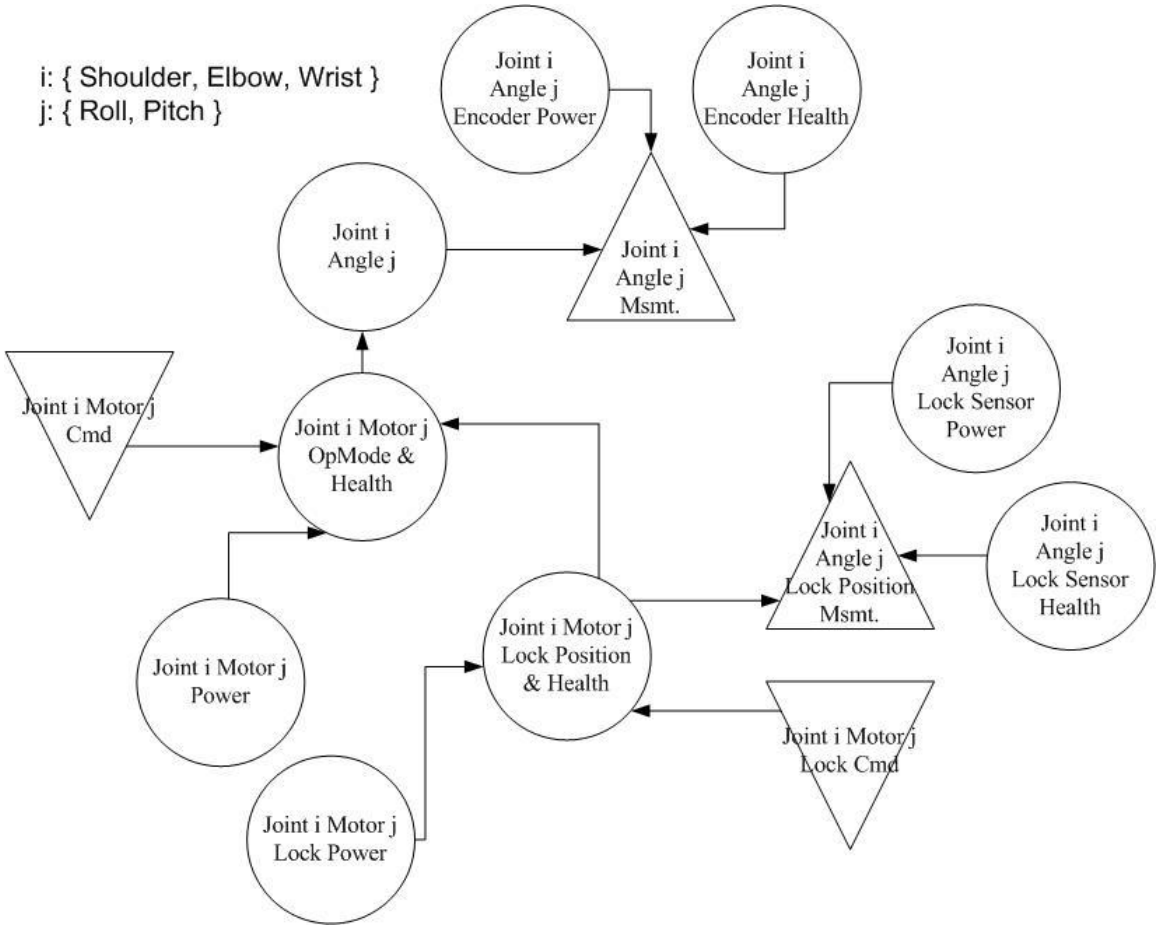
Further specification of the system design decisions is beyond the scope of this study.

State Effects Diagrams:

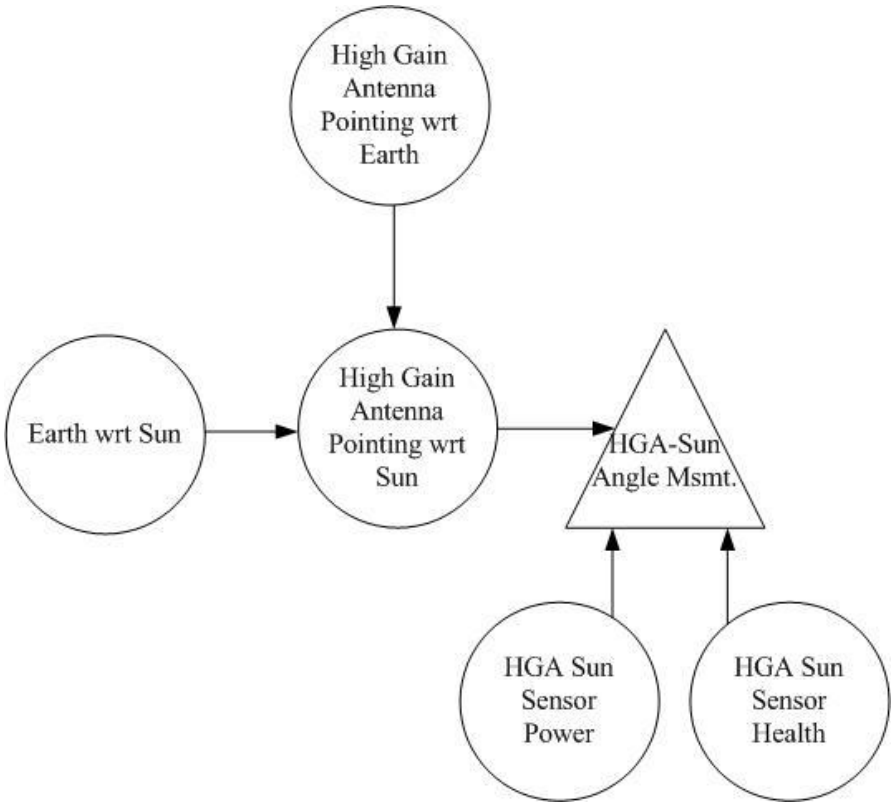
SED1. (→SV-2, SV-3, SV-4, SV-5, SV-6, SV-7, SV-8, SV-9, SV-10, SV-11, SV-12, SV-13, SV-14, SV-15, SV-16, SV-17, SV-18)



SED2. (→SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-25, SV-26, SV-27, SV-28, SV-29, SV-30, SV-31, SV-32, SV-33, SV-34, SV-35, SV-36, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42, SV-43, SV-44, SV-45, SV-46, SV-47, SV-48, SV-49, SV-50, SV-51, SV-52, SV-53, SV-54, SV-55 SV-56, SV-57, SV-58, SV-59, SV-60, SV-61, SV-62, SV-63, SV-64, SV-65, SV-66, SV-67, SV-68, SV-69, SV-70, SV-71, SV-72)



SED3. (→SV-18, SV-73, SV-74, SV-75, SV-76)



System Under Control State Variables

SV-1. Spacecraft Attitude and Position with respect to Outer Planet Moon (↑EC1, H4, SC4, HLR1, HLR2, HLR3, HLR4, HLR5, S/C-R1, S/C-R1, S/C-R3, S/C-SC3, S/C-SC4, C&DH-R6, C&DH-R7, A&AC-R1, A&AC-R2, A&AC-R3, A&AC-R4, A&AC-R5, A&AC-R6, A&AC-SC15, AC&DH-R2, AC&DH-R3, HA&T-R5), (←2.1, S/C-2.3, C&DH-2.1.6, A&AC-2.6, HA&T-2.4, HA&T-2.5)

SV-2. Spacecraft Position and Attitude with respect to Earth. (↑H5, H6, SC5, SC6, SC7, SC8, S/C-R4, S/C-R5, S/C-R6, S/C-SC5, S/C-SC6, S/C-SC7, C&DH-R6, C&DH-R7, C&DH-CF1.1, C&DH-SC10, A&AC-G1, A&AC-G2, A&AC-R1, A&AC-R6, A&AC-SC15, AC&DH-R2, AC&DH-R3, HA&T-R5), (←2.1, 2.2, 2.3, 2.5, S/C-2.3, C&DH-2.1.6, A&AC-2.6, SED1, HA&T-2.4, HA&T-2.5)

SV-3. Spacecraft Vibration Excitation Sources. (←SED1), (↑A&AC-CF2.3, A&AC-CF4.3, A&AC-SC7)

SV-4. HGA Boom Shoulder Joint Frame Position and Orientation with respect to Spacecraft. (←SED1, A&AC-2.2)

SV-5. Spacecraft Flex Modes. (←SED1), (↑1, A&AC-CF2.3, A&AC-CF4.3, A&AC-SC7)

SV-6. High Gain Antenna Boom Segment 1 Flex Modes. (←SED1), (↑A&AC1.2, A&AC-CF2.3, A&AC-CF4.3, A&AC-SC7)

SV-7. HGA Boom Elbow Joint Frame Position and Orientation with respect to Spacecraft. (←SED1, A&AC-2.2)

SV-8. HGA Boom Shoulder Joint Roll Angle. (↑A&AC1.1, A&AC-ICA9, A&AC-ICA10, A&AC-ICA11, A&AC-SC8, A&AC-SC11, A&AC-SC13), (←SED1, SED2, A&AC-2.2.1.1, A&AC-2.2.1.7, A&AC-2.2.1.5, A&AC-2.2.1.8, AC&DH-2.1.1.1, AC&DH-2.1.2, HA&T-2.1, HA&T-2.3)

State Effects Model for Joint i Angle j:

$$\theta_j^i = f(\text{Joint i Motor j OpMode \& Health})$$

Here's a simplified model:

$$\theta_j^i = \int_{t_0}^{t_f} \dot{\theta}_j^i \, dt$$

$$\dot{\theta}_j^i = \begin{Bmatrix} +\omega_{max}, \text{if OpMode} = \text{Rotate} + \\ -\omega_{max}, \text{if OpMode} = \text{Rotate} - \\ 0, \text{otherwise} \end{Bmatrix}$$

SV-9. HGA Boom Shoulder Joint Pitch Angle. (↑A&AC1.1, A&AC-ICA9, A&AC-ICA10, A&AC-ICA11, A&AC-SC8, A&AC-SC11, A&AC-SC13), (←SED1, SED2, A&AC-2.2.1.1, A&AC-2.2.1.6, A&AC-2.2.1.5, A&AC-2.2.1.8, AC&DH-2.1.1.1, AC&DH-2.1.2, HA&T-2.1, HA&T-2.3)

Refer to state variable model for SV-8

SV-10. HGA Boom Segment 2 Flex Modes. (←SED1), (↑A&AC1.2, A&AC-CF2.3, A&AC-CF4.3, A&AC-SC7)

SV-11. HGA Wrist Joint Position and Orientation with respect to Spacecraft. (←SED1, A&AC-2.2)

SV-12. HGA Boom Elbow Joint Roll Angle. (↑A&AC1.1, A&AC-ICA9, A&AC-ICA10, A&AC-ICA11, A&AC-SC8, A&AC-SC11, A&AC-SC13), (←SED1, SED2, A&AC-2.2.1.1, A&AC-2.2.1.7, A&AC-2.2.1.5, A&AC-2.2.1.8, AC&DH-2.1.1.1, AC&DH-2.1.2, HA&T-2.1, HA&T-2.3))

Refer to state variable model for SV-8

SV-13. HGA Boom Elbow Joint Pitch Angle. (↑A&AC1.1, A&AC-ICA9, A&AC-ICA10, A&AC-ICA11, A&AC-SC8, A&AC-SC11, A&AC-SC13), (←SED1, SED2, A&AC-2.2.1.1, A&AC-2.2.1.6, A&AC-2.2.1.5, A&AC-2.2.1.8, AC&DH-2.1.1.1, AC&DH-2.1.2, HA&T-2.1, HA&T-2.3)

Refer to state variable model for SV-8

SV-14. HGA Flex Modes. (↑COM1, A&AC-CF2.3, A&AC-CF4.3, A&AC-SC7), (←SED1)

SV-15. HGA Frame Position and Orientation with respect to Spacecraft. (←SED1, A&AC-2.1, A&AC-2.2)

SV-16. HGA Boom Wrist Joint Roll Angle. (↑A&AC1.1, A&AC-ICA9, A&AC-ICA10, A&AC-ICA11, A&AC-SC8, A&AC-SC11, A&AC-SC13), (←SED1, SED2, A&AC-2.2.1.1, A&AC-2.2.1.7, A&AC-2.2.1.5, A&AC-2.2.1.8, AC&DH-2.1.1.1, AC&DH-2.1.2, HA&T-2.1, HA&T-2.3)

Refer to state variable model for SV-8

SV-17. HGA Boom Wrist Joint Pitch Angle. (↑A&AC1.1, A&AC-ICA9, A&AC-ICA10, A&AC-ICA11, A&AC-SC8, A&AC-SC11, A&AC-SC13), (←SED1, SED2, A&AC-2.2.1.1, A&AC-2.2.1.6, A&AC-2.2.1.5, A&AC-2.2.1.8, AC&DH-2.1.1.1, AC&DH-2.1.2, HA&T-2.1, HA&T-2.3)

Refer to state variable model for SV-8

SV-18. HGA Pointing with respect to Earth. (←SED1, SED3, A&AC-2.1)

SV-19. Spacecraft Opmode (↑1)

SV-20. DSN Opmode (↑2)

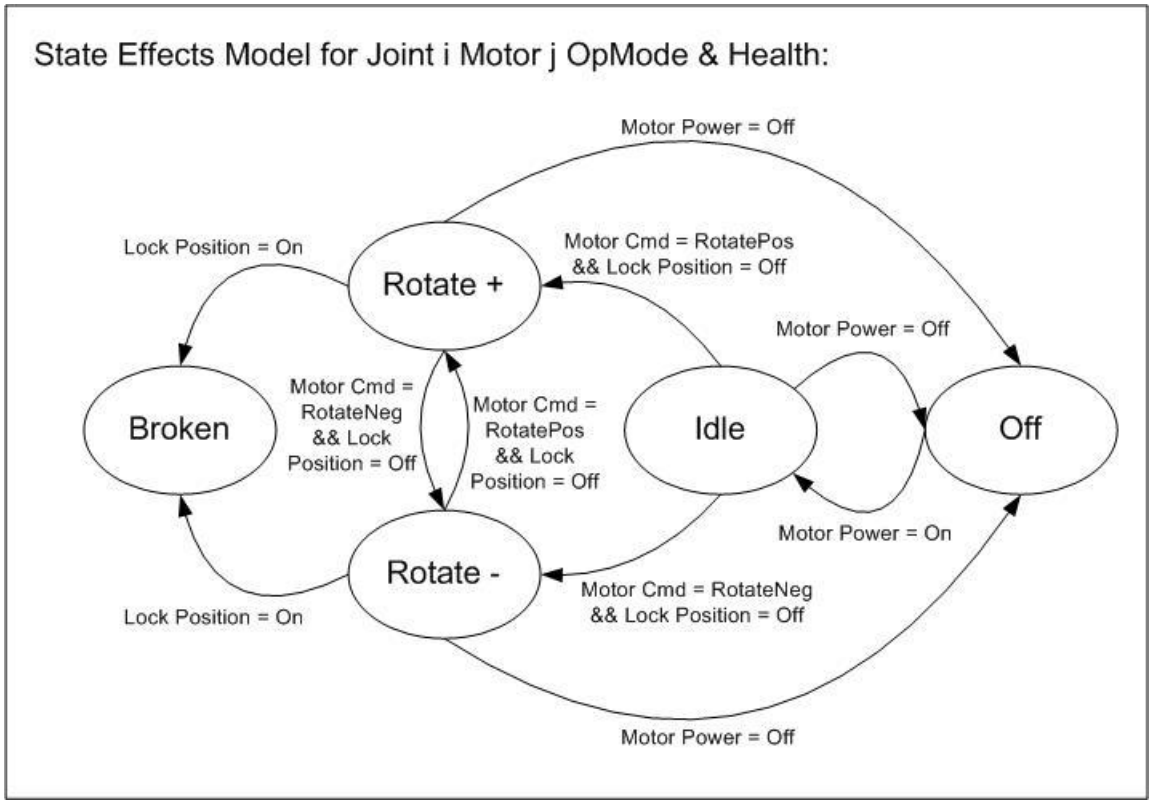
SV-21. Launch Vehicle Opmode (↑3, A&AC-CF3.1)

SV-22. MOC Opmode (↑4)

SV-23. GN Opmode (↑5)

SV-24. HGA Opmode (↑COM1)

SV-25. HGA Boom Shoulder Joint Pitch Motor Opmode and Health. (↑A&AC1.1.1, A&AC-CF9.5, A&AC-CF10.2, A&AC-CF10.3, A&AC-CF10.4, A&AC-CF10.5, A&AC-SC13, A&AC-SC14, A&AC-SC15, HA&T-R2), (←SED2, A&AC-2.2.1.8, HA&T-2.3)



SV-26. HGA Boom Elbow Joint Pitch Motor Opmode and Health. (↑A&AC1.1.1, A&AC-CF9.5, A&AC-CF10.2, A&AC-CF10.3, A&AC-CF10.4, A&AC-CF10.5, A&AC-SC13, A&AC-SC14, A&AC-SC15, HA&T-R2), (←SED2, A&AC-2.2.1.8, HA&T-2.3)

Refer to state variable model for SV-25

SV-27. HGA Boom Wrist Joint Pitch Motor Opmode and Health. (↑A&AC1.1.1, A&AC-CF9.5, A&AC-CF10.2, A&AC-CF10.3, A&AC-CF10.4, A&AC-CF10.5, A&AC-SC13, A&AC-SC14, A&AC-SC15, HA&T-R2), (←SED2, A&AC-2.2.1.8, HA&T-2.3)

Refer to state variable model for SV-25

SV-28. HGA Boom Shoulder Joint Roll Motor Opmode and Health. (↑A&AC1.1.1, A&AC-CF9.5, A&AC-CF10.2, A&AC-CF10.3, A&AC-CF10.4, A&AC-CF10.5, A&AC-SC13, A&AC-SC14, A&AC-SC15, HA&T-R2), (←SED2, A&AC-2.2.1.8, HA&T-2.3)

Refer to state variable model for SV-25

SV-29. HGA Boom Elbow Joint Roll Motor Opmode and Health. (↑A&AC1.1.1, A&AC-CF9.5, A&AC-CF10.2, A&AC-CF10.3, A&AC-CF10.4, A&AC-CF10.5, A&AC-SC13, A&AC-SC14, A&AC-SC15, HA&T-R2), (←SED2, A&AC-2.2.1.8, HA&T-2.3)

Refer to state variable model for SV-25

SV-30. HGA Boom Wrist Joint Roll Motor Opmode and Health. (↑A&AC1.1.1, A&AC-CF9.5, A&AC-CF10.2, A&AC-CF10.3, A&AC-CF10.4, A&AC-CF10.5, A&AC-SC13, A&AC-SC14, A&AC-SC15, HA&T-R2), (←SED2, A&AC-2.2.1.8, HA&T-2.3)

Refer to state variable model for SV-25

SV-31. HGA Boom Shoulder Joint Pitch Motor Power. (↑A&AC-CF9.4, A&AC-SC12), (←SED2, A&AC-2.1.1)

SV-32. HGA Boom Elbow Joint Pitch Motor Power. (↑A&AC-CF9.4, A&AC-SC12), (←SED2, A&AC-2.1.1)

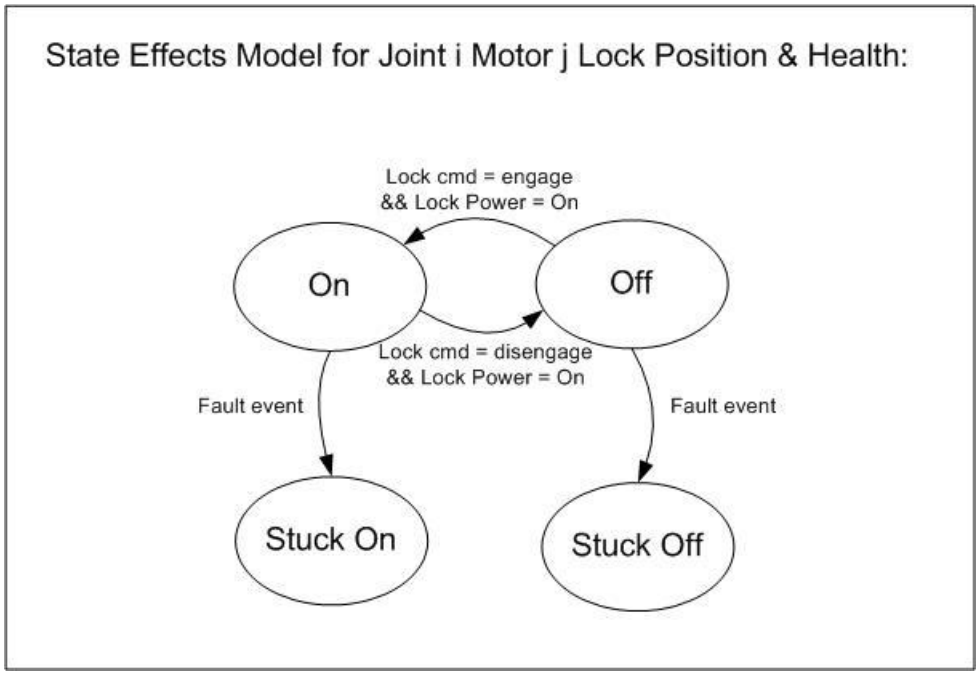
SV-33. HGA Boom Wrist Joint Pitch Motor Power. (↑A&AC-CF9.4, A&AC-SC12), (←SED2, A&AC-2.1.1)

SV-34. HGA Boom Shoulder Joint Roll Motor Power. (↑A&AC-CF9.4, A&AC-SC12), (←SED2, A&AC-2.1.1)

SV-35. HGA Boom Elbow Joint Roll Motor Power. (↑A&AC-CF9.4, A&AC-SC12), (←SED2, A&AC-2.1.1)

SV-36. HGA Boom Wrist Joint Roll Motor Power. (↑A&AC-CF9.4, A&AC-SC12), (←SED2, A&AC-2.1.1)

SV-37. HGA Boom Shoulder Joint Pitch Lock Position and Health. (↑A&AC1.1.2, A&AC-ICA10, A&AC-ICA11, A&AC-CF9.1, A&AC-CF9.3, A&AC-CF10.4, A&AC-CF11.1, A&AC-CF11.2, A&AC-CF11.3, A&AC-SC8, A&AC-SC10, A&AC-SC14, A&AC-SC15, A&AC-SC17, HA&T-R4, HA&T-R5), (←SED2, A&AC-2.2.1.4, A&AC-2.2.1.8, A&AC-2.2.1.10, A&AC-2.2.1.12, HA&T-2.2, HA&T-2.3, HA&T-2.4, HA&T-2.5)



SV-38. HGA Boom Elbow Joint Pitch Lock Position and Health. (↑A&AC1.1.2, A&AC-ICA10, A&AC-ICA11, A&AC-CF9.1, A&AC-CF9.3, A&AC-CF10.4, A&AC-CF11.1, A&AC-CF11.2, A&AC-CF11.3, A&AC-SC8, A&AC-SC10, A&AC-SC14, A&AC-SC15, A&AC-SC17, HA&T-R4, HA&T-R5), (←SED2, A&AC-2.2.1.4, A&AC-2.2.1.8, A&AC-2.2.1.10, A&AC-2.2.1.12, HA&T-2.2, HA&T-2.3, HA&T-2.4, HA&T-2.5)

Refer to state variable model for SV-37

SV-39. HGA Boom Wrist Joint Pitch Lock Position and Health. (↑A&AC1.1.2, A&AC-ICA10, A&AC-ICA11, A&AC-CF9.1, A&AC-CF9.3, A&AC-CF10.4, A&AC-CF11.1, A&AC-CF11.2, A&AC-CF11.3, A&AC-SC8, A&AC-SC10, A&AC-SC14, A&AC-SC15, A&AC-SC17, HA&T-R4, HA&T-R5), (←SED2, A&AC-2.2.1.4, A&AC-2.2.1.8, A&AC-2.2.1.10, A&AC-2.2.1.12, HA&T-2.2, HA&T-2.3, HA&T-2.4, HA&T-2.5)

Refer to state variable model for SV-37

SV-40. HGA Boom Shoulder Joint Roll Lock Position and Health. (↑A&AC1.1.2, A&AC-ICA10, A&AC-ICA11, A&AC-CF9.1, A&AC-CF9.3, A&AC-CF10.4, A&AC-CF11.1, A&AC-CF11.2, A&AC-CF11.3, A&AC-SC8, A&AC-SC10, A&AC-SC14, A&AC-SC15, A&AC-SC17, HA&T-R4, HA&T-R5), (←SED2, A&AC-2.2.1.4, A&AC-2.2.1.8, A&AC-2.2.1.10, A&AC-2.2.1.12, HA&T-2.2, HA&T-2.3, HA&T-2.4, HA&T-2.5)

Refer to state variable model for SV-37

SV-41. HGA Boom Elbow Joint Roll Lock Position and Health. (↑A&AC1.1.2, A&AC-ICA10, A&AC-ICA11, A&AC-CF9.1, A&AC-CF9.3, A&AC-CF10.4, A&AC-CF11.1, A&AC-CF11.2, A&AC-CF11.3, A&AC-SC8, A&AC-SC10, A&AC-SC14, A&AC-SC15, A&AC-SC17, HA&T-R4, HA&T-R5), (←SED2, A&AC-2.2.1.4, A&AC-2.2.1.8, A&AC-2.2.1.10, A&AC-2.2.1.12, HA&T-2.2, HA&T-2.3, HA&T-2.4, HA&T-2.5)

Refer to state variable model for SV-37

SV-42. HGA Boom Wrist Joint Roll Lock Position and Health. (↑A&AC1.1.2, A&AC-ICA10, A&AC-ICA11, A&AC-CF9.1, A&AC-CF9.3, A&AC-CF10.4, A&AC-CF11.1, A&AC-CF11.2, A&AC-CF11.3, A&AC-SC8, A&AC-SC10, A&AC-SC14, A&AC-SC15, A&AC-SC17, HA&T-R4, HA&T-R5), (←SED2, A&AC-2.2.1.4, A&AC-2.2.1.8, A&AC-2.2.1.10, A&AC-2.2.1.12, HA&T-2.2, HA&T-2.3, HA&T-2.4, HA&T-2.5)

Refer to state variable model for SV-37

SV-43. HGA Boom Shoulder Joint Pitch Lock Power. (↑A&AC-CF9.2, A&AC-SC9), (←SED2, A&AC-2.2.1.4)

SV-44. HGA Boom Elbow Joint Pitch Lock Power. (↑A&AC-CF9.2, A&AC-SC9), (←SED2, A&AC-2.2.1.4)

SV-45. HGA Boom Wrist Joint Pitch Lock Power. (↑A&AC-CF9.2, A&AC-SC9), (←SED2, A&AC-2.2.1.4)

SV-46. HGA Boom Shoulder Joint Roll Lock Power. (↑A&AC-CF9.2, A&AC-SC9), (←SED2, A&AC-2.2.1.4)

SV-47. HGA Boom Elbow Joint Roll Lock Power. (↑A&AC-CF9.2, A&AC-SC9), (←SED2, A&AC-2.2.1.4)

SV-48. HGA Boom Wrist Joint Roll Lock Power. (↑A&AC-CF9.2, A&AC-SC9), (←SED2, A&AC-2.2.1.4)

SV-49. HGA Boom Shoulder Joint Pitch Encoder Power. (←SED2)

SV-50. HGA Boom Elbow Joint Pitch Encoder Power. (←SED2)

SV-51. HGA Boom Wrist Joint Pitch Encoder Power. (←SED2)

SV-52. HGA Boom Shoulder Joint Roll Encoder Power. (←SED2)

SV-53. HGA Boom Elbow Joint Roll Encoder Power. (←SED2)

SV-54. HGA Boom Wrist Joint Roll Encoder Power. (←SED2)

SV-55. HGA Boom Shoulder Joint Pitch Encoder Health. (←SED2)

SV-56. HGA Boom Elbow Joint Pitch Encoder Health. (←SED2)

SV-57. HGA Boom Wrist Joint Pitch Encoder Health. (←SED2)

SV-58. HGA Boom Shoulder Joint Roll Encoder Health. (←SED2)

SV-59. HGA Boom Elbow Joint Roll Encoder Health. (←SED2)

SV-60. HGA Boom Wrist Joint Roll Encoder Health. (←SED2)

SV-61. HGA Boom Shoulder Joint Pitch Lock Sensor Power. (←SED2)

SV-62. HGA Boom Elbow Joint Pitch Lock Sensor Power. (←SED2)

SV-63. HGA Boom Wrist Joint Pitch Lock Sensor Power. (←SED2)

SV-64. HGA Boom Shoulder Joint Roll Lock Sensor Power. (←SED2)

SV-65. HGA Boom Elbow Joint Roll Lock Sensor Power. (←SED2)

SV-66. HGA Boom Wrist Joint Roll Lock Sensor Power. (←SED2)

SV-67. HGA Boom Shoulder Joint Pitch Lock Sensor Health. (←SED2)

SV-68. HGA Boom Elbow Joint Pitch Lock Sensor Health. (←SED2)

SV-69. HGA Boom Wrist Joint Pitch Lock Sensor Health. (←SED2)

SV-70. HGA Boom Shoulder Joint Roll Lock Sensor Health. (←SED2)

SV-71. HGA Boom Elbow Joint Roll Lock Sensor Health. (←SED2)

SV-72. HGA Boom Wrist Joint Roll Lock Sensor Health. (←SED2)

SV-73. HGA Sun Sensor Power. (←SED3)

SV-74. HGA Sun Sensor Health. (←SED3)

SV-75. HGA Pointing with respect to Sun. (←SED3)

SV-76. Earth with respect to Sun. (←SED3)

SV-77. Humans Injured. (↑ACC1, ACC2)

SV-78. Humans Killed. (↑ACC1, ACC2)

SV-79. Human Property Damage. (↑ACC1, ACC2)

SV-80. Scientific Data Status. (↑ACC4, ACC5)

SV-81. Other Mission Status. (↑ACC7)

SV-82. Knowledge of Subsurface Ocean. (↑G1)

SV-83. Solar Flux in Orbit of Outer Planet Moon. (↑EC1)

SV-84. Technology Readiness Level of Technology X. (↑DC1)

SV-85. Mission Data Collection Functionality. (↑H1, SC1)

SV-86. Mission Data Transfer Functionality. (↑H2, SC2)

SV-87. Mission Data Availability. (↑H3, SC3)

SV-88. Mission Data Quality. (↑H3, SC3)

SV-89. Number of Earth Organisms on Outer Planet Moons. (↑H4, SC4, SC5)

SV-90. Amount of Chemical Energy in Mission Elements. (↑H5, H6, SC7)

SV-91. Amount of Potential Energy of Mission Elements. (↑H5, H6, SC7)

SV-92. Amount of Kinetic Energy of Mission Elements. (↑H5, H6, SC6, SC7, SC8)

SV-93. Amount of Radioactive Material in Mission Elements. (↑H5, H6, SC7)

SV-94. Toxicity of Mission Elements. (↑H5, H6, SC7)

SV-95. Amount of Thermal Energy in Mission Elements. (↑H5, H6, SC7)

SV-96. Availability of Space Exploration Infrastructure to Other Missions. (↑H7, SC9)

SV-97. Percent of Icy Moon Surface Imaged in the Visual Spectrum. (↑HLR1)

SV-98. Resolution of Visual Images of Icy Moon Surface. (↑HLR1)

SV-99. Percent of Icy Moon Surface Imaged in the Infrared Spectrum. (↑HLR2)

SV-100. Resolution of Infrared Images of Icy Moon Surface. (↑HLR2)

SV-101. Percent of Icy Moon Surface Imaged in Other Spectra. (↑HLR3)

SV-102. Resolution of Other Spectra Images of Icy Moon Surface. (↑HLR3)

SV-103. Percent of Icy Moon Magnetic Field Measured. (↑HLR4)

SV-104. Percent of Space around Icy Moon in which Flux of Radiation Particles are Measured (↑HLR5)

SV-105. Measurable Radiation Particle Energy Levels (↑HLR5)

Level 3: Blackbox Behavior

Spacecraft C&DH Blackbox Behavior
Further specification of this black box model is beyond the scope of this study.

A&AC C&DH (AC&DH) Blackbox Behavior
Further specification of this black box model is beyond the scope of this study.

HA&T Blackbox Behavior

Control Modes

Control Mode
HA&T Control

Description:
Comments: While a preliminary set of HA&T control modes has been defined, the definition of the transition conditions for these modes requires a trade study during the next iteration of the STPA, which is beyond the scope of this study.
References:
Appears In: (↑HA&T-2.3), (→3.EngageShoulderRollLockCMD, 3.DisengageShoulderRollLockCMD)

DEFINITION

= Safe

TBD	T

= Wrist

TBD	T

= Elbow_Wrist

TBD	T

= Shoulder_Wrist

TBD	T

= Shoulder_Elbow

TBD	T

= Pre_Deploy

TBD	T

= Deploy

TBD	T

= Lock

TBD	T

Further specification of the control modes of this black box model is beyond the scope of this study.

Outputs

Output Command

EngageShoulderRollLockCMD

Destination: Shoulder Roll Lock
Fields:
  Name: Command
    Type: {Engage, Disengage}
    Acceptable Values: {Engage}
      Units:
      Granularity:
      Hazardous Values:
      Exception-Handling:
    Description:
    Comments:
Timing Behavior:
  Initiation Delay:
  Completion Deadline:
  Output Capacity Assumptions:
    Load:
    Minimum Time Between Outputs:
    Maximum Time Between Outputs:
  Hazardous Timing Behavior:
  Exception-Handling:
Feedback Information:
  Variables:

Values:
Relationship:
Minimum Latency:
Maximum Latency:
Exception-Handling:
Reversed By:
Description:
Comments: While the engage and disengage commands for the joint rotation locks have been defined, the triggering conditions for these commands requires a trade study during the next iteration of the STPA, which is beyond the scope of this study.
References: (↑HA&T-2.4), (←3. HA&T Control), (→3.ShoulderRollLockPosition)

TRIGGERING CONDITION

TBD	T

MESSAGE CONTENTS

Field:	Value:
Command	Engage

Output Command

DisengageShoulderRollLockCMD

Destination: Shoulder Roll Lock
Fields:
Name: Command
Type: {Engage, Disengage}
Acceptable Values: {Disengage}
Units:
Granularity:
Hazardous Values:
Exception-Handling:
Description:
Comments:
Timing Behavior:
Initiation Delay:
Completion Deadline:
Output Capacity Assumptions:
Load:
Minimum Time Between Outputs:
Maximum Time Between Outputs:
Hazardous Timing Behavior:
Exception-Handling:
Feedback Information:
Variables:
Values:
Relationship:
Minimum Latency:
Maximum Latency:

Exception-Handling:
Reversed By:
Description:
Comments: While the engage and disengage commands for the joint rotation locks have been defined, the triggering conditions for these commands requires a trade study during the next iteration of the STPA, which is beyond the scope of this study.
References: (↑HA&T-2.5), (←3. HA&T Control), (→3.ShoulderRollLockPosition)

TRIGGERING CONDITION

TBD	T

MESSAGE CONTENTS

Field:	Value:
Command	Disengage

Further specification of outputs of this black box model is beyond the scope of this study.

States

State Value

ShoulderRollLockPosition

Obsolescence:
Exception-Handling:
Related Inputs: (→3.ShoulderRollLockPositionMSMT)
Description:
Comments:
References:
Appears In: (↑HA&T-2.2)

DEFINITION

= Unknown

ShoulderRollLockPositionMSMT is Obsolete	T

= Engaged

ShoulderRollLockPositionMSMT is Engaged	T

= Disengaged

ShoulderRollLockPositionMSMT is Disengaged	T

Further specification of inferred states of this black box model is beyond the scope of this study.

Inputs

Input Value

ShoulderRollMSMT

Source: Shoulder Roll Encoder
Type: Integer
Possible Values (Expected Range): [0..TBD]
  Units: milliradians
  Granularity:
  Exception-Handling: None
Timing Behavior:
  Load:
  Minimum Time Between Inputs:
  Maximum Time Between Inputs:
  Maximum Time Before First Input:
  Related Outputs:
    Latency:
    Time After Output:
  Exception-Handling:
Obsolescence:
  Exception-Handling:
Description:
Comments:
References:
Appears In: (↑A&AC-2.2.1.5, HA&T-2.1)

DEFINITION

= New Data for ShoulderRollMSMT

ShoulderRollMSMT was Received	T

= Previous Value of ShoulderRollMSMT

ShoulderRollMSMT was Received	F
Time Since ShoulderRollMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
ShoulderRollMSMT was Never Received	T	T	*
Time Since ShoulderRollMSMT was Last Received > TBD seconds	*	*	T

Input Value

ShoulderRollLockPositionMSMT

Source: Shoulder Roll Lock
Type: {Engaged, Disengaged}
Possible Values (Expected Range): Any
  Units:
  Granularity:
  Exception-Handling: None

Timing Behavior:
Load:
Minimum Time Between Inputs:
Maximum Time Between Inputs:
Maximum Time Before First Input:
Related Outputs:
Latency:
Time After Output:
Exception-Handling:
Obsolescence:
Exception-Handling:
Description:
Comments:
References:
Appears In: (↑A&AC-2.2.1.12, HA&T-2.2), (←3. ShoulderRollLockPosition)

DEFINITION

= New Data for ShoulderRollLockPositionMSMT

ShoulderRollLockPositionMSMT was Received	T

= Previous Value of ShoulderRollLockPositionMSMT

ShoulderRollLockPositionMSMT was Received	F
Time Since ShoulderRollLockPositionMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
ShoulderRollLockPositionMSMT was Never Received	T	T	*
Time Since ShoulderRollLockPositionMSMT was Last Received > TBD seconds	*	*	T

Input Value

ShoulderPitchMSMT

Source: Shoulder Pitch Encoder
Type: Integer
Possible Values (Expected Range): [0..TBD]
Units: milliradians
Granularity:
Exception-Handling: None
Timing Behavior:
Load:
Minimum Time Between Inputs:
Maximum Time Between Inputs:
Maximum Time Before First Input:
Related Outputs:
Latency:
Time After Output:
Exception-Handling:
Obsolescence:
Exception-Handling:

Description:
Comments:
References:
Appears In: (↑A&AC-2.2.1.5, HA&T-2.1)

DEFINITION

= New Data for ShoulderPitchMSMT

ShoulderPitchMSMT was Received	T

= Previous Value of ShoulderPitchMSMT

ShoulderPitchMSMT was Received	F
Time Since ShoulderPitchMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
ShoulderPitchMSMT was Never Received	T	T	*
Time Since ShoulderPitchMSMT was Last Received > TBD seconds	*	*	T

Input Value

ShoulderPitchLockPositionMSMT

Source: Shoulder Pitch Lock Sensor
Type: {Engaged, Disengaged}
Possible Values (Expected Range): Any
Units:
Granularity:
Exception-Handling: None
Timing Behavior:
Load:
Minimum Time Between Inputs:
Maximum Time Between Inputs:
Maximum Time Before First Input:
Related Outputs:
Latency:
Time After Output:
Exception-Handling:
Obsolescence:
Exception-Handling:
Description:
Comments:
References:
Appears In: (↑A&AC-2.2.1.12, HA&T-2.2)

DEFINITION

= New Data for ShoulderPitchLockPositionMSMT

ShoulderPitchLockPositionMSMT was Received	T

= Previous Value of ShoulderPitchLockPositionMSMT

ShoulderPitchLockPositionMSMT was Received	F
Time Since ShoulderPitchLockPositionMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
ShoulderPitchLockPositionMSMT was Never Received	T	T	*
Time Since ShoulderPitchLockPositionMSMT was Last Received > TBD seconds	*	*	T

Input Value

ElbowRollMSMT

Source: Elbow Roll Encoder
Type: Integer
Possible Values (Expected Range): [0..TBD]
  Units: milliradians
  Granularity:
  Exception-Handling: None
Timing Behavior:
  Load:
  Minimum Time Between Inputs:
  Maximum Time Between Inputs:
  Maximum Time Before First Input:
  Related Outputs:
    Latency:
    Time After Output:
  Exception-Handling:
Obsolescence:
  Exception-Handling:
Description:
Comments:
References:
Appears In: (↑A&AC-2.2.1.5, HA&T-2.1)

DEFINITION

= New Data for ElbowRollMSMT

ElbowRollMSMT was Received	T

= Previous Value of ElbowRollMSMT

ElbowRollMSMT was Received	F
Time Since ElbowRollMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
ElbowRollMSMT was Never Received	T	T	*
Time Since ElbowRollMSMT was Last Received > TBD seconds	*	*	T

Input Value

ElbowRollLockPositionMSMT

Source: Elbow Roll Lock Sensor
Type: {Engaged, Disengaged}
Possible Values (Expected Range): Any
  Units:
  Granularity:
  Exception-Handling: None
Timing Behavior:
  Load:
  Minimum Time Between Inputs:
  Maximum Time Between Inputs:
  Maximum Time Before First Input:
  Related Outputs:
    Latency:
    Time After Output:
  Exception-Handling:
Obsolescence:
  Exception-Handling:
Description:
Comments:
References:
Appears In: (↑A&AC-2.2.1.12, HA&T-2.2)

DEFINITION

= New Data for ElbowRollLockPositionMSMT

ElbowRollLockPositionMSMT was Received	T

= Previous Value of ElbowRollLockPositionMSMT

ElbowRollLockPositionMSMT was Received	F
Time Since ElbowRollLockPositionMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
ElbowRollLockPositionMSMT was Never Received	T	T	*
Time Since ElbowRollLockPositionMSMT was Last Received > TBD seconds	*	*	T

Input Value

ElbowPitchMSMT

Source: Elbow Pitch Encoder
Type: Integer
Possible Values (Expected Range): [0..TBD]
  Units: milliradians
  Granularity:

Exception-Handling: None
Timing Behavior:
Load:
Minimum Time Between Inputs:
Maximum Time Between Inputs:
Maximum Time Before First Input:
Related Outputs:
Latency:
Time After Output:
Exception-Handling:
Obsolescence:
Exception-Handling:
Description:
Comments:
References:
Appears In: (↑A&AC-2.2.1.5, HA&T-2.1)

DEFINITION

= New Data for ElbowPitchMSMT

ElbowPitchMSMT was Received	T

= Previous Value of ElbowPitchMSMT

ElbowPitchMSMT was Received	F
Time Since ElbowPitchMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
ElbowPitchMSMT was Never Received	T	T	*
Time Since ElbowPitchMSMT was Last Received > TBD seconds	*	*	T

Input Value

ElbowPitchLockPositionMSMT

Source: Elbow Pitch Lock Sensor
Type: {Engaged, Disengaged}
Possible Values (Expected Range): Any
Units:
Granularity:
Exception-Handling: None
Timing Behavior:
Load:
Minimum Time Between Inputs:
Maximum Time Between Inputs:
Maximum Time Before First Input:
Related Outputs:
Latency:
Time After Output:
Exception-Handling:
Obsolescence:
Exception-Handling:

Description:
Comments:
References:
Appears In: (↑A&AC-2.2.1.12, HA&T-2.2)

DEFINITION

= New Data for ElbowPitchLockPositionMSMT

ElbowPitchLockPositionMSMT was Received	T

= Previous Value of ElbowPitchLockPositionMSMT

ElbowPitchLockPositionMSMT was Received	F
Time Since ElbowPitchLockPositionMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
ElbowPitchLockPositionMSMT was Never Received	T	T	*
Time Since ElbowPitchLockPositionMSMT was Last Received > TBD seconds	*	*	T

Input Value

WristRollMSMT

Source: Wrist Roll Encoder
Type: Integer
Possible Values (Expected Range): [0..TBD]
  Units: milliradians
  Granularity:
  Exception-Handling: None
Timing Behavior:
  Load:
  Minimum Time Between Inputs:
  Maximum Time Between Inputs:
  Maximum Time Before First Input:
  Related Outputs:
    Latency:
    Time After Output:
  Exception-Handling:
Obsolescence:
  Exception-Handling:
Description:
Comments:
References:
Appears In: (↑A&AC-2.2.1.5, HA&T-2.1)

DEFINITION

= New Data for WristRollMSMT

WristRollMSMT was Received	T

= Previous Value of WristRollMSMT

WristRollMSMT was Received	F
Time Since WristRollMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
WristRollMSMT was Never Received	T	T	*
Time Since WristRollMSMT was Last Received > TBD seconds	*	*	T

Input Value

WristRollLockPositionMSMT

Source: Wrist Roll Lock Sensor
Type: {Engaged, Disengaged}
Possible Values (Expected Range): Any
Units:
Granularity:
Exception-Handling: None
Timing Behavior:
Load:
Minimum Time Between Inputs:
Maximum Time Between Inputs:
Maximum Time Before First Input:
Related Outputs:
Latency:
Time After Output:
Exception-Handling:
Obsolescence:
Exception-Handling:
Description:
Comments:
References:
Appears In: (↑A&AC-2.2.1.12, HA&T-2.2)

DEFINITION

= New Data for WristRollLockPositionMSMT

WristRollLockPositionMSMT was Received	T

= Previous Value of WristRollLockPositionMSMT

WristRollLockPositionMSMT was Received	F
Time Since WristRollLockPositionMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
WristRollLockPositionMSMT was Never Received	T	T	*
Time Since WristRollLockPositionMSMT was Last Received > TBD seconds	*	*	T

Input Value

WristPitchMSMT

Source: Wrist Pitch Encoder
Type: Integer
Possible Values (Expected Range): [0..TBD]
  Units: milliradians
  Granularity:
  Exception-Handling: None
Timing Behavior:
  Load:
  Minimum Time Between Inputs:
  Maximum Time Between Inputs:
  Maximum Time Before First Input:
  Related Outputs:
    Latency:
    Time After Output:
  Exception-Handling:
Obsolescence:
  Exception-Handling:
Description:
Comments:
References:
Appears In: (↑A&AC-2.2.1.5, HA&T-2.1)

DEFINITION

= New Data for WristPitchMSMT

WristPitchMSMT was Received	T

= Previous Value of WristPitchMSMT

WristPitchMSMT was Received	F
Time Since WristPitchMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
WristPitchMSMT was Never Received	T	T	*
Time Since WristPitchMSMT was Last Received > TBD seconds	*	*	T

Input Value

WristPitchLockPositionMSMT

Source: Wrist Pitch Lock Sensor
Type: {Engaged, Disengaged}
Possible Values (Expected Range): Any
  Units:
  Granularity:
  Exception-Handling: None

Timing Behavior:
Load:
Minimum Time Between Inputs:
Maximum Time Between Inputs:
Maximum Time Before First Input:
Related Outputs:
Latency:
Time After Output:
Exception-Handling:
Obsolescence:
Exception-Handling:
Description:
Comments:
References:
Appears In: (↑A&AC-2.2.1.12, HA&T-2.2)

DEFINITION

= New Data for WristPitchLockPositionMSMT

WristPitchLockPositionMSMT was Received	T

= Previous Value of WristPitchLockPositionMSMT

WristPitchLockPositionMSMT was Received	F
Time Since WristPitchLockPositionMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
WristPitchLockPositionMSMT was Never Received	T	T	*
Time Since WristPitchLockPositionMSMT was Last Received > TBD seconds	*	*	T

Input Value

SunAngleMSMT

Source: HGA Sun Sensor
Type: Integer
Possible Values (Expected Range): [0..TBD]
Units: milliradians
Granularity:
Exception-Handling: None
Timing Behavior:
Load:
Minimum Time Between Inputs:
Maximum Time Between Inputs:
Maximum Time Before First Input:
Related Outputs:
Latency:
Time After Output:
Exception-Handling:
Obsolescence:
Exception-Handling:
Description:

Comments:
References:
Appears In: (↑A&AC-2.2.1.11)

DEFINITION

= New Data for SunAngleMSMT

SunAngleMSMT was Received	T

= Previous Value of SunAngleMSMT

SunAngleMSMT was Received	F
Time Since SunAngleMSMT was Last Received <= TBD seconds	T

= Obsolete

System Start	T	*	*
SunAngleMSMT was Never Received	T	T	*
Time Since SunAngleMSMT was Last Received > TBD seconds	*	*	T

Further specification of the inputs for this black box model is beyond the scope of this study.

3 Derivation of Basic High-Gain Antenna (HGA) Boom Configurations for OPE

In this section, the derivation of the basic HGA boom configurations, design decision A&AC-2.2.1, is presented.

Adapting the scientific goals from an early study of a Europa mission[3], we have the following goal (shown in Figure 1), among others:

G1. Characterize the presence of a subsurface ocean on an icy moon of an outer planet. (↑ACC4, ACC5), (→HLR3, HLR4), (↓SV-81)

Figure 1. Derivation of the basic HGA boom configuration (part 1 of 11).

This goal establishes the need for the following high-level requirement (shown in Figure 2), among others:

HLR3. The mission shall image TBD% of the surface of the icy moon of the outer planet in spectra other than visual and infrared, to a resolution of TBD. (←G1, G2, G3, G4, G6), (→S/C-G1, S/C-G2, S/C-R1, S/C-R2), (↓2.1, SV-1, SV-101, SV-102)
Rationale: The bands of the spectrum other than infrared and visual provide insights into the chemical composition of the icy moon

Figure 2. Derivation of the basic HGA boom configuration (part 2 of 11).

Given this requirement and the design constraint and assumptions in Figure 3, we decide that we need to send a spacecraft to make the required observations. This design decision is captured in Figure 4.

DC1. The mission must be carried out with existing technologies and space exploration infrastructures as needed (i.e., technologies rated at Technology Readiness Level TBD as defined by NASA). (↓2.1)
Rationale: While technology development is expected to be an ongoing activity of NASA, it is assumed to be beyond the mandate of the mission.

A1. Technology for Earth-based observation of outer planets and their moons is inadequate to achieve the mission goals. (↓2.1)

A2. Technology for Low Earth Orbit based observation of outer planets and their moons is inadequate to achieve the mission goals. (↓2.1)

Figure 3. Derivation of the basic HGA boom configuration (part 3 of 11).

[3]Karla Clark, "Europa Explorer—An Exceptional Mission Using Existing Technology," *2007 IEEE Aerospace Conference Proceedings*, Big Sky, MT, March 3–10, 2007.

2.1. A new spacecraft will be used for data collection (↑HLR1, HLR2, HLR3, HLR4, HLR5, DC1, SC1, SC2, SC3, SC4, SC5, SC6, SC7, SC8, SC9, A1, A2, MOC-G1), (→2.2, 2.3, 2.4, 2.5, S/C-2.1, SV-1, SV-2)
Rationale: The data cannot be collected from Earth's surface or orbit. Additionally, no existing spacecraft design will be able to accomplish the mission goals.

Figure 4. Derivation of the basic HGA boom configuration (part 4 of 11).

In order for the spacecraft to execute the directives of the human operators of the spacecraft, the spacecraft will need a command and data handling (C&DH) functional element to evaluate these directives, assign them to functional elements of the spacecraft, and otherwise manage the interactions between functional elements of the spacecraft. This need is captured by the design decision in Figure 5.

S/C-2.1. The interfaces of the spacecraft-level functional elements are monitored and managed by a spacecraft command and data handling (C&DH) functional element that translates directives generated by the MOC (after they have been transmitted through the GN or DSN and demodulated) into directives for other functional elements after evaluating if the conditions for the directives are satisfied. (↑S/C-C4, S/C-R3, S/C-R5, S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC4, S/C-SC5, S/C-SC6, S/C-SC7, C&DH-G1), (←2.1)
Rationale: A central concept in control and systems theory is that of hierarchy. By definition, control involves the imposition of constraints from one level of the control hierarchy to a lower level [13]. The C&DH functional element represents control on the spacecraft-level while the other functional elements mentioned in this design principle all control lower-level functions and need a higher-level controller to manage their interactions with each other.

Figure 5. Derivation of the basic HGA boom configuration (part 5 of 11).

In defining the (C&DH) functional element we establish the functional element goal shown in Figure 6.

C&DH-G1. To monitor the health and manage the interfaces of the following spacecraft-level functional elements: Electrical Power (EP), Attitude and Articulation Control (A&AC), Science Data Collection (SCI), and Communications Signal Processing (COM). (←S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC4, S/C-SC5, S/C-SC6, S/C-SC7), (→C&DH-R1, C&DH-R2, C&DH-R3, C&DH-R4, C&DH-R5, C&DH-R6, C&DH-R7, C&DH-R8, C&DH-R9), (↓S/C-2.1, S/C-2.2, S/C-2.3, S/C-2.4, S/C-2.5)

Figure 6. Derivation of the basic HGA boom configuration (part 6 of 11).

The requirement in Figure 7 is among the many requirements necessary to fulfill this goal.

C&DH-R7. The C&DH shall provide spacecraft attitude directives to the A&AC in accordance with the needs of the COM and SCI functional elements. (←C&DH-G1), (↓C&DH-2.1.6, SV-1, SV-2)
Rationale: Spacecraft attitude affects both science data collection and spacecraft-to-Earth communications.

Figure 7. Derivation of the basic HGA boom configuration (part 7 of 11).

Requirement C&DH-R7 is fulfilled through design decision C&DH-2.1.6 and its refinements (refer to Figure 8).

C&DH-2.1.6. The C&DH provides attitude and translation directives to the A&AC functional element in accordance with SCI and COM subsystem needs and MOC Directives. (↑C&DH-R6, C&DH-R7, C&DH-C1, A&AC-C2), (→SV-1, SV-2)
…
C&DH-2.1.6.3. The C&DH receives a 'Science Data Collection' State Information input from the SCI functional element and uses this information to update directives for the A&AC and SCI health and status data. (↑C&DH-ICA10)

Figure 8. Derivation of the basic HGA boom configuration (part 8 of 11).

Design decision C&DH-2.1.6.3 creates the potential for the inadequate control action shown in Figure 9, through the listed control flaw.

C&DH-ICA10. The C&DH determines the wrong directives for the A&AC when considering the Science Data Collection State Information. (←S/C-SC1, S/C-SC2), (↓C&DH-2.1.6.3)

C&DH-CF10.1. During periods of simultaneous data communication with the DSN or GN and science data collection, the C&DH issues directives for the A&AC that degrades one of the two functions.

Figure 9. Derivation of the basic HGA boom configuration (part 9 of 11).

The inadequate control action in Figure 9 relates to both Hazard 1: Inability of Mission to collect data and Hazard 2: Inability of Mission to return collected data, which relate back to accidents ACC4 and ACC5, respectively. The safety constraint shown in Figure 10 is warranted to prevent these hazards.

C&DH-SC11. During times of simultaneous communication with the DSN or GN and science data collection, the C&DH must provide directives to the A&AC that do not degrade either function. (←H1, H2), (↓A&AC-2.1, A&AC-2.2)

Figure 10. Derivation of the basic HGA boom configuration (part 10 of 11).

Enforcing this constraint can involve several aspects of the spacecraft system design ranging from C&DH logic design to the physical design of the antenna and data collection instruments. Two of the design decisions made to enforce this constraint are provided in Figure 11. Finally, A&AC-2.2 refines directly into A&AC-2.2.1.

A&AC-2.1. The A&AC functional element rotates the HGA relative to the main structure of the spacecraft. (↑A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, C&DH-SC11, A&AC-ICA1, A&AC-ICA2), (→COM-2.1, A&AC-2.2, AC&DH-2.1.2, A&AC-2.4, SV-15, SV-18)
Rationale: Having the HGA articulate relative to the spacecraft decouples antenna pointing from science data collection. If the HGA was spacecraft-fixed, the spacecraft as a whole would have to rotate, possibly altering science data collection instrument pointing (which is essential to satisfactory data collection).

A&AC-2.2. The A&AC functional element translates the HGA relative to the main spacecraft structure. (←A&AC-2.1), (↑A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, C&DH-SC11, A&AC-ICA3, A&AC-ICA4), (→SV-4, SV-7, SV-11, SV-15)
Rationale: Translating (or deploying) the HGA away from the main spacecraft structure allows for a wider range of rotation of the HGA (i.e., it distances the HGA from other parts of the spacecraft that it could collide with). It also distances the HGA from potential EMI noise sources in the main spacecraft structure.

Figure 11. Derivation of the basic HGA boom configuration (part 11 of 11).

It is worth noting that design decisions A&AC-2.1 and A&AC-2.2 relate to several state variables (e.g., HGA Frame Position and Orientation with respect to Spacecraft, HGA Boom Elbow Joint Frame Position and Orientation with respect to Spacecraft, HGA Wrist Joint Position and Orientation with respect to Spacecraft, etc.) that will be used in the HGA pointing control laws. Also, it is worth noting that the design decision to articulate the HGA also relates to volume constraints for the spacecraft while it is in the launch vehicle. This constraint-design relationship is derived from an additional thread in the intent specification that split off from the one described in this appendix after design decision 2.1. That thread diverged from the one in this appendix to capture launch vehicle selection and the corresponding volume constraints resulting from that selection. Ultimately, these threads partially re-converged at design decision A&AC-2.2.1, as it was the first design decision to describe volume and packaging characteristics of the HGA boom.

4 Safety-Related Trade Study of HGA Boom Design Options for OPE

Designers typically have many design options for enforcing safety-related constraints and the options that they ultimately choose greatly affect the cost and efficacy of constraint enforcement. In this section, we present a brief, comparative analysis of design options considered for the enforcement of specific safety-related constraints in the OPE Intent Specification. Because the development of methodologies for exploration of the safety-related constraint tradespace was beyond the scope of this study, the analysis presented here is minimal and introductory. While previous research[4] in this area has been conducted by the MIT Complex Systems Research Laboratory, the topic is still very much an open area of study.

In this trade study, we are concerned with the inadequate control actions and control flaws related to rotation of the High Gain Antenna (HGA) boom joints.

The following requirements and constraints established the need for a parabolic antenna and mechanisms to articulate it[5]:

[4] Dulac, Nicolas and Leveson, Nancy G. (2004), "Incorporating Safety in Early System Architecture Trade Studies," *Proceedings of the 2004 International System Safety Conference*, San Diego, CA.

[5] Detailed information relating to the derivation of these requirements is available in the full intent specification and the preceding section of this report.

COM-R5. The COM functional element shall radiate the modulated spacecraft data at frequencies ranging from TBD GHz to TBD GHz. (←COM-G1, COM-G2), (↓COM-2.1)

COM-R6. The COM functional element shall absorb radiated signals from the DSN and/or GN and convert them into electrical signals. (←COM-G3, COM-G4), (↓COM-2.1)

COM-C1. All communications signal-processing components must fit within TBD% of the space beneath the payload fairing of a Delta-IVH. (←S/C-C2), (→COM-A1), (↓COM-2.1.2)

Rationale: Space is a limited resource inside the payload fairing of a launch vehicle and thus, space for each component of the spacecraft must be carefully budgeted. The space allocation process involves a number of architectural tradeoffs beyond the scope of this study. Therefore, we will use a TBD% space allocation to the communications functional elements.

A&AC-R7. The A&AC shall articulate all necessary antennas relative to the main spacecraft structure as needed for radiation of modulated data and carrier signal to the GN. (←A&AC-G2), (↓A&AC-2.1, A&AC-2.2)

A&AC-R8. The A&AC shall articulate all necessary antennas relative to the main spacecraft structure as needed for radiation of modulated data and carrier signal to the DSN. (←A&AC-G2), (↓A&AC-2.1, A&AC-2.2)

A&AC-R9. The A&AC shall articulate all necessary antennas relative to the main spacecraft structure as needed for reception of signals radiated from the GN. (←A&AC-G2), (↓A&AC-2.1, A&AC-2.2)

A&AC-R10. The A&AC shall articulate all necessary antennas relative to the main spacecraft structure as needed for reception of signals radiated from the DSN. (←A&AC-G2), (↓A&AC-2.1, A&AC-2.2)

These requirements and constraints led to the following design principles:

COM-2.1. A passive (i.e., no electrical power is required to convert the processed electrical signal to radiation) High Gain Antenna (HGA) is deployed on the spacecraft for bi-directional communication over the DSN and GN operating frequencies. (↑COM-R5, COM-R6), (←A&AC-2.1)

COM-2.1.1. The antenna converts the processed electrical signal modulated with packetized data into focused electromagnetic radiation on DSN and GN operating frequencies. Similarly, the antenna converts received electromagnetic radiation into electrical signals.

COM-2.1.2. The High Gain Antenna (HGA) is composed of a 3-meter parabolic dish which efficiently increases the Signal to Noise Ratio of the communications link by utilizing a directional radiation pattern. (↑COM-A1, COM-A2, COM-C1)

Rationale: Antenna geometry is a major factor in strength of a communications link. A parabolic shape focuses the power of the radiated signal in a specific direction, thereby increasing the strength of the signal when it is ultimately received. Due to the assumed detrimental effects of stowing the HGA in a non-parabolic shape while it is in the launch vehicle, the HGA will be a stowed in a parabolic shape and thus can be no larger than 3 meters in diameter.

A&AC-2.1. The A&AC functional element rotates the HGA relative to the main structure of the spacecraft. (↑A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, C&DH-SC11, A&AC-ICA1, A&AC-ICA2), (→A&AC-2.2, AC&DH-2.1.2, A&AC-2.4, COM-2.1, SV-15, SV-18)

Rationale: Having the HGA articulate relative to the spacecraft decouples antenna pointing from science data collection. If the HGA were spacecraft-fixed, the spacecraft as a whole would have to rotate, possibly altering science data collection instrument pointing (which is essential to satisfactory data collection).

A&AC-2.2. The A&AC functional element translates the HGA relative to the main spacecraft structure. (←A&AC-2.1), (↑A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, C&DH-SC11, A&AC-ICA3, A&AC-ICA4), (→SV-4, SV-7, SV-11, SV-15)

Rationale: Translating (or deploying) the HGA away from the main spacecraft structure allows for a wider range of rotation of the HGA (i.e., it distances the HGA from other parts of the spacecraft that it could collide with). It also distances the HGA from potential EMI noise sources in the main spacecraft structure.

Accordingly, the rotation and translation of the HGA mentioned in these design principles presented the possibility of the following inadequate control actions and control flaws:

A&AC-ICA1. The HGA rotates relative to the spacecraft at the wrong time. (→S/C-SC1, S/C-SC2, S/C-SC5, S/C-SC7), (↓A&AC-2.1)

A&AC-CF1.1. The HGA rotates relative to the spacecraft while the spacecraft is within the payload fairing.

Rationale: Because space is constrained within the payload fairing, articulation of the HGA relative to the spacecraft could cause damage to the HGA, Launch Vehicle, and/or other parts of the spacecraft. The effects of such damage could range from degradation in HGA functionality to partial break up of the spacecraft and launch vehicle.

A&AC-ICA2. The HGA rotates too quickly or too much with respect to the spacecraft. (→S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC5, S/C-SC7), (↓A&AC-2.1)

A&AC-CF2.2. Other parts of the spacecraft are within the allowable range of HGA rotation and signal radiation.

A&AC-CF2.3. An unidentified mechanical disturbance induces rotational oscillation of the HGA about its desired rotation setpoint. (↓SV-3, SV-5, SV-6, SV-10, SV-14)

Rationale: Mechanical disturbances include interactions with the spacecraft's environment (e.g., micrometeorite impacts, atmospheric drag, etc.) as well as vibrations created by processes performed by the spacecraft's other functional elements (e.g., power generation, etc.)

A&AC-ICA3. The HGA translates relative to the main spacecraft structure at the wrong time. (→S/C-SC1, S/C-SC2, S/C-SC5, S/C-SC7), (↓A&AC-2.2)

A&AC-CF3.1. The HGA translates relative to the main spacecraft structure while the spacecraft is within the payload fairing. (↓SV-21)

A&AC-ICA4. The HGA translates relative to the main spacecraft structure too much or too quickly. (→S/C-SC1, S/C-SC2, S/C-SC3, S/C-SC5, S/C-SC7), (↓A&AC-2.2)

A&AC-CF4.2. Other parts of the spacecraft are within the allowable range of HGA translation and signal radiation.

A&AC-CF4.3. An unidentified mechanical disturbance induces translational oscillation of the HGA about its desired translation setpoint. (↓SV-3, SV-5, SV-6, SV-10, SV-14)

Rationale: Mechanical disturbances include interactions with the spacecraft's environment (e.g., micrometeorite impacts, atmospheric drag, etc.) as well as vibrations created by processes performed by the spacecraft's other functional elements (e.g., power generation, etc.)

These inadequate control actions and control flaws can instantiate the following hazards:

H1. Inability of Mission to collect data.

Rationale: The HGA could collide with data collection instruments.

H2. Inability of Mission to return collected data.

Rationale: The mission cannot return data if the HGA loses functionality after a collision with another element of the spacecraft or if the loads creating HGA oscillation are too large.

H4. Contamination of Outer Planet Moon with biological agents of Earth origin on mission hardware. (←A4, A5)

Rationale: A collision between the HGA and any part of the spacecraft or launch vehicle and/or extreme vibration of the HGA could create orbital debris. If such an event were to occur in orbit of the outer planet moon, the debris, which may not be properly sterilized, could eventually make its way to the surface of the outer planet moon.

H5. Exposure of Earth life or human assets on Earth to toxic, radioactive, and/or energetic elements of mission hardware.

Rationale: A collision between the HGA and any other part of the spacecraft or launch and/or extreme vibration of the HGA could create orbital debris that could eventually re-enter the Earth's atmosphere in an uncontrolled manner.

H6. Exposure of Earth life or human assets off Earth to toxic, radioactive, and/or energetic elements of mission hardware.

Rationale: A collision between the HGA and any other part of the spacecraft and/or extreme vibration of the HGA could create orbital debris.

H7. Inability of other space exploration missions to use shared space exploration infrastructure to collect, return, and/or use data.

Rationale: A collision between the HGA and any other part of the spacecraft or launch vehicle and/or extreme vibration of the HGA could create orbital debris that could impact elements of the GN or DSN. Also, in extreme cases, the launch pad could be damaged.

These control flaws and inadequate control flaws are unacceptable and necessitate further constraint of the system behavior. Thus, the following safety-related design constraints were derived:

A&AC-SC1. The HGA must not rotate or translate with respect to the main spacecraft structure while the spacecraft is inside the payload fairing of the launch vehicle. (←H1, H2, H5, H6, H7), (↓A&AC-2.2.1.4, A&AC-2.2.1.8, A&AC-2.3, A&AC-2.4), (→A&AC-ICA10, A&AC-ICA11, AC&DH-G1, HA&T-G1, HA&T-G2, HA&T-G3)

A&AC-SC3. While translating and/or rotating, the HGA and the radiation it emits must maintain minimum separation from other parts of the spacecraft. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.2.1.5, A&AC-2.3, A&AC-2.4, AC&DH-2.1.2, A&AC-2.2.1.9), (→A&AC-ICA10, A&AC-ICA11, AC&DH-G1, HA&T-G1, HA&T-G2)

A&AC-SC7. Mechanical disturbances to the HGA must not create rotational or translational oscillations of the HGA that are large enough to prevent data return. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.3, A&AC-2.4 SV-3, SV-5, SV-6, SV-10, SV-14), (→A&AC-ICA10, AC&DH-G1, AC&DH-C4, HA&T-G1, HA&T-G2, HA&T-G3)

Before implementing these constraints in the design, we made the following assumptions:

A&AC-A1. Telescoping boom segments for the HGA are not practical for this mission. (↓A&AC-2.2.1)

Rationale: While this assumption is largely a simplifying assumption, the complexity associated with telescoping boom segments for an object as massive as the HGA would warrant a trade study beyond the scope of this study if they were to be considered.

A&AC-A2. Four or more HGA boom joints are not practical for this mission. (↓A&AC-2.2.1)

Rationale: While this assumption is largely a simplifying assumption, the complexity associated with four or more boom joints would warrant a trade study beyond the scope of this study if they were to be considered.

Given these assumptions and the requirements and constraints above, we developed the following design principle to describe the basic structure of the HGA boom:

A&AC-2.2.1. The HGA boom consists of 3 rotation joints (shoulder, elbow, and wrist) driven by TBD electric motors and connected by 2 solid (i.e., non-telescoping) boom segments. (↑A&AC-A1, A&AC-A2, A&AC-C1, HA&T-G2), (←A&AC-2.1.1)

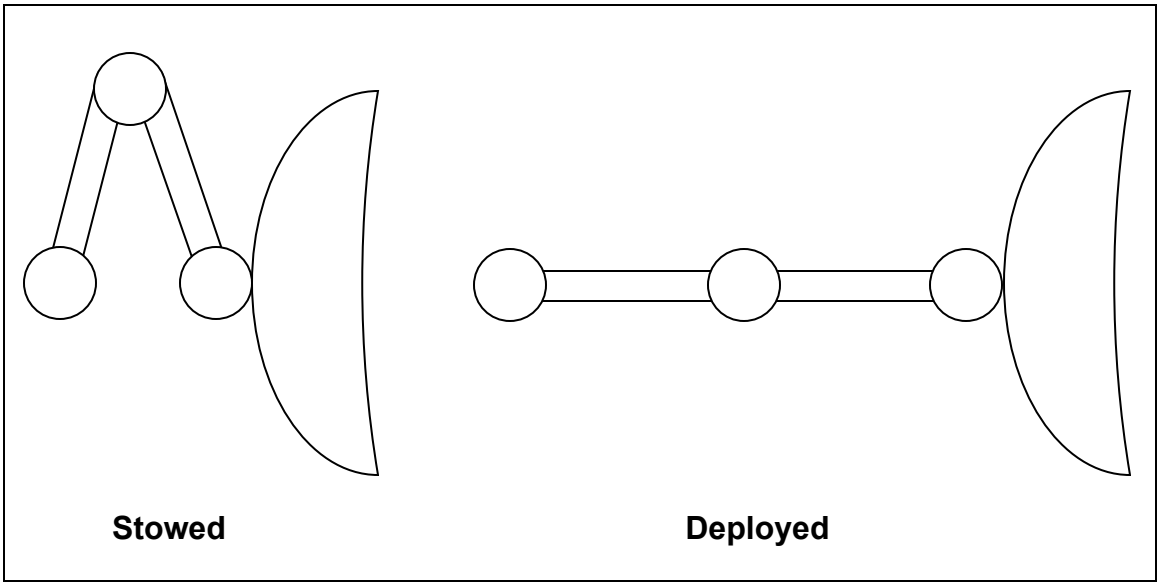


Figure 12. The HGA boom in the stowed and deployed configurations.

This design principle specifies a boom architecture in which the HGA translates and rotates through rotation of the three rotation joints. Figure 12 above illustrates the stowed and deployed configurations of the HGA boom. However, further specification of the rotation joints is necessary to evaluate the efficacy of the enforcement of A&AC-SC1, A&AC-SC3, and A&AC-SC7. The design variables of interest are: the rotational degrees of freedom in each joint, the presence and capability of mechanical locks on each degree of freedom, and the type of actuator used for each degree of freedom. Accordingly, the tradespace that was considered in this study is described in Table 3 below. All design options include a pitch degree of freedom in each joint and a roll degree of freedom in the wrist joint. Pitch is required in each joint for deployment and roll is required in the wrist in order to create a hemispherical range of HGA motion. In each design, wrist roll and pitch are the primary degrees of freedom used for HGA articulation after deployment and thus, these degrees of freedom are actuated by motors. In some options, redundant pointing capabilities are provided by pitch and roll degrees of freedom in the elbow and shoulder joints and thus these degrees of freedom are also actuated by motors. In Option 5, no redundancy is provided as the pitch degrees of freedom are only used for deployment and are actuated by damped springs. Finally, while all options include locks on all of the available degrees of freedom to restrict rotation while the HGA is under the payload fairing, only two include locks that can be re-engaged after HGA boom deployment.

Design Option	Shoulder Roll	Shoulder Pitch	Elbow Roll	Elbow Pitch	Wrist Roll	Wrist Pitch	Rotation Locks	Rotation Lock Sensors
Option 1	Available as 2nd Backup to Wrist Roll (motorized)	Used for deployment and available as 2nd Backup to Wrist Pitch (motorized)	Available as 1st Backup to Wrist Roll (motorized)	Used for deployment and available as 1st Backup to Wrist Pitch (motorized)	Primary Roll DOF for HGA Pointing (motorized)	Primary Pitch DOF for HGA Pointing (motorized)	Can be selectively engaged/disengaged throughout mission	Six
Option 2	Available as 2nd Backup to Wrist Roll (motorized)	Used for deployment and available as 2nd Backup to Wrist Pitch (motorized)	Available as 1st Backup to Wrist Roll (motorized)	Used for deployment and available as 1st Backup to Wrist Pitch (motorized)	Primary Roll DOF for HGA Pointing (motorized)	Primary Pitch DOF for HGA Pointing (motorized)	Engaged for pre-deployment phases and permanently disengaged at deployment[6]	Six
Option 3	Not Available	Used for deployment and available as 2nd Backup to Wrist Pitch (motorized)	Not Available	Used for deployment and available as 1st Backup to Wrist Pitch (motorized)	Primary Roll DOF for HGA Pointing (motorized)	Primary Pitch DOF for HGA Pointing (motorized)	Can be selectively engaged/disengaged throughout mission	Four
Option 4	Not Available	Used for deployment and available as 2nd Backup to Wrist Pitch (motorized)	Not Available	Used for deployment and available as 1st Backup to Wrist Pitch (motorized)	Primary Roll DOF for HGA Pointing (motorized)	Primary Pitch DOF for HGA Pointing (motorized)	Engaged for pre-deployment phases and permanently disengaged at deployment	Four
Option 5	Not Available	Used for deployment only (spring-loaded)	Not Available	Used for deployment only (spring-loaded)	Primary Roll DOF for HGA Pointing (motorized)	Primary Pitch DOF for HGA Pointing (motorized)	Engaged for pre-deployment phases and permanently disengaged at deployment	Four

Table 3. Design options considered in this study for HGA Boom Joint Rotation.

[6] After deployment, locking of the joints is only provided by actuation of the joint motors.

In the interest of the brevity, only two of the design options (Option 1 and Option 5) in Table 3 above are expanded on. These options represent opposite extremes of the design tradespace that was evaluated.

Design Option 1

Option 1 in Table 3 would lead to the following design principles:

A&AC-2.2.1.1. Each rotation joint has two rotational degrees of freedom: roll and pitch. (→A&AC-2.2.1.3, A&AC-2.2.1.5, A&AC-2.2.1.6, A&AC-2.2.1.7, A&AC-2.2.1.8, AC&DH-2.1.1.1, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17)

Rationale: Though roll has no direct effect on the translation of material downstream of the rotation joint or the HGA's beam direction, it can be coupled with pitch or yaw to create a hemispheric range of motion for beam pointing or material translation.

A&AC-2.2.1.2. The HGA boom segments are TBD meters long cylindrical shells, each TBD centimeters thick. (↑A&AC-A1, A&AC-C1)

A&AC-2.2.1.3. Translation of the HGA with respect to the main spacecraft structure is controlled through rotation of HGA boom segments. (←A&AC-2.2.1.1)

A&AC-2.2.1.4. Each HGA Boom rotation joint degree of freedom can be restrained during launch, spacecraft velocity changes, and as otherwise needed by TBD mechanical locks that can be engaged electrically. While electrical power is required to change the state of the locks (i.e., engaged, disengaged), no power is required to maintain the current state of the locks. (↑A&AC-SC1, A&AC-SC2, A&AC-ICA11, HA&T-G2), (→A&AC-2.2.1.12, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42, SV-43, SV-44, SV-45, SV-46, SV-47, SV-48)

A&AC-2.2.1.5. Each HGA boom rotation joint degree of freedom is measured every TBD seconds by an angle encoder. (↑A&AC-C3, A&AC-C4, A&AC-SC3, A&AC-SC6, A&AC-ICA10, HA&T-G1, HA&T-G3), (←A&AC 2.2.1.1), (→A&AC-2.2.1.11, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17), (↓3.ShoulderRollMSMT, 3.ShoulderPitchMSMT, 3.ElbowRollMSMT, 3.ElbowPitchMSMT, 3.WristRollMSMT, 3.WristPitchMSMT)

A&AC-2.2.1.6. The maximum range of pitch rotation at each joint is TBD radians in the forward and reverse directions with the zero radian defined by the angle in which the boom segment (or antenna center) downstream of the joint is parallel to the boom segment upstream of the joint. (←A&AC 2.2.1.1), (→SV-9, SV-13, SV-17)

A&AC-2.2.1.7. The maximum range of roll rotation at each joint is TBD Radians in the forward and reverse directions. (←A&AC 2.2.1.1), (→SV-8, SV-12, SV-16)

A&AC-2.2.1.8. Rotation in each rotational degree of freedom is created and resisted, as needed, by an electric motor when the locks on the degree of freedom are disengaged. (←A&AC 2.2.1.1), (↑A&AC-SC1, A&AC-ICA9, A&AC-ICA10, A&AC-ICA11), (→SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-25, SV-26, SV-27, SV-28, SV-29, SV-30, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

A&AC-2.2.1.9. To the extent that it is prudent, the HGA Boom will be mounted on a part of the main spacecraft structure that reduces the overlap in its range of articulation and signal radiation with the range of articulation of other spacecraft appendages. (↑A&AC-SC3)

With these design principles defined, we can elaborate on spacecraft-level safety constraints in addition to evaluating how well this design option enforces A&AC-SC1, A&AC-SC3, and A&AC-SC7. Because joint rotation depends on the performance of motors and locks, we now have an inadequate control action relating to the Hazard 2, inability of the spacecraft to return collected data: A&AC-ICA9. Furthermore, the design option does not eliminate the possibility of not enforcing A&AC-SC1, A&AC-SC3, and A&AC-SC7. Thus, we now have two inadequate control actions relating to the enforcement of these constraints: A&AC-ICA10 and A&AC-ICA11.

A&AC-ICA9. The HGA boom rotation joints do not rotate along the appropriate degrees of freedom at the required times. (→S/C-SC2), (↓A&AC-2.2.1.4, A&AC-2.2.1.8, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17)

> A&AC-CF9.1. The lock controller does not command the locks to disengage at the appropriate times. (↓SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)
>
> A&AC-CF9.2. Power is not provided to disengage the locks. (↓SV-43, SV-44, SV-45, SV-46, SV-47, SV-48)
>
> A&AC-CF9.3. The locks do not receive or act on a command to disengage. (↓SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)
>
> A&AC-CF9.4. Power is not provided to the motor on the degree of freedom. (↓SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)
>
> A&AC-CF9.5. Torque is not transferred from the motor to the joint due to slippage. (↓SV-25, SV-26, SV-27, SV-28, SV-29, SV-30)
>
> A&AC-CF9.6. The joint jams along the degree of freedom.

A&AC-ICA10. The HGA Boom Rotation Joints rotate too little, too slowly, or too much along the HGA Boom Rotation Joint degrees of freedom when the locks are disengaged. (→A&AC-SC3, A&AC-SC7), (↓A&AC-2.2.1.5, A&AC-2.2.1.8, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

> A&AC-CF10.1. The process model of the motor controller incorrectly accounts for spacecraft velocity changes.
>
> A&AC-CF10.2. Spacecraft velocity changes create inertial loads exceeding the torque capacity of the motor. (↓SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)
>
> A&AC-CF10.3. The process model of the motor controller does not account for time delay in motor actuation. (↓SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)

A&AC-CF10.4. The process model of the motor controller does not account for joint friction, slippage, partial disengagement of the lock, or other physical effects. (↓SV-31, SV-32, SV-33, SV-34, SV-35, SV-36, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

A&AC-CF10.5. The process model of the motor controller does not account for changes in joint friction, slippage, rotation joint angle measurement errors, or other physical effects. (↓SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)

A&AC-CF10.6. The motor controller receives a control input (or goal) that would violate minimum separation between the HGA boom, HGA, or HGA radiation and the rest of the spacecraft.

A&AC-CF10.7. Power is not provided to the HGA Boom Rotation Joint Motors.

Rationale: If no power is provided to a joint motor while the locks are disengaged, the only resistance to rotational disturbances along the affected degree of freedom will be the rotational inertia of the joint and all HGA Boom Assembly mass downstream of it. Thus, if the disturbance is large enough, oscillation can occur about the desired pointing vector or, worse yet, minimum separation between the HGA, HGA boom, or HGA radiation and other parts of the spacecraft could be violated.

A&AC-CF10.8. The motor controller does not receive up-to-date feedback on the HGA Boom Rotation Joint Angles.

A&AC-ICA11. The locks on the degrees of freedom in the joints of the HGA boom disengage (i.e., allow rotation) at the wrong time. (→A&AC-SC1, A&AC-SC3), (↓A&AC-2.2.1.8, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

A&AC-CF11.1. The lock controller commands the locks to disengage while the HGA is in the payload fairing. (↓SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

A&AC-CF11.2. The joint(s) receive a mechanical disturbance greater than the designed capacity of the lock. (↓SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

A&AC-CF11.3. The locks receive and act upon the command to disengage with an unaccounted-for delay. (↓SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

These inadequate control actions and control flaws can be mitigated through enforcement of the following safety-related constraints:

A&AC-SC8. A command must be sent to disengage the HGA Boom Joint Rotation Locks at the desired HGA Boom deployment time (i.e., after separation of the launch vehicle payload fairing) or any time in which rotation of a locked degree of freedom is

desired. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.3, A&AC-2.4, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42), (→AC&DH-G1, HA&T-G3)

Note: This safety constraint is related to A&AC-CF9.1 and A&AC-CF11.1.

A&AC-SC9. Power must be provided to all HGA Boom Joint Rotation Locks at the desired times of lock disengagement. (←H2), (↓A&AC-2.3, A&AC-2.7, SV-43, SV-44, SV-45, SV-46, SV-47, SV-48), (→AC&DH-G1)

Note: This safety constraint is related to A&AC-CF9.2.

A&AC-SC10. The HGA Boom Joint Rotation Locks must receive and respond to a disengagement command within TBD milliseconds. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.3, A&AC-2.4, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42), (→AC&DH-G1, HA&T-G3)

Note: This safety constraint is related to A&AC-CF9.3 and A&AC-CF11.3.

A&AC-SC11. All rotation joints must not jam along a rotational degree of freedom. (←H2), (↓SV-8, SV-9, SV-12, SV-13, SV-16, SV-17)

Note: This safety constraint is related to A&AC-CF9.6.

A&AC-SC12. The power supply to the HGA Boom Rotation Joint Motors must not be interrupted for greater than a TBD second interval unless the HGA Boom Rotation Joint Locks engage within TBD seconds. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.3, A&AC-2.4, A&AC-2.7, SV-31, SV-32, SV-33, SV-34, SV-35, SV-36), (→AC&DH-G1, HA&T-G3)

Note: This safety constraint is related to A&AC-CF9.4 and A&AC-CF10.7
Rationale: If an HGA Boom Rotation Joint Motor loses power and the lock on the corresponding degree of freedom does not engage, the only resistance to mechanical disturbances will be the rotational inertia of the joint and the HGA/HGA Boom mass downstream of it.

A&AC-SC13. The HGA Boom Rotation Joint Motors must not slip more than TBD radians/revolution with respect to the joints. (←H2), (↓SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-31, SV-32, SV-33, SV-34, SV-35, SV-36)

Note: This safety constraint is related to A&AC-CF9.5.

A&AC-SC14. The process model of the controller of the HGA Boom Rotation Joint Motors must explicitly or implicitly account for time delays in the motor actuation, joint friction, slippage, partial disengagement of the joint rotation locks, inertial loads from spacecraft velocity changes, other physical effects on joint rotation, and changes thereof.

(←H1, H2, H4, H5, H6, H7), (↓A&AC-2.3, A&AC-2.4, A&AC-2.2.1.12, SV-31, SV-32, SV-33, SV-34, SV-35, SV-36, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42), (→AC&DH-G1, HA&T-G2, HA&T-G3)

Note: This safety constraint is related to A&AC-CF10.1, A&AC-CF10.3, A&AC-CF10.4, and A&AC-CF10.5.
Rationale: Note that even a PID control law implicitly accounts for the effects mentioned in the constraint by altering the control effort in response to proportion, changes, and the summation of pointing error over time.

A&AC-SC15. The spacecraft velocity must not change by more than TBD m/s^2 along an axis perpendicular to the axis of the deployed boom and TBD m/s^2 along an axis parallel to the axis of the deployed boom unless all rotation can be locked along all HGA Boom rotational degrees of freedom. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.3, A&AC-2.4, A&AC-2.5, A&AC2.6, SV-1, SV-2, SV-31, SV-32, SV-33, SV-34, SV-35, SV-36, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42), (→AC&DH-G1, HA&T-G3)

Note: This safety constraint is related to A&AC-CF10.2.
Rationale: If spacecraft accelerations exceed these values, the inertial loads created at the HGA Boom joints will overpower the HGA Boom Rotation Joint Motors as they try to null them. The ensuing rotation could potentially cause a violation of minimum separation between the HGA, HGA Boom, or HGA radiation and other parts of the spacecraft.

A&AC-SC16. The HGA Boom Rotation Joint motor controller must not receive a control input (goal) that would violate minimum separation between the HGA boom, HGA, or HGA radiation and the rest of the spacecraft. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.1.2, A&AC-2.3, A&AC-2.4), (→AC&DH-G1, HA&T-G1)

Note: This safety constraint is related to A&AC-CF10.6.

A&AC-SC17. The HGA Boom Rotation Joint Locks must be able to counteract all torques on the rotation joints when they are engaged. (←H1, H2, H4, H5, H6, H7), (↓A&AC-2.2.1.10, SV-37, SV-38, SV-39, SV-40, SV-41, SV-42)

Note: This safety constraint is related to A&AC-CF11.2.

A&AC-SC18. The HGA Boom Angle Encoders must provide HGA Boom Rotation Joint angles to the HGA Boom Rotation Joint Motors every TBD seconds. (←H1, H2, H4, H5, H6, H7), (→AC&DH-G1, HA&T-G1)

Note: This safety constraint is related to A&AC-CF10.8.

A&AC-SC19. The HGA Boom Rotation Joint Motor controllers must account for HGA Boom Rotation Joint Angle Encoder measurement errors. (←H1, H2, H4, H5, H6, H7),

(→AC&DH-G1, HA&T-G1), (↓A&AC-2.2.1.11, AC&DH-2.1.2.3, AC&DH-2.1.2.4, AC&DH-2.1.2.5)

Note: This safety constraint is related to A&AC-CF10.5.

In analyzing the above constraints, it appears that some progress would be made in the enforcement of A&AC-SC1, A&AC-SC3, and A&AC-SC7 by choosing this design option. The presence of the HGA Boom Joint Rotation Locks constrains the behavior of the system and could reduce the significance of A&AC-ICA10 and A&AC-ICA11. The tradeoff that comes with constraining the system behavior in this way is an increased relevance of A&AC-ICA9, however, it should be noted that the potential impacts of this inadequate control action are less severe than those of A&AC-ICA10 and A&AC-ICA11 (data will not be returned, but at least there will not be a collision between the HGA or HGA Boom and other parts of the spacecraft that would generate orbital debris).

Design Option 5

Option 5 in Table 3 would lead to the following design principles (note that some design principles associated with Option 1 appear here as well):

A&AC-2.2.1.1. The shoulder and elbow rotation joints of the boom have one rotational degree of freedom (pitch) while the wrist joint has two rotational degrees of freedom: roll and pitch. (→A&AC-2.2.1.3, A&AC-2.2.1.6, A&AC-2.2.1.7)

Rationale: Though roll has no direct effect on the translation of material downstream of the rotation joint or the HGA's beam direction, it can be coupled with pitch or yaw to create a hemispheric range of motion for beam pointing or material translation.

A&AC-2.2.1.2. The HGA boom segments are TBD meters long cylindrical shells, each TBD centimeters thick. (↑A&AC-A1, A&AC-C1),

A&AC-2.2.1.3. Translation of the HGA with respect to the main spacecraft structure is controlled through rotation of HGA boom segments. (←A&AC-2.2.1.1)

A&AC-2.2.1.4. Each HGA boom rotation joint degree of freedom is restrained while the HGA is in the payload fairing of the launch vehicle by TBD mechanical locks that are permanently disengaged during deployment. Electrical power is required to disengage the locks, but no electrical power is required to maintain engagement of the locks. (↑A&AC-SC1, A&AC-SC2)

A&AC-2.2.1.5. Each HGA boom rotation joint degree of freedom is measured every TBD seconds by an angle encoder. (↑A&AC-C3, A&AC-C4, A&AC-SC3, A&AC-SC6)

A&AC-2.2.1.6. The maximum range of pitch rotation at each joint is TBD radians in the forward and reverse directions with the zero radian defined by the angle in which the boom segment (or antenna center) downstream of the joint is parallel to the boom segment upstream of the joint. (←A&AC-2.2.1.1)

A&AC-2.2.1.7. The maximum range of roll rotation in the wrist joint is TBD Radians in the forward and reverse directions. (←A&AC-2.2.1.1)

A&AC-2.2.1.8. Pitch rotation in the shoulder and elbow joints is initially created and then resisted by a set of damped torsion springs that are held in a loaded state by the mechanical locks on the pitch degree of freedom until HGA Boom deployment. (←A&AC-2.2.1.1, A&AC-2.2.1.4), (↑A&AC-SC1, A&AC-SC3, A&AC-SC7)

A&AC-2.2.1.9. Rotation in the pitch and roll rotational degrees of freedom in the wrist joint is created and resisted, as needed, by an electric motor for each degree of freedom. (←A&AC 2.2.1.1), (↑A&AC-SC1, A&AC-SC3, A&AC-SC7)

A&AC-2.2.1.10. To the extent that it is prudent, the HGA Boom will be mounted on a part of the main spacecraft structure that reduces the overlap in its range of articulation and signal radiation with the range of articulation of other spacecraft appendages. (↑A&AC-SC3)

With these design principles defined, we can elaborate on spacecraft-level safety constraints in addition to evaluating how well this design option enforces A&AC-SC1, A&AC-SC3, and A&AC-SC7. As was the case in Design Option 1, we now have an inadequate control action relating to the inability of the spacecraft to return data: A&AC-ICA9. Furthermore, the design option does not eliminate the possibility of not enforcing A&AC-SC1, A&AC-SC3, and A&AC-SC7. Thus, we now have two inadequate control actions relating to the enforcement of these constraints: A&AC-ICA10 and A&AC-ICA11.

A&AC-ICA9. The HGA boom rotation joints do not rotate along the appropriate degrees of freedom at the required times. (→S/C-SC2), (↓A&AC-2.2.1.4, A&AC-2.2.1.8, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17)

A&AC-CF9.1. The lock controller does not command the locks to disengage.

A&AC-CF9.2. Power is not provided to disengage the locks.

A&AC-CF9.3. The locks do not receive or act on a command to disengage.

A&AC-CF9.4. The torsion spring jams upon disengagement of the lock on the rotational degree of freedom.

A&AC-CF9.5. Power is not provided to the motor on the degree of freedom.

A&AC-CF9.6. Torque is not transferred from the motor to the joint due to slippage.

A&AC-CF9.7. The joint jams along the degree of freedom.

A&AC-ICA10. The HGA Boom Rotation Joints rotate too little, too slowly, or too much along the HGA Boom Rotation Joint degrees of freedom when the locks are disengaged. (→A&AC-SC3, A&AC-SC7), (↓A&AC-2.2.1.5, A&AC-2.2.1.8, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-37, SV-38, SV-39)

A&AC-CF10.1. The process model of the motor controller incorrectly accounts for spacecraft velocity changes.

A&AC-CF10.2. Spacecraft velocity changes create inertial loads exceeding the torque capacity of the motor.

A&AC-CF10.3. The process model of the motor controller does not account for time delay in motor actuation.

A&AC-CF10.4. The process model of the motor controller does not account for joint friction, slippage, partial disengagement of the lock, or other physical effects.

A&AC-CF10.5. The process model of the motor controller does not account for changes in joint friction, slippage, partial disengagement of the lock, rotation joint angle measurement errors, or other physical effects.

A&AC-CF10.6. The torsion springs are excited by a mechanical disturbance

A&AC-CF10.7. The motor controller receives a control input (or goal) that would violate minimum separation between the HGA boom, HGA, or HGA radiation and the rest of the spacecraft.

A&AC-CF10.8. Power is not provided to the HGA Boom Rotation Joint Motors.

Rationale: If no power is provided to a joint motor after the locks have been disengaged, the only resistance to rotational disturbances along the affected degree of freedom will be the rotational inertia of joint and all HGA Boom Assembly mass downstream of it. Thus, if the disturbance is large enough, oscillation can occur about the desired pointing vector or, worse yet, minimum separation between the HGA, HGA boom, or HGA radiation and other parts of the spacecraft could be violated.

A&AC-CF10.9. The motor controller does not receive up-to-date feedback on the HGA Boom Rotation Joint Angles.

A&AC-ICA11. The locks on the pitch degree of freedom in the shoulder and elbow joints of the HGA boom disengage (i.e., allow rotation) at the wrong time. (→A&AC-SC1, A&AC-SC3), (↓A&AC-2.2.1.8, SV-8, SV-9, SV-12, SV-13, SV-16, SV-17, SV-37, SV-38, SV-39)

A&AC-CF11.1. The controller of the locks commands the locks to disengage while the HGA is in the payload fairing.

A&AC-CF11.2. The joint(s) receive a mechanical disturbance greater than designed capacity of the lock.

A&AC-CF11.3. The lock controller commands one lock to disengage significantly before the other.

Rationale: The HGA could rotate into the main spacecraft if only one of the elbow and shoulder joints rotates in the pitch degree of freedom at a time.

A&AC-CF11.4. The locks receive and act upon the command to disengage with an unaccounted-for delay.

A&AC-CF11.5. Power required for disengaging the locks is provided to one lock before the other.

These inadequate control actions and control flaws can be mitigated through enforcement of the following safety-related constraints:

A&AC-SC8. A command must be sent to disengage the HGA Boom Joint Rotation Locks at the desired HGA Boom deployment time (i.e., after separation of the launch vehicle payload fairing) or later. Furthermore, this command must be sent to all of the locks in the shoulder and elbow joints within a TBD millisecond interval.

> Note: This safety constraint is related to A&AC-CF9.1, A&AC-CF11.1, and A&AC-CF11.3.

A&AC-SC9. Power must be provided to all HGA Boom Joint Rotation Locks at the desired time of lock disengagement. Furthermore, power must be provided to all the locks in the shoulder and elbow joints within a TBD millisecond interval.

> Note: This safety constraint is related to A&AC-CF9.2 and A&AC-CF11.5.

A&AC-SC10. The HGA Boom Joint Rotation Locks must receive and respond to a disengagement command within TBD milliseconds.

> Note: This safety constraint is related to A&AC-CF9.3 and A&AC-CF11.4.

A&AC-SC11. All rotation joints must not jam along a rotational degree of freedom.

> Note: This safety constraint is related to A&AC-CF9.4 and A&AC-CF9.7.

A&AC-SC12. The power supply to the HGA Boom Rotation Joint Motors must not be interrupted for greater than a TBD second interval after the HGA Boom Rotation Joint Locks have been disengaged.

> Note: This safety constraint is related to A&AC-CF9.5 and A&AC-CF10.8

A&AC-SC13. The HGA Boom Rotation Joint Motors must not slip more than TBD radians/revolution with respect to the joints.

> Note: This safety constraint is related to A&AC-CF9.6.

A&AC-SC14. The process model of the controller of the HGA Boom Rotation Joint Motors must explicitly or implicitly account for time delays in the motor actuation, joint friction, slippage, partial disengagement of the joint rotation locks, inertial loads from spacecraft velocity changes, other physical effects on joint rotation, and changes thereof.

> Note: This safety constraint is related to A&AC-CF10.1, A&AC-CF10.3, A&AC-CF10.4, and A&AC-CF10.5.

Rationale: Note that even a PID control law implicitly accounts for the effects mentioned in the constraint by altering the control effort in response to proportion, changes, and the summation of pointing error over time.

A&AC-SC15. The spacecraft velocity must not change by more than TBD m/s^2 along an axis perpendicular to the axis of the deployed boom and TBD m/s^2 along an axis parallel to the axis of the deployed boom.

Note: This safety constraint is related to A&AC-CF10.2.
Rationale: If spacecraft accelerations exceed these values, the inertial loads created at the HGA Boom joints will overpower the HGA Boom Rotation Joint Motors as they try to null them. The ensuing rotation could potentially cause a violation of minimum separation between the HGA, HGA Boom, or HGA radiation and other parts of the spacecraft.

A&AC-SC16. The torsion springs in the pitch degrees of freedom in the elbow and shoulder joints of the HGA Boom must not be excited to amplitudes of TBD degrees and TBD degrees, respectively, by mechanical disturbances encountered during the mission.

Note: This safety constraint is related to A&AC-CF10.6.

A&AC-SC17. The HGA Boom Rotation Joint motor controller must not receive a control input (goal) that would violate minimum separation between the HGA boom, HGA, or HGA radiation and the rest of the spacecraft.

Note: This safety constraint is related to A&AC-CF10.7.

A&AC-SC18. The HGA Boom Rotation Joint Locks must be able to counteract all torques on the rotation joints when they are engaged.

Note: This safety constraint is related to A&AC-CF11.2.

A&AC-SC19. The HGA Boom Angle Encoders must provide HGA Boom Rotation Joint angles to the HGA Boom Rotation Joint Motors every TBD seconds.

Note: This safety constraint is related to A&AC-CF10.9.

A&AC-SC20. The HGA Boom Rotation Joint Motor controllers must account for HGA Boom Rotation Joint Angle Encoder measurement errors.

Note: This safety constraint is related to A&AC-CF10.5.

In analyzing the above constraints, it once again appears that some progress would be made in choosing this design option. The presence of the HGA Boom Joint Rotation Locks constrains the behavior of the system before HGA Boom deployment and thus reduces the significance of A&AC-ICA10 and A&AC-ICA11 during that time.

However, the significance of A&AC-ICA10 and A&AC-ICA11 are higher than they would be for Design Option 1 because of the timing requirements for disengaging the locks on the shoulder and elbow joints and the absence of locks to restrain the wrist degrees of freedom in the event that the motors along those degrees of freedom cannot null out mechanical disturbances.

4.1 Discussion

As can be seen in the analysis above, the two design options produce similar inadequate control actions and control flaws. However, the differences in these inadequate control actions and control flaws have important implications in the enforcement of the safety constraints generated from them. For example, preventing an interruption in power to a joint motor for some interval between HGA Boom deployment and the end of the mission (i.e., A&AC-SC12 of Design Option 5) can be a much more difficult problem than engaging a joint rotation lock in the event of a such a power interruption (A&AC-SC12 of Design Option 1). Additionally, the use of springs in the shoulder and elbow pitch degrees of freedom in Design Option 5 introduces a timing constraint on the lock disengagement of these two degrees of freedom (i.e., if one is released and the other is significantly late in its release, the HGA and/or boom might contact another part of the spacecraft). Accordingly, the design options affect which inadequate control actions will be of most relevance throughout the mission. Because Design Option 1, more than Design Option 5, leads to increased relevance of an inadequate control action that leads only to data loss and decreased relevance of inadequate control actions leading to data loss, mission failure, and orbital debris generation, we chose Design Option 1 for further elaboration in the Outer Planets Explorer Intent Specification.

5 Traceability Analysis of OPE Intent Specification

Traceability between systems engineering artifacts is becoming increasingly important in the design of spacecraft. As stated in the NASA Software Safety Standard[7]:

> *"Because many software safety requirements are derived from hazard analysis, these requirements will also be linked to specific hazard reports…Tracing requirements is a vital part of system verification and validation, and especially in safety verifications. Full requirements test coverage is virtually impossible without some form of requirements traceability. Tracing also provides a way to understand the impact on the system of changing requirements or modification of software elements."*

Given the importance of traceability, it worth noting how traceability is captured in the products generated from the methodology used in this study. Figure 13 below shows traceability between all Level 0 through Level 2 artifacts of the OPE Intent Specification. A matrix representation[8] of the traceability structure is provided in Figure 14. In these figures, a link between "Customer Programmatic Constraints" and "Component/Functional Element Constraints," for example, indicates that at least one Component/Functional Element is hyperlinked to at least one Customer Programmatic Constraint in the OPE Intent Specification. These links, as mentioned in the Intent Specification background section in Part 1 of this report, represent "means-ends" relationships between linked items. These types of relationships are important to consider in the derivation and modification of specification items. As can be seen in the figure, the methodology in this study led to traceability (and the documentation thereof) of Design Decisions to High-Level Hazards and High-Level Hazard Causal Factors, among other things, through High-Level and Component/Functional Element Safety Constraints. Note the closed loop between Component/Functional Element Safety Constraints, Design Decisions, Inadequate Control Actions, Control Flaws, and High-Level Hazard Causal Factors; this loop represents the concurrent hazard analysis and design work occurring in step 9.5 of the methodology. Moreover, traceability was also captured between design decisions and many other traditional systems engineering artifacts, as well as those that were previously unique to STAMP and STPA, Intent Specification, or State Analysis.

[7] National Aeronautics and Space Administration (2004), *NASA Software Safety Standard*, NASA-STD-8719.13B, July 2004 Revision.

[8] While the matrix representation contains the same information as the graphical representation, it is more suited for mathematical analysis of the traceability structure (e.g., the comparison of traceability structures would be a simple matrix addition or subtraction operation). Therefore, it is provided for the reader's convenience.

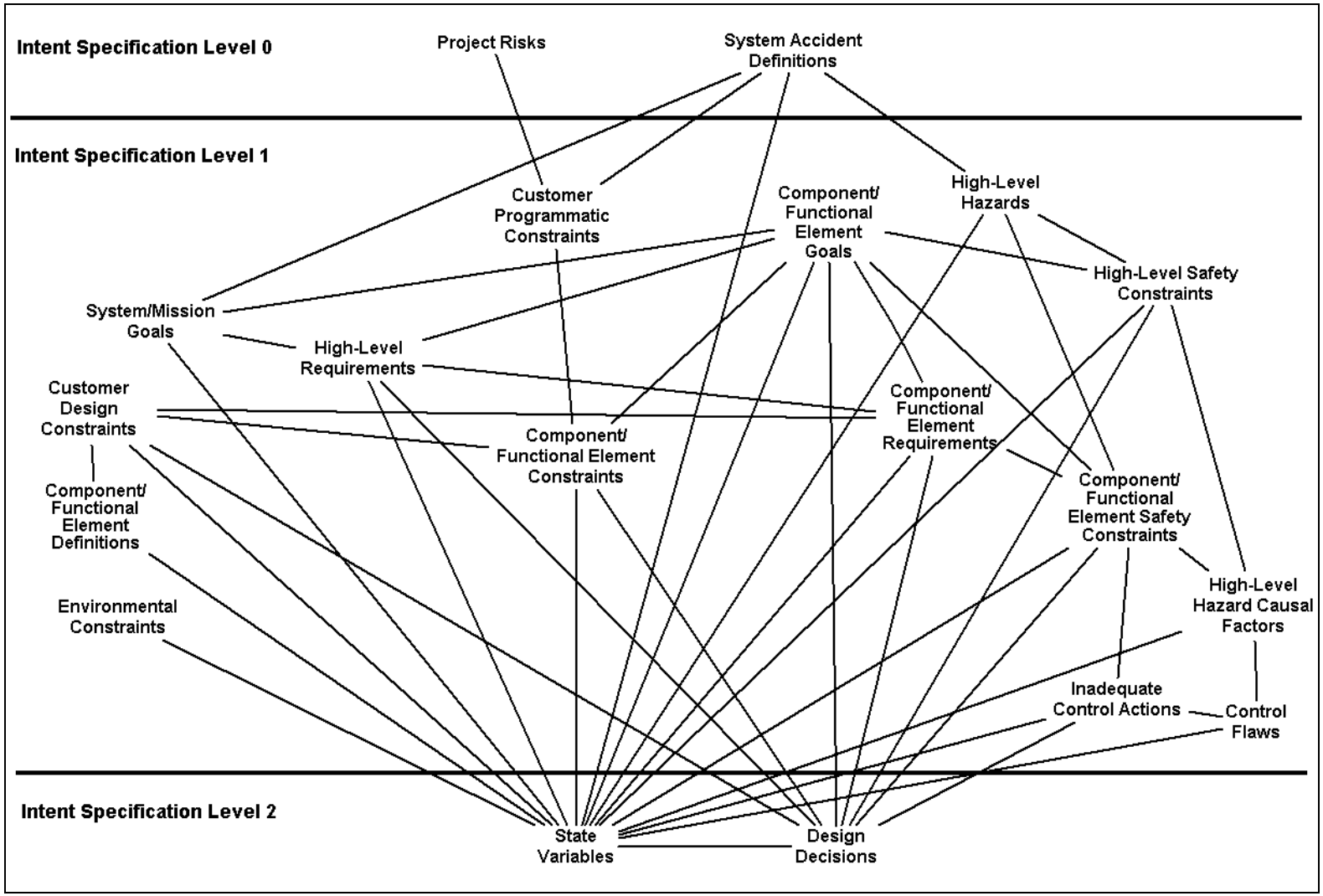


Figure 13. Traceability Structure of the OPE Intent Specification (Graphical Representation).

Name		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
System/Mission Goals	1	1					1	1											1	1
Environmental Constraints	2		2																	1
Customer Design Constraints	3			3							1	1	1	1						1
Customer Programmatic Constraints	4				4	1		1				1								
Project Risks	5				1	5														
High-Level Requirements	6	1					6						1	1					1	1
System Accident Definitions	7	1			1			7	1											1
High-Level Hazards	8							1	8	1								1		1
High-Level Safety Constraints	9								1	9				1			1		1	1
Component/Functional Element Definitions	10			1							10									1
Component/Functional Element Constraints	11			1	1							11		1					1	1
Component/Functional Element Requirements	12			1			1						12	1				1	1	1
Design Decisions	13			1			1			1		1	1	13	1			1	1	1
Inadequate Control Actions	14													1	14			1		1
Control Flaws	15														1	15	1			1
High-Level Hazard Causal Factors	16									1						1	16	1		1
Component/Functional Element Safety Constraint	17								1				1	1	1		1	17	1	1
Component/Functional Element Goals	18	1					1			1		1	1	1				1	18	1
State Variables	19	1	1	1			1	1	1	1	1	1	1	1	1	1	1	1	1	19

Figure 14. The Traceability Structure of the OPE Intent Specification (Matrix Representation).

6 Functional Analysis of OPE

As mentioned in the intent specification, the components, functional elements, and control structure of this system have been defined through three separate decomposition iterations. In the first iteration, the five major system elements (i.e., spacecraft, launch vehicle, Deep Space Network, Ground Network, and Mission Operations Center) were identified from mission constraints and assumptions about the technology available for the mission. These five elements place interfacing constraints on each other and because most of them are already in existence (i.e., launch vehicle, Deep Space Network, Ground Network), it was possible to immediately identify a number of detailed functions that must be performed by the elements developed specifically for this mission (i.e., spacecraft). These identified functions and the requirements, constraints, and/or design decisions that they originated from are shown in Table 4. In the second iteration of system decomposition, the energy, information, and material interactions necessary for the identified functions for the spacecraft were encoded in a Design Structure Matrix (DSM) and clustered through manual manipulation of the matrix rows and columns. This DSM is provided below in Figure 15. This clustering of the functional interactions aided the assignment of the functions to functional elements so that energy, information, and material interactions across the elements would be minimized (i.e., to decouple the functional elements). This process was repeated in the third iteration of system decomposition after a new set of required functions for spacecraft attitude and articulation control were identified. The required functions for spacecraft attitude and articulation control are provided in Table 5 along with the design decisions, constraints, and/or requirements from which they originated. The DSM for the third iteration can be found in Figure 16.

Function:	Associated Design Decisions, Constraints, and/or Requirements
Spacecraft MOC Directive Execution	S/C-C4
Spacecraft MOC Directive Storage	S/C-C4
Spacecraft H&S Data Evaluation	S/C-C4
Spacecraft H&S Data Collection	S/C-C4
Spacecraft H&S Data Storage	S/C-C3
Spacecraft H&S Data Retrieval from Storage	S/C-C3
Spacecraft Data Packetization	S/C-R3 and S/C-R5
Spacecraft Power Generation	S/C-R7
Spacecraft Power Distribution	S/C-R7
Spacecraft Translation	S/C-R1
Spacecraft Pointing	S/C-R1
Spacecraft Antenna Deployment	S/C-C2, S/C-R3 and S/C-R5
Spacecraft Antenna Pointing	S/C-R3 and S/C-R5
Spacecraft Science Data Collection	S/C-R2
Spacecraft Science Data Storage	S/C-C3
Spacecraft Science Data Retrieval from Storage	S/C-C3
Spacecraft Science Data Packetization	S/C-R3 and S/C-R5
Spacecraft Data Modulation	S/C-R3 and S/C-R5
Spacecraft MOC Directive Demodulation	S/C-C4, S/C-R4, and S/C-R6
RF Transmission/Reception of Data	S/C-R3 and S/C-R5

Table 4. The initial spacecraft functions identified and the design decisions, constraints, and/or requirements from which they originated.

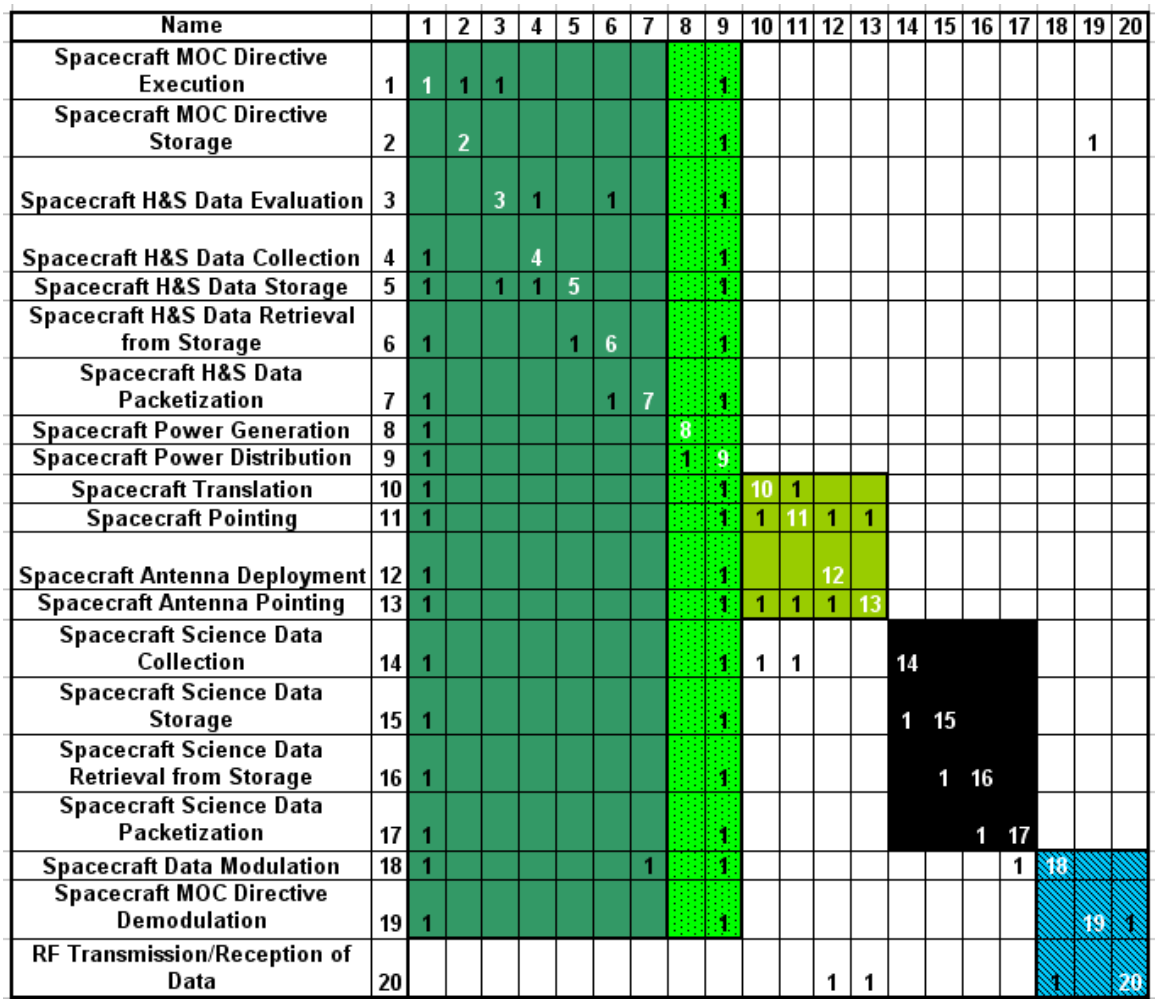


Figure 15. Clustered Design Structure Matrix for the Spacecraft-Level Functional Decomposition.

Function:	Associated Design Decision(s), Constraint(s), or Requirement(s)
A&AC C&DH Directive Reception	A&AC-C2
A&AC C&DH Directive Storage	A&AC-C2
A&AC H&S Data Evaluation	A&AC-C2
HGA Pointing State Information Transfer to C&DH	A&AC-C3
HGA Translation State Information Transfer to C&DH	A&AC-C4
A&AC C&DH Directive Execution	A&AC-C2
A&AC H&S Data Collection	A&AC-C2
HGA Translation State Determination	A&AC-C4
HGA Pointing State Determination	A&AC-C3
A&AC Electrical Power Reception	A&AC-C5
A&AC Power Distribution	A&AC-C5
Spacecraft Velocity Changes	A&AC-R1, A&AC-R2, A&AC-R3, A&AC-R4, and A&AC-R5
Spacecraft Pointing	A&AC-R6
HGA Boom Joint i Roll Rotation	A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, and A&AC-2.2.1.1
HGA Boom Joint i Roll Data Collection	A&AC-C3 and A&AC-C4
HGA Boom Joint i Pitch Rotation	A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, and A&AC-2.2.1.1
HGA Boom Joint i Pitch Data Collection	A&AC-C3 and A&AC-C4
HGA Restraint	A&AC-SC1 and A&AC-SC2
HBA Boom Joint i+1 SC-Fixed X Translation	A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, and A&AC-2.2.1.3
HBA Boom Joint i+1 SC-Fixed Y Translation	A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, and A&AC-2.2.1.3
HBA Boom Joint i+1 SC-Fixed Z Translation	A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, and A&AC-2.2.1.3
HGA Deployment	A&AC-R7, A&AC-R8, A&AC-R9, A&AC-R10, and A&AC-2.2.1.3

Table 5. The identified A&AC functions and the design decisions, constraints, and/or requirements from which they originated.

Name		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
A&AC C&DH Directive Reception	1	1										1											
A&AC C&DH Directive Storage	2	1	2									1											
A&AC H&S Data Evaluation	3			3			1			1		1											
HGA Pointing State Information Transfer to C&DH	4				4				1			1											
HGA Translation State Information Transfer to C&DH	5					5		1				1											
A&AC H&S Data Collection	6						6			1		1											
HGA Translation State Determination	7							7		1		1				1		1					
HGA Pointing State Determination	8								8	1		1				1		1					
A&AC C&DH Directive Execution	9		1	1				1	1	9		1											
A&AC Electrical Power	10										10												
A&AC Power Distribution	11										1	11											
Spacecraft Velocity Changes	12									1		1	12	1									
Spacecraft Pointing	13									1		1	1	13	1		1						
HGA Boom Joint i Roll Rotation	14									1		1	1	1	14				1				
HGA Boom Joint i Roll Data Collection	15									1		1			1	15							
HGA Boom Joint i Pitch Rotation	16									1		1	1	1	1		16		1				
HGA Boom Joint i Pitch Data Collection	17									1		1					1	17					
HGA Restraint	18									1		1							18				
HBA Boom Joint i+1 SC-Fixed X Translation	19																1		1	19			
HBA Boom Joint i+1 SC-Fixed Y Translation	20																1		1		20		
HBA Boom Joint i+1 SC-Fixed Z Translation	21																1		1			21	
HGA Deployment	22																			1	1	1	22

Functional Elements:
A&AC C&DH
A&AC EP
Translation Controller
Attitude Controller
HGA Attitude and Translation Controller

Figure 16. Clustered Design Structure Matrix for the A&AC-Level Functional Decomposition.