

SAFETY-DRIVEN SYSTEM ENGINEERING PROCESS

by

MARGARET VIRGINIA STRINGFELLOW

S.B. Aeronautics and Astronautics, S.B. Electrical Engineering
Massachusetts Institute of Technology, 2004

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

MASTER OF SCIENCE IN
AERONAUTICS AND ASTRONAUTICS

at the

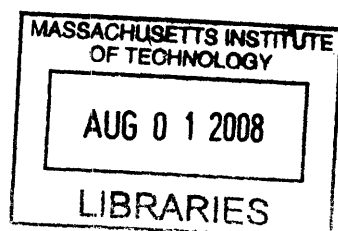
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
June, 2008

© Massachusetts Institute of Technology, 2008
All rights reserved.

Signature of Author: _____
Department of Aeronautics and Astronautics
May 9, 2008

Certified by _____
Professor Nancy G. Leveson
Department of Aeronautics and Astronautics
Thesis Supervisor

Accepted by: _____
Professor David L. Darmofal
Associate Department Head
Chair, Committee on Graduate Students



Safety-Driven System Engineering Process

by

Margaret Virginia Stringfellow

Submitted to the Department of Aeronautics and Astronautics
in partial fulfillment of the requirements for the
Degree of Master of Science.

Abstract

As the demand for high-performing complex systems has increased, the ability of engineers to meet that demand has not kept pace. The creators of the traditional system engineering processes did not anticipate modern complex systems, and the application of traditional processes to complex systems such as spacecraft has repeatedly led to disastrous results. Too often, system safety is considered late in the design process, after much of the design is set. This thesis presents an iterative safety-driven system engineering process to address this problem. The process integrates safety into the design process, ensuring that safety is designed *into* the system, rather than *added on*. The techniques used in this process are: 1) Intent Specifications, a framework for organizing system development and operational information in a hierarchical structure; 2) the System-Theoretic Accident Modeling and Processes (STAMP) model of accident causation, a framework upon which to base powerful safety engineering techniques; 3) STAMP-based Hazard Analysis (STPA) a novel hazard analysis technique; and 4) SpecTRM-Requirements Language (SpecTRM-RL), a formal modeling language. Intent Specification is used to document the design with complete traceability from system goals, requirements, and constraints to the operational design and software code. The STAMP framework is used to apply concepts from control theory to system engineering. STPA is used to identify hazards and eliminate them or mitigate their effects to ensure a safe system design. Finally, SpecTRM-RL is used to create the blackbox behavior models. An example of this process applied to an outer moon exploration mission is presented (in the form of an intent specification) and discussed. The specification focuses on the design of the control system and functionality of the scientific instruments, while also including a high-level design of the entire spacecraft. The application of the process described in this thesis demonstrates that design decisions are safety-driven, and that the results of the hazard analysis are integrated into all aspects of the design.

Thesis Supervisor: Professor Nancy G. Leveson
Professor of Aeronautics and Astronautics

Acknowledgements

This research was supported by JPL University Subcontract 1297013.

I would like to thank the many people that this research possible:

Professor Nancy Leveson: Whether she is in her office down the hall, across the country, or halfway around the globe, she has always made time for me. Her insights into both this research as well as the graduate student process model have been invaluable. From typical control flaws found in any graduate student to the complex control flaws unique to the multiple coordinated controllers in this system, she was able to help me mitigate and control them if not eliminate them altogether. I look forward to our next exciting projects together.

Dr. Nicolas Dulac and Brandon Owens: Thank you for helping untangle the web of definitions. Together we were able to rigorously say what we meant all along. (↓Thesis).

Dr. Michel Ingham and Dr. Katie Weiss: I am grateful to have had another opportunity to work with each of you and present our work to the rest of the JPL all-stars.

Sara and Leigh-leigh: I am lucky! To, have-- two such skilled; () and generous: Sisters.

Chalie: I am grateful for all of the fantastic desktop pictures. Whether as subject or as photographer, your presence in the art world is deeply felt.

Parents: Mommie and Papa, thank you for being the best parents ever.

Keith: LOML, thank you for the thesis paper.....and making my life fantastic and lovely. How will I write the next thesis without seeing you everyday? I love you for ∞ .

Lastly, I would like to thank my best friend, Edgar Raul Gonzalez. We have explored great mysteries together: from what is missing in Maxwell's equations to how many times a personality can dare lasso. Everytime I climbed on top of a narrow wooden beam you always climbed up with me. I miss your genius mind, your challenging nature, and your sparkling soul, and dedicate this thesis to you.

Table of Contents

Abstract.....	2
Acknowledgements.....	3
Table of Contents.....	4
List of Figures.....	5
1. Introduction.....	6
2. Background.....	6
2.1 Intent Specifications.....	6
2.1.1 Writing Intent Specifications.....	9
2.1.2 Visualization and the Design Process.....	11
2.2 STAMP.....	13
2.3 STPA.....	14
2.4 SpecTRM-RL.....	21
2.5 Literature Review.....	23
2.6 Summary.....	26
3. System Engineering Process.....	26
Step 1. Identify Mission Goals and Requirements.....	26
Step 2. Define System Accidents or Unacceptable Losses.....	27
Step 3. Define High-level Hazards.....	28
Step 4. Define High-level Safety-related Constraints.....	28
Step 5. Identify Environmental Constraints, Customer-derived Constraints and Programmatic Risks.....	29
Step 6. Perform High-level Functional Decomposition.....	32
Step 7. Design High-level System Control Structure.....	32
Step 8. Perform Preliminary Hazard Analysis.....	34
Step 9. Define Lower-level level 1 Specifications.....	40
Step 10. Define Lower-level Design.....	42
Step 11. Define and Design System Operational Behavior.....	44
Step 12. Develop Formal Models of the System.....	45
Iteratively Refine the System Design and Continue to Perform STPA.....	47
Step 13. Perform Validation Tests.....	49
Step 14. Generate Designs and Software Code.....	49
3.1 Partial Safety-driven System Engineering Process Map.....	49
3.2 Process Summary.....	52
4. Application of Process to a Outer Planet Moon Exploration Spacecraft.....	53
5. Discussion of Safety-driven System Engineering Process Application and Future Work ...	53
6. Conclusions.....	56
7. References.....	56
Appendix.....	60

List of Figures

Figure 1. Intent Specification Hierarchy.....	7
Figure 2. Partial Example of a Mars Lander Intent Specification	9
Figure 3. Spacecraft Pointing Dependencies	12
Figure 4. Control Structure	13
Figure 5. Generic System Control Structure.....	14
Figure 6. Generic STPA Low-level Process Control Loop	15
Figure 7. Inadequate Control Action Types.....	16
Figure 8. Inadequate Control Actions for the Mars Lander Example.....	16
Figure 9. Mars Lander Descent Process Control Loop.....	17
Figure 10. Control Flaw Taxonomy.....	17
Figure 11. Sources of Inadequate Control for the Mars Lander	18
Figure 12. Refinement of Safety Constraints and the Resultant Design Decisions.....	19
Figure 13. Control loop with Control Flaws Superimposed	20
Figure 14. Example <i>And/Or</i> Table from Camera State Transition Logic.....	22
Figure 15. SpecTRM-RL Camera Mode Control Process Model.....	23
Figure 16. Level 1 Mission Goals.....	27
Figure 17. High Level Requirement	27
Figure 18. System Accidents	28
Figure 19. High-level Hazards.....	28
Figure 20. High-level Hazards and Constraints.....	28
Figure 21. Example Environmental Assumptions	29
Figure 22. Jupiter Radiation Model	30
Figure 23. GIRE Output for Various Radiation Sources on Europa [31].....	30
Figure 24. Examples of Customer-Derived Design Constraints.....	31
Figure 25. Examples of Customer-Derived Programmatic Constraints	31
Figure 26. Example of a Programmatic Risk.....	31
Figure 27. Control Structure and Legend	34
Figure 28. Partial STPA Hazard Analysis	39
Figure 29. Partial Hazard Log Example	40
Figure 30. Level 1 Outer Planet Moon Mission Example	41
Figure 31. Level 1 Constraints Outer Planet Moon Explorer Mission Example.....	42
Figure 32. Level 2 Intent Specification.....	43
Figure 33. Outer Planet Moon Explorer Mission Example of System Operational Behavior.....	44
Figure 34. Example <i>And/Or</i> Table.....	45
Figure 35. Outer Planet Moon Explorer Mission Example of Science Functional Element Controller	46
Figure 36. System States Influencing SCI Data Collection.....	49
Figure 37. Partial Map of the Safety-driven System Engineering Process.....	51
Figure 38. Traceability Structure of the Intent Specification: Levels 0-3.	54
Figure 40. GIRE Output For Various Radiation Sources on Europa (Klark 2007).....	66

1. Introduction

This thesis presents a safety-driven system engineering process that addresses the need for safety-driven design in complex systems and applies the process to the design of a spacecraft. Current system engineering methods are not sufficient for the design of safe and successful software-controlled systems [30, 31]. Safety engineers typically perform hazard analyses as a separate part of the system engineering effort. After a system is designed, the hazard analysis is performed, and the results are used to add fault protection to the existing design. This approach does not ensure safety and is ineffective; even if hazards are identified, they are rarely eliminated with fault protection. Safety should be built into the system rather than adding it on after the system design is completed. Furthermore, when safety is designed and built into a system, it is more effective and less costly [5]. Traditional safety design and analysis techniques were developed for electro-mechanical systems and do not fit the underlying assumptions of software-controlled systems. To cope with the inherent complexity of software-based control systems and new technology, new types of hazard analysis and system engineering approaches to building safety-critical systems¹ are needed.

The safety-driven system engineering process presented in this thesis enables system engineers to design systems from a safety point-of-view. Hazard analysis is folded into the nominal design process, rather than conducted as a separate activity. This process combines four state-of-the-art techniques: 1) Intent Specifications, a framework for organizing system development and operational information in a hierarchical structure; 2) the System-Theoretic Accident Modeling and Processes (STAMP) model accident causation, a framework upon which to base powerful safety engineering techniques; 3) STAMP-based Hazard Analysis (STPA) a novel hazard analysis technique; and 4) SpecTRM-Requirements Language (SpecTRM-RL), a formal modeling language.

The intent specification of a spacecraft design is presented in the appendix and provides an example of the application of this process. The design is focused on the design of the control system and functionality of the scientific instruments, while still giving a high-level design of the entire spacecraft.

2. Background

2.1 Intent Specifications

An intent specification is a specification and development framework supporting system design and other system engineering activities, intended to provide more readable and reviewable specifications. The content of an intent specification is similar to that of a traditional specification but its structure and linking are unique. The structure and linking allows for

¹ The definition of safety used here includes loss of life or injury, equipment damage, mission failure, environmental damage, i.e., any unacceptable loss. With respect to the JPL spacecraft used as the example in this paper, The NASA General Safety Program Requirements (Document NPR 8715.3B) defines Safety Critical as “describing any condition, event, operation, process, equipment, or system that could cause or lead to severe injury, major damage, or mission failure if performed or built improperly, or allowed to remain uncorrected.”

complete and exhaustive requirements tracing, supports the recording of design rationale, and facilitates the assurance of system properties from the initial design phase to implementation. The seven-layer structure of an intent specification is shown below in Figure 1 [1].

	Environment	Operator	System and Components	V&V
Level 0	Project management plans, status information, safety plans, etc.			
Level 1: System Purpose	Assumptions Constraints	Responsibilities Requirements I/F Requirements	System Goals, High-Level Requirements, Design Constraints, Limitations	Hazard Analysis
Level 2: System Design	External Interfaces	Task Analyses Task Allocation Controls/displays	Logic Principles, Control Laws, Functional Decomposition and Allocation	Validation Plans and Results
Level 3: Blackbox Models	Environment Models	Operator Task and HCI Models	Blackbox Functional Models, Interface Specifications	Analysis Plans and Results
Level 4: Design Representation		HCI Design	Software and Hardware Design Specifications	Test Plans and Results
Level 5: Physical Representation		GUI and Physical Controls Designs	Software Code, Hardware Assembly Instructions	Test Plans and Results
Level 6: Operations	Audit Procedures	Operator Manuals Maintenance Training Materials	Error Reports, Change Requests, etc.	Performance Monitoring and Audits

Figure 1. Intent Specification Hierarchy

Levels in an intent specification do not represent refinement, as in other commonly used hierarchical specification frameworks. Instead, each level of an intent specification represents a completely different model of the same system and supports a different type of reasoning about it: each model or level presents a complete view of the system from a different perspective. The model at each level is described in terms of a different set of attributes or language. Refinement and decomposition occurs within each level of the specification. In addition to intra-level refinement, the levels are organized in a “Means-Ends” hierarchy. In such a hierarchy, the information at a level acts as the goals (the ends) with respect to the model at the next lower-level [1]. In other words, the next lower-level is where the means to the ends of the current level are implemented

A brief description of the purpose of each level is as follows:

Level 0: Management Level. This level gives a top-level view of the project, and provides a place for non-engineering requirements and constraints, such as budget and schedule constraints.

Level 1: System Purpose. This level represents the customer view and contains all of the customer’s system-level requirements and constraints. In this level, system goals, requirements, design constraints, hazards, environmental assumptions, and system limitations are recorded. Customers can verify that these requirements and constraints are met upon system validation.

Level 2: System Design. This level is the system engineering view and documents the basic system-level design decisions made to satisfy the requirements and constraints at level 1. Detailed design is recorded here so that engineers from individual disciplines have enough engineering context, given in the form of design rationale, state variable models, and design to implement safety constraints and to design components.

Level 3: Formal Blackbox Behavior Representation. This level is written in a formal modeling language and provides “unambiguous interface” between system engineering and component engineering. The blackbox models of the control system can be used in informal review, formal analysis, and simulation.

Levels 4 and 5: Design and Physical Representation. These levels provide the information necessary to reason about individual component design and implementation issues.

Level 6: Operational Representation. This level documents operational procedures, processes, problem reports, and other data.

Figure 2 shows an example of intent specification traceability between Levels 0, 1, and 2 through partial specification of a spacecraft capable of landing on a planet surface. Traceability is captured through hyperlinks denoted by arrows and the specification item tag (for example, ↓Hazard.1). Traceability links denote different relationships between specifications based on their direction. An up arrow (↑) denotes that the current specification item is involved in the implementation of the intent of a specification item at a higher-level in the “means-ends” hierarchy denoted by the tag after the arrow. A down arrow (↓) points to a specification item at a lower-level in the “means-ends” hierarchy that is involved in the implementation of the intent of the current specification item. Left and right arrows denote relationships between specification items at the same level in the “means-ends” hierarchy that affect the items’ relationships to items on other levels. The direction of the arrow for this type of relationship depends on the physical location of the specification item in the intent specification document. A left arrow (←) points to a specification item at the same level that appears earlier in the specification than the current specification item. Conversely, a right arrow (→) points to another specification item at the same level that appears later in the current specification document. Thus, in Figure 2, the hazard (H1 at level 1) will show an upwards link pointing to an accident (ACC1 at level 0). This relationship shows ‘why’ the hazard is of concern: it can lead to the accident ACC1 shown in level 0. The accident has a downward arrow pointing to H1 showing ‘how’ the accident could occur. Similarly, H1 points across the level to a safety constraint (SC1) derived from the hazard. The safety constraint has downward pointing links to level 2 where that safety constraint is enforced with system design decisions. Lastly, the relationship between the design decisions is captured through traces across level 2.

Level 0: Accidents

Accident.1 Spacecraft experiences uncontrolled descent into the surface of Mars and is consequently destroyed. (↓Hazard.1)

Level 1: Hazards and Safety Constraints

Hazard.1 Spacecraft comes in contact with surface with an impact greater than 100 N. (↑Accident.1), (→SafetyConstraint.1, SafetyConstraint.2)

SafetyConstraint.1 The spacecraft must control its terminal descent to the surface of Mars at a velocity less than 10 m/s. (←Hazard.1), (↓DesignDecision.1, DesignDecision.2, DesignDecision.3))

SafetyConstraint.2 The spacecraft must be protected from impact with the surface. (←Hazard.1), (↓DesignDecision.2)

Rationale: The spacecraft structure is susceptible to damage even at an impact velocity of <10m/s and therefore must have some type of impact protection.

Level 2: Design Decisions

Design Decision.1 Thrusters on the spacecraft will be used to provide reverse thrust and slow the spacecraft descent. (↑SafetyConstraint.1)

Design Decision.2 When the spacecraft is within TBD meters of the planet surface, pressured, gas-filled balloons will inflate around the spacecraft to protect the spacecraft structure during the impact of landing. (↑SafetyConstraint.1, SafetyConstraint.2)

Design Decision.3 A vertical velocity sensor will measure spacecraft velocity during descent and ensure that reverse thrust is not stopped prematurely. (↑SafetyConstraint.1)

Figure 2. Partial Example of a Mars Lander Intent Specification

The example in Figure 2 illustrates a key feature of the intent specification: embedded design rationale. Oftentimes the rationale for a design choice or requirement goes unrecorded. As the project evolves or time passes, the perhaps once-obvious rationale for a design decision is lost, and it is difficult to identify the parts of the design affected by that rationale. It is critical that rationale be made obvious and traced to the parts of the implementation they affect. The discovery of new environment parameter values could require changes in all the design affected by an assumption made using outdated values. Engineers must be able to easily find all the affected parts of the design to make the necessary changes.

2.1.1 Writing Intent Specifications

The capture of design rationale and the traceability of rationale from design to implementation are key to the assurance of safety. Design rationale is the record of an engineer's mental model of the system's environment, the system itself, or how the system should behave or be operated. These recorded mental models are used to inform the development of requirements, constraints or design. The rationale can be recorded as a textual description of assumptions, a set of mathematical equations, state charts, numerical simulations, or any other standard engineering representation. Ideally, the intent specification should include all of the relevant design rationale necessary to understand key design decisions or trades, or programmatic decisions or trades. In this way, engineers can reference one document that is both a model of the system as well as a

transparent and easily accessible record explaining the reasoning behind modeling choices. Since the intent specification is a model from the point of view of each stakeholder (manager, customer, system, and component engineer), the relevant rationale must be captured for decisions pertaining to each stakeholder.

Analysis of most complex systems is performed on a model or abstraction of the system, rather than the real system itself. It is important that the abstraction (in this case, the intent specification) be structured to be as amenable to analysis as possible. Embedding design rationale in the intent specification is imperative.

Safety-driven design relies on models to describe the environment of the system to be built, and the physical processes of the system itself. The environment models influence design choices and can be used as a form of system design rationale. While design rationale can often be captured in text, engineers are free to use other representational forms, such as describing a trajectory with mathematical equations, to capture design in a way that is most natural to them.

For example, system engineers exploring the trade-space of wheel size and wheel number for a Mars rover, rely on models that show how driving performance and power scale with wheel radius and wheel number. The driving performance demanded from the rover is calculated using customer requirements and an environment model containing the spatial distribution and the size distribution of rocks on the surface of Mars. These principal environment models should be recorded in the intent specification (perhaps expressed as a Matlab simulation), and can serve as the design rationale for wheel radius and wheel number design. Links are created from the environment models and descriptions to the design motivated by them.

In standard practice, if requirements pertaining to the rover wheels change, the wheels will need to be redesigned and engineers will use the embedded Mars rock model again. Similarly, if new Mars environmental data becomes available, the embedded rock model can be updated and the design trade performed again. Inclusion of the rock model into the intent specification allows engineers to utilize the complete traceability of intent specifications, and identify all dependent design created with the Mars rock model. If engineers discover that the affected design is too tightly coupled with other parts of the system, such that a low-priority requirements change or model update would require a cascade of changes to other parts of the system, engineers may choose to not to make changes. Either way, engineers can use the traceability in the intent specification to inform their decision to waive requirements, pursue design changes, or update environment models.

Another example: Component engineers may determine the length and radius of a scientific boom so that its stiffness is robust to oscillations of $A\sin(\omega t)$; the expected maximum disturbance amplitude and frequency. To justify the dimensions chosen, a link is recorded in the intent specification to the finite element analysis (FEA) model of the spacecraft used to determine the dimensions. If the hazard analysis results show the disturbance amplitude or frequency to be greater than expected, engineers can use the traceability in the intent specification to make design changes. For example, if the links in the intent specification show that the disturbance model, $A\sin(\omega t)$, was used in the FEA model used to generate the boom measurements,

engineers can rerun an appropriately updated FEA model to generate new boom dimensions robust to the disturbances found by the hazard analysis.

2.1.2 Visualization and the Design Process

Models of the physical relationships between state variables capture relationships that complement those highlighted in the control structure. The control structure illustrates the flow of control in the system design, but other illustrations showing the flow of data are useful as well. The process described in this thesis does not specify which graphical modeling technique to use, but presents a few different options.

Causal Loop Diagrams

Causal loop diagrams describe the dynamic behavior of a system. System state variables are identified and relationships between the state variables are shown with arrows. If an increase in one state variable leads to an increase in another, the link is positive and if a decrease in one state variable leads to a decrease in another, the link is negative. Combinations of these relationships can form reinforcing positive or negative loops, or balancing loops. These diagrams show dynamic cause and effect relationships within a system, or between the system and its environment [22].

Data Flow Diagrams

Data flow diagrams show how information is processed and passed between components of a system. Similar to a block diagram, data flow diagrams are created in a top-down fashion to show input and output data between system components. Each block is then decomposed to show how data is processed in that block. These diagrams may be labeled to describe the process [23].

State Analysis's State Effects Diagrams

Aspects of the Jet Propulsion Laboratory's State Analysis methodology have been used in applications of the safety-driven system engineering process described in this thesis. In particular, the state effects diagrams were used to depict the relationships between system state variables, and control system inputs and outputs [6], [24].

Design Structure Matrix

Design-Structure Matrices (DSMs) can be used to perform functional decomposition on a system, show data flow in a system, or show the communication structure of an organization. The structure of a DSM is amenable to standard techniques from linear algebra that can be used to eliminate coupling in the system [9].

State Diagrams

State diagrams are graphical representations of finite state machines. The representation is a directed graph showing possible states of a system state variable as nodes on the graph. The system state variable can only be in one state at a time and the labeled arrows between nodes describe how the state variable (or system) transitions between states [25].

The creation of graphical representations depicting system operations and interactions with the environment is part of the standard system engineering process [14]. Visualizations help manage the complexity in the engineering process and reduce cognitive load. A graphical representation of the system interacting with the environment is easier to analyze than a mental model [26]. The graphical model can provide cues for engineers to identify process inputs, outputs or the effects and sources of disturbances in a controlled process. Diagrams, therefore, can be useful in formal control system design and the translation of textual design to formal blackbox behavior models of the system. Engineers are free to use any visualization of the system design they choose, (including none at all) and use visualizations to whatever extent they find helpful. The diagrams need not be included in the final intent specification as all of the information in them is contained in the blackbox behavior models of the system in level 3.

The relationship between state effects diagrams and the control structure:

Any of the diagrams described above are complementary to the control structure and can aid in its design. Design of the control hierarchy is informed by the physical relationships between system components. If subsystems A and B have a physical dependency, there must be a controller C that manages their relationship. One superior controller managing the relationship between A and B is preferable to other controller arrangements, as it reduces coupling. When control is executed in a one-to-many fashion, coupling is reduced and coordination problems between controllers are avoided. For example, in a space system, science instrument pointing and Earth communication pointing are both physically dependent on spacecraft pointing. To ensure that the pointing goals of both the science functional element (camera pointing) and the communication functional element (line-of-sight antenna pointing) are met, there must be an attitude and articulation controller that manages the pointing of both subsystems. A diagram illustrating these pointing dependencies is shown in Figure 3. The control hierarchy created to manage the spacecraft, science and communication pointing relationships depicted in Figure 3 is shown in Figure 4.

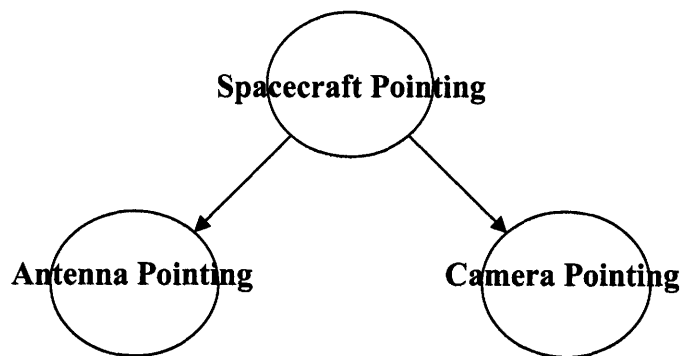


Figure 3. Spacecraft Pointing Dependencies

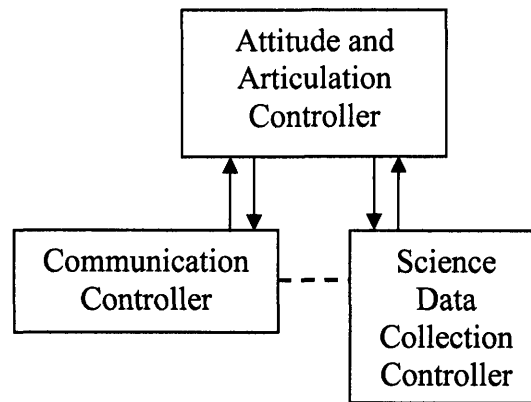


Figure 4. Control Structure

Diagrams depicting the physical relationships between functional elements or components are not necessary to create the control structure, but they can be helpful in forming the control hierarchy for systems with complex physical coupling. Graphical visualizations can aid in the design process, as well as the safety-driven system engineering process described in section 3.

2.2 STAMP

STAMP is an accident causality model in which accidents stem from inadequate control or inadequate enforcement of safety-related constraints on the design, development, and operation of the system [1], [2]. Instead of viewing accidents as the result of an initiating (root cause) event in a series of events leading to a loss, accidents are viewed as resulting from interactions among components that result in a violation of system safety constraints.

STAMP treats safety as a control problem; accidents occur when component interactions and disturbances are not controlled, or if components fail or feedback is corrupted or missing. If a system is adequately controlled, no unsafe states exist and no safety constraints are violated. In Figure 5 a generic example hierarchical control structure is shown. Each level in the structure imposes control on the level below it and receives feedback from it. Both system operations and system development are shown as they are both responsible for the enforcement of safe system behavior.

Any controller in the hierarchy must contain a model of the system being controlled. The model of the process may contain only a few state variables (such as can be found in a thermostat) or hundreds of state variables and transitions (such as that required for a spacecraft). For proper control the process model must contain: the current state (the current values of the system variables), the ways the process can change state (the system dynamics), and the target values and relationship between system state variables (the control laws). This process model is used by the controller (human or automated) to select control actions. The process model is updated through feedback from the process. Accidents result when the process model does not adequately match the controlled process [3].

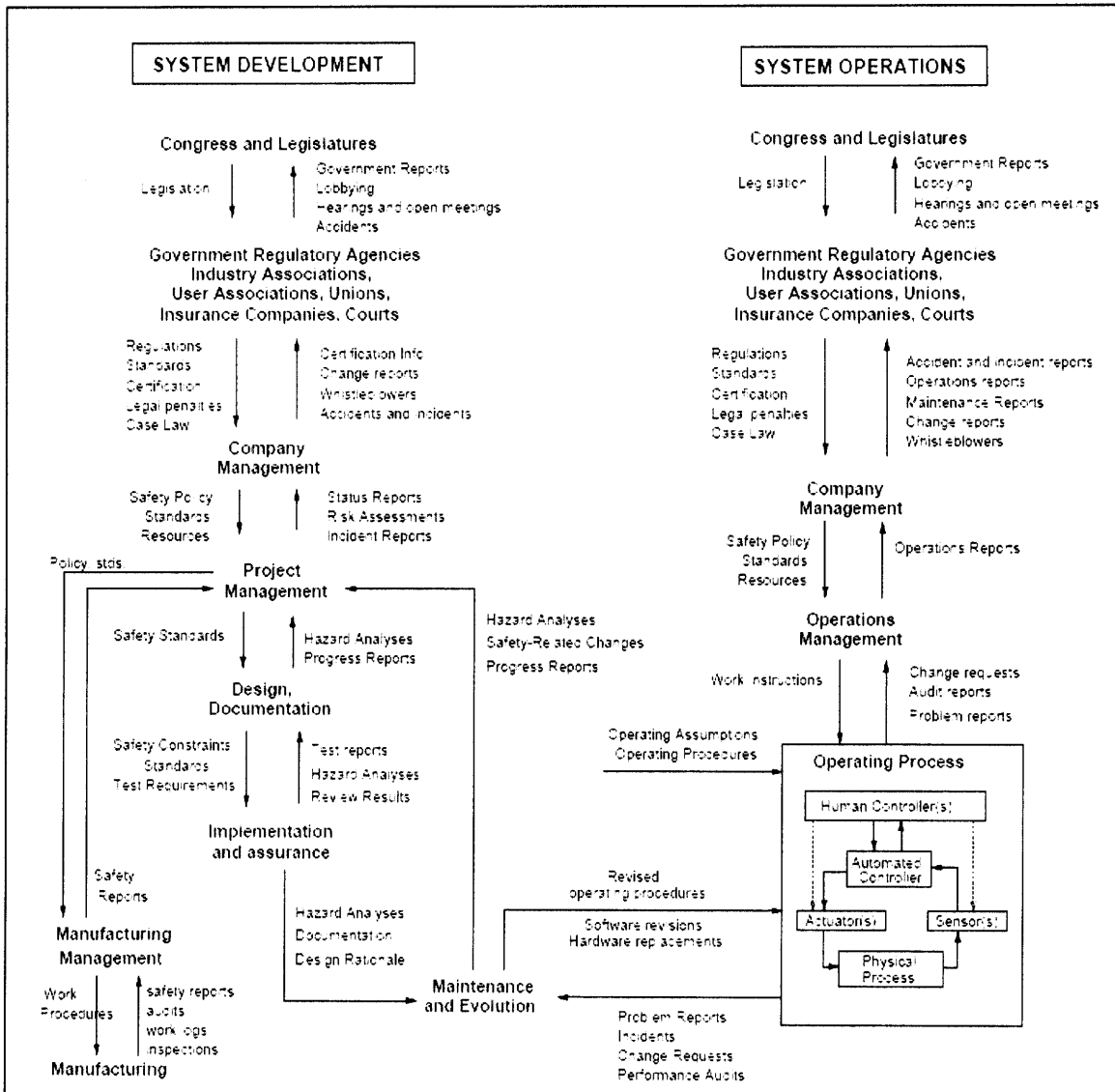


Figure 5. Generic System Control Structure

2.3 STPA

STPA is a hazard analysis technique based on the STAMP model of accident causation. The objectives, as described in [4], are to identify instances of inadequate control that could lead to the presence of hazards and the safety-related constraints necessary to ensure acceptable risk. Furthermore, performing STPA produces information about how the safety constraints may be violated and this information can be used to control, eliminate, and mitigate hazards in the system design and operation [5]. Although the first steps of STPA are similar to those performed in other hazard analysis techniques, the later steps either deviate from traditional practice or provide a rigorous framework for doing what is traditionally done in an ad hoc manner.

Underlying the STPA process is the notion that hazards are eliminated or controlled through system design. Figure 6 presents a generic, low-level process control loop in STPA. As seen in the figure, the control input is a reference signal. The controller uses the control input in conjunction with received measurements to generate operating commands. Continuing along the loop, the

command is sent to the actuator, which implements the command through the arrow labeled U . The U vector refers to actions of the actuator that influence the controlled process. The control algorithm used by the controller is based on an internal process model of the controlled process. The controlled process, or plant, is subject to process inputs and disturbances. The process output may become input into another linked process control loop. The sensors measure the output resulting from the actuator's actions and disturbances, and generate measurements that are then fed into the estimator.

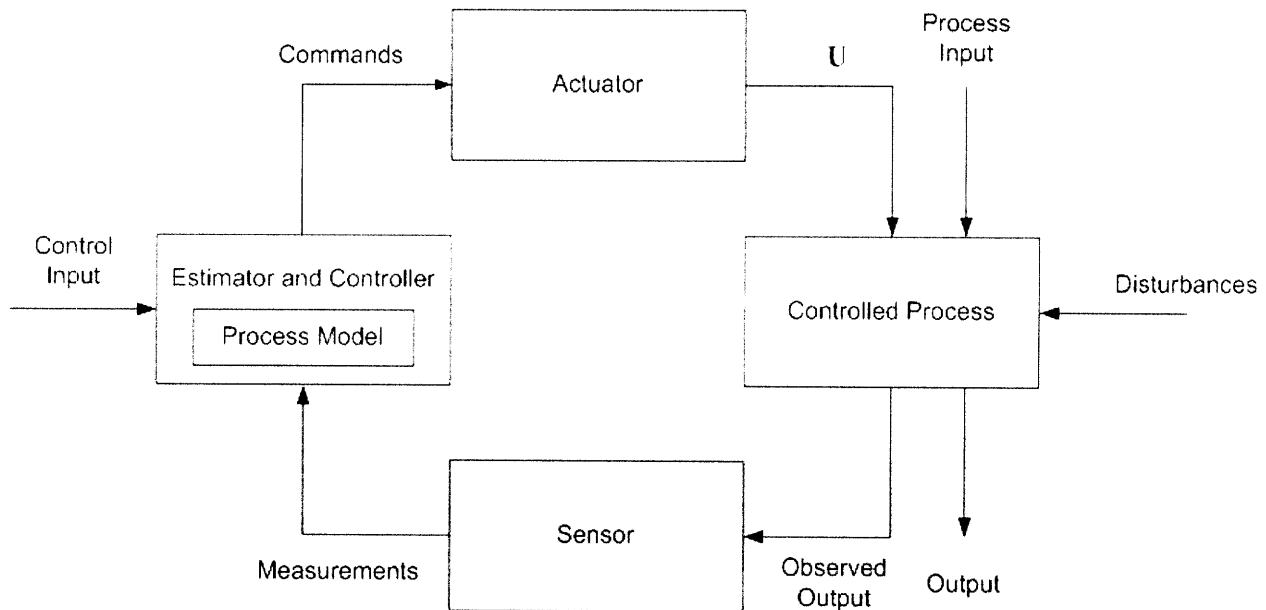


Figure 6. Generic STPA Low-level Process Control Loop

Depending on the particular system, the control input may be referred to as a goal, plan, sequence, directive or set point in spacecraft engineering parlance. The controller may send directives to a lower-level controller rather than an actuator in order to affect control on that process. Similarly, the lower-level control loop, rather than a sensor, may pass measurements or status information (such as its health and other components of its current state) to the higher-level control loop.

STAMP is based on the concept of controlling hazards rather than eliminating component failures (which are only one cause of hazards). When a safety constraint is violated, the hazard occurs and accidents can happen. For example, as illustrated in the Mars Lander example captured in Figure 2, if the physical process being controlled is the landing of a spacecraft, the relevant hazard is “Spacecraft comes in contact with surface with an impact greater than 100 N.” The spacecraft could be inadequately controlled, and the hazard state could occur, if the landing controller directs or commands the thrusters to land such that the spacecraft impact is 120 N, for example. A control flaw, such as an incorrectly calibrated velocity sensor, could contribute to inadequate control of the landing process. The concepts of inadequate control and control flaws are discussed below.

Each hazard and related safety constraint is analyzed using STPA. Starting with a hazard and a safety constraint to control the hazard, *inadequate control actions* that could violate the safety constraint are identified. An inadequate control action is an action or inaction by the controller that leads to the violation of a safety constraint. The four types of inadequate control are shown in Figure 7.

1. A required control action is not provided or is inadequately executed.
2. An incorrect or unsafe action is provided.
3. A potentially correct or adequate control action is provided too late or at the wrong time.
4. A correct control action is stopped too soon or continued too long.

Figure 7. Inadequate Control Action Types

Examples of each of the four types of inadequate control are shown for the Mars Lander example in Figure 8. The first step of an STPA hazard analysis is to list each combination of identified hazard and related safety constraint with the inadequate control actions that could lead to the violation of the safety constraint. The result of the first STPA step is shown in Figure 8 and is built from the partial intent specification of Figure 2.

SafetyConstraint.1: The spacecraft must control its terminal descent to the surface of Mars at a velocity less than 10 m/s.

- ICA.1 Spacecraft descent control is not engaged.
- ICA.2 Spacecraft descent control allows descent velocity in the range of 10 to 15 m/s.
- ICA.3 Spacecraft descent control is activated too late.
- ICA.4 Spacecraft descent control is de-activated too soon.

Figure 8. Inadequate Control Actions for the Mars Lander Example

Using knowledge of the current system design, the next step in the STPA process is the identification of *control flaws* and *inadequate control executions*. Control flaws are the mechanisms that could lead to inadequate control actions due to errors in the control algorithm, poor understanding of the process, or poor coordination between multiple controllers. Control flaws are identified through inspecting the process control loop to determine how the system can produce an inadequate control action. Figure 9 depicts the process control loop for the Controlled Process of “descent” for the Mars Lander example. For example, the inadequate control action “Spacecraft descent control is not engaged” may result if the control input “Initiate Descent” is not received by the Mars Lander Estimator and Controller. Figure 10 contains a taxonomy to assist in the process of inspecting the control loop and identifying control flaws such as these. Early in the STPA process when most control loops are high-level, examination of the control loops are especially useful, as the number of loops and complexity of their interactions is tractable.

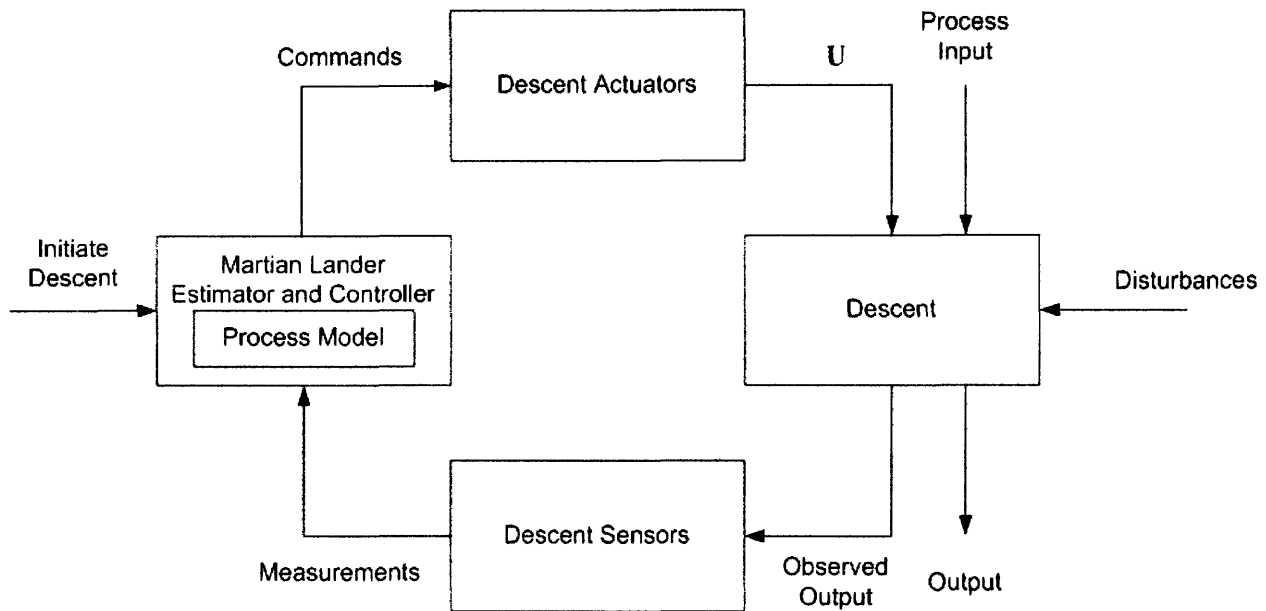


Figure 9. Mars Lander Descent Process Control Loop

1. Design of the control algorithm does not enforce constraints
 - Flaw(s) in creation process
 - Process changes without appropriate change in control algorithm (asynchronous evolution)
 - Incorrect modification or adaptation
2. Process models inconsistent, incomplete, or incorrect
 - Flaw(s) in creation process
 - Flaw(s) in updating process
 - Inadequate or missing feedback
 - Not provided in system design
 - Communication flaw
 - Time lag
 - Inadequate sensor operation
 - Time lags and measurement inaccuracies not accounted for
 - Expected process inputs are wrong or missing
 - Expected control inputs are wrong or missing
 - Disturbance model is wrong
 - Amplitude, frequency or period is out of range
 - Unidentified disturbance
3. Inadequate coordination among controllers and decision makers

Figure 10. Control Flow Taxonomy

In addition to control flaws, the inadequate control executions listed below can also lead to inadequate control:

1. Communication flaw
2. Inadequate actuator operation
3. Time lag

Inadequate control occurs through transmission of control (communication line failure) or failure of the mechanisms that actuate control (such as a motor failure) or time lags (such as the sluggish response of the motor; perhaps an indicator that the motor is soon to fail). In other words, inadequate control execution can occur when the process model is correct, and the correct control action is selected, but the control action is not successfully applied due to inadequate actuator or sensor operation, time lag, or a communication flaw. For example, as seen in Figure 9, if the descent sensors fail, the proper measurements will not be received by the Mars Lander Estimator and Controller, which may lead to the spacecraft not limiting the descent velocity to below 10 m/s.

As previously stated, the process control loops, control flaw taxonomy, and identification of inadequate control executions are all used to guide the hazard analysis process and identify sources of inadequate control. The Mars Lander example is continued in Figure 11, which contains the sources of inadequate control for SafetyConstraint.1.

<p>SafetyConstraint.1: The spacecraft must control its descent to the surface of Mars at a velocity less than 10 m/s.</p> <ul style="list-style-type: none">ICA.1 Spacecraft descent control is not engaged.<ul style="list-style-type: none">CF.1.1 The spacecraft controller does not receive an initiate descent control input.CF.1.2 The spacecraft controller does not command the descent actuators to activate.CF.1.3 The descent actuators do not receive a command to activate.ICE.1.1 The descent actuators do not activate.ICA.2 Spacecraft descent control allows descent velocity only in the range of 10 to 15 m/s.<ul style="list-style-type: none">CF.2.1 The descent controller receives incorrect feedback from a velocity sensor.ICA.3 Spacecraft descent control is activated too late.ICA.4 Spacecraft descent control is de-activated too soon.

Figure 11. Sources of Inadequate Control for the Mars Lander

Once the sources of inadequate control have been identified, the associated hazard is mitigated through elimination, control, or damage reduction. The mitigation of hazards is accomplished through one of the following strategies:

1. Create a new safety constraint, modify the related safety constraint, or refine the related safety constraint to better enforce control.
2. Create new design or modify existing design to eliminate, prevent or mitigate the effect of the control flaw or inadequate control execution.
3. Accept the design as is and record the rationale for doing so.

Figure 12 illustrates the refinement of two safety constraints and the design decisions made to enforce them.

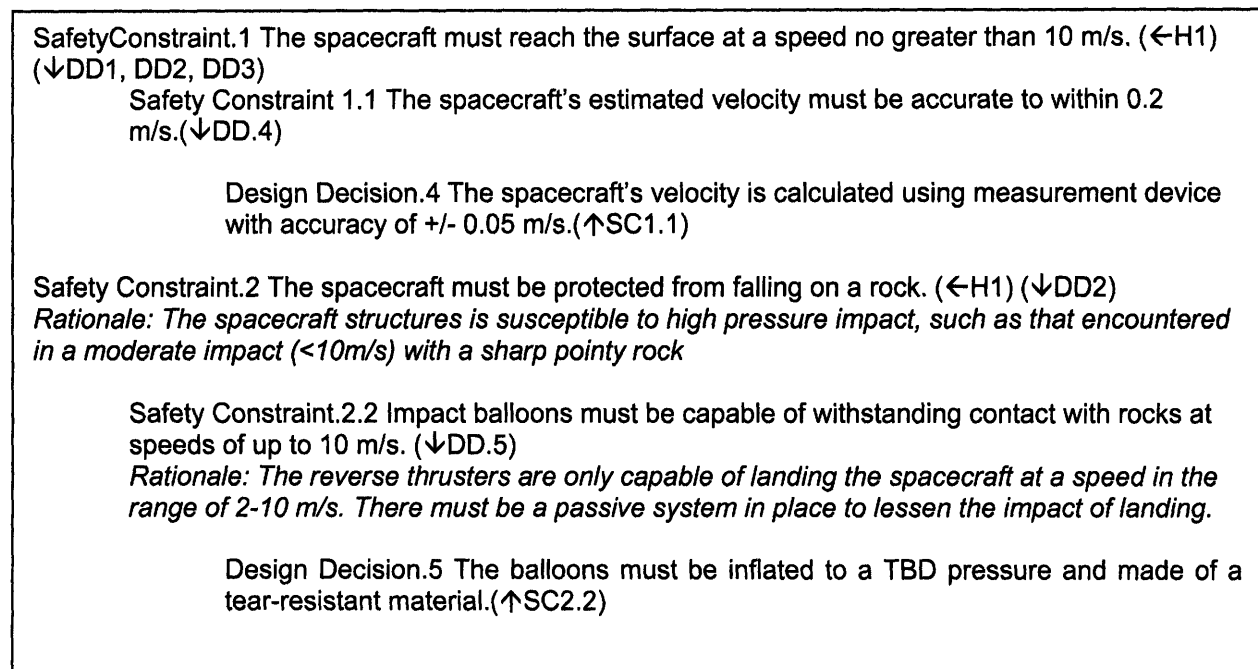


Figure 12. Refinement of Safety Constraints and the Resultant Design Decisions

SC 1.1 is a refinement of SC1, and was created to prevent ICA.1 and ICA.4 by trying to eliminate CF 1.1 and CF 4.1. In this case, one new safety constraint (and a new design decision to enforce the new safety constraint) helps to eliminate two inadequate control actions. The outer planet mission examples described in section 3.Step 8 show how the creation and refinement of safety constraints are recorded in the hazard log of the intent specification.

STPA should be performed iteratively and opportunistically. Engineers can either drill down into a particular hazard they wish to control or apply STPA more broadly across several hazards. In the early stages of intent specification creation, few design decisions have been made and control flaws and inadequate control executions may not yet be identified. However, performing STPA early will allow the results of the hazard analysis to inform the design process.

In essence, STPA starts with a hazard and its related requirements or constraints. The STPA taxonomy is used to identify inadequate control actions and the control flaws and/or inadequate control executions that lead to inadequate control actions. From there, engineers create new constraints or refine the existing constraints and create new design or modify the existing design until all hazards are mitigated, eliminated, or controlled. Engineering judgment is used to determine when the design is “safe and complete enough.”

The results of STPA (hazard analysis) are documented in the hazard log in level 1 of the intent specification.

Mapping STPA to the Control Structure and Control Loops to Create New Design

STPA is more than just a hazard analysis; it is a technique that fully integrates hazard analysis and design. Each item in the control flaw and inadequate control execution taxonomy relates to a component of the control loop, and examination of the process control loop(s) (as shown in Figure 6) leads to the discovery and identification of control flaws and inadequate executions.

The control structure is an especially useful visual aid to performing STPA. Inadequate control actions can be listed for each point of control and/or feedback between hierarchical control elements. The control structure is also helpful for identifying instances of the Inadequate Coordination Control Flow. Inadequate Coordination flaws can occur when one component is controlled by more than one controller. Control flaws and inadequate control executions can be elicited from more detailed control loops, which is especially useful early in the STPA process when most control loops are high-level and the complexity of their interactions is tractable.

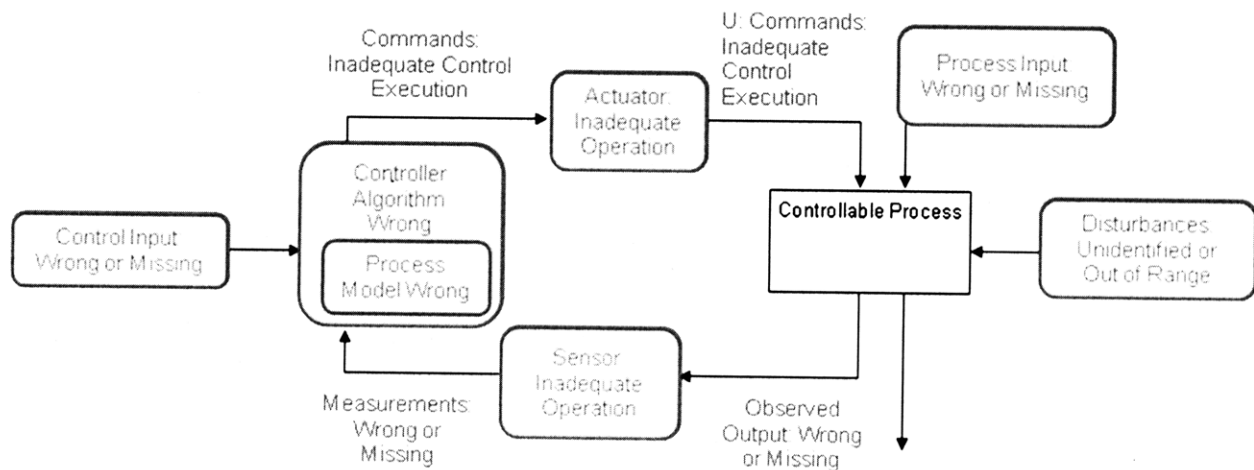


Figure 13. Control loop with Control Flaws Superimposed

Finding Control Flaws

The examples of using the control loops and the Control Flaw taxonomy to find control flaws in design presented above are by no means complete. The STPA taxonomy is a useful guide in the discovery of control flaws and provides a rigorous basis for categorizing control flaws; however, the discovery of control flaws always relies on domain knowledge. Only the proper application of domain knowledge to a design can ferret out how instances of inadequate control can arise. System engineers should collaborate with other experts in order to analyze subsystem design for control flaws.

STPA can be applied to any complex system, from socio-technical systems such as business industries, organizations, Boston's Big Dig, and spaceflight operations to low-level embedded software systems found in spacecraft systems. For each system, and design level of abstraction, domain knowledge will be essential for the discovery of control flaws. Discovery of control flaws also requires that engineers are able to determine, for their system, what constitutes an actuator, controller, disturbance, control input or process input. The application and translation

of control theory terminology for socio-technical systems is not trivial, as these systems have not traditionally been considered in a control theory context.

For example, the high-level design of an insurance company providing malpractice insurance, control inputs could be regulations, laws, or dynamic financial incentives and internal company policies can be interpreted to be the controller algorithm. With this in mind, control flaws that lead to inadequate control can be identified in flawed policies and process outputs can be monitored by higher-level controllers (such as the government or regulatory agencies) with regulations and financial incentives.

In another example, an ideal academic research lab, the controller could be the lab director and the controlled process may be research. In this case, the lab's funding may be considered a control input, rather than a process input because the amount and source of the funding affects the type of research performed. The students performing the research can be considered a process input, as they are a required input for the research to be conducted, but they do not have control over the research conducted. This situation is analogous to an imaging process in a camera. Power does not directly influence the target of the image (it's not a control input), but if there is no power provided to the imaging process, there will be no image (it is a process input). In either system, the absence of the crucial process input is a control flaw that leads inadequate control.

2.4 SpecTRM-RL

To model the system blackbox behavior described in level three of the intent specification, I used the formal modeling language of a commercial system engineering toolset, SpecTRM Requirements Language (SpecTRM-RL). SpecTRM-RL is an easily readable language that does not require extensive expertise in discrete mathematics, yet the models are executable, analyzable, and tools have been developed to check for completeness, consistency, and robustness.

SpecTRM-RL models use a tabular representation of disjunctive normal form (DNF) called *and/or* tables. Figure 14 shows an example of operational mode control logic for a camera expressed as an *and/or* table; it defines the criteria for the transition of a spacecraft camera state into an *Idle* mode. The far-left column of the *and/or* table lists the logical phrases of a predicate logic statement. Each of the other columns is a conjunction of those phrases and contains the logical values of the expressions. The rows of the table represent *and* relationships while the columns represent *or* relationships. The state variable takes the specified value (in this case, *Idle*) if any of the columns evaluate to true. If one of the columns evaluates to *true*, then the entire table evaluates to *true*. A column evaluates to true if all the rows have the value specified for that row in the column. An asterisk denotes "don't care" while 'T' and 'F' denote true and false, respectively. Underlined variables represent hyperlinks. For example, clicking on Camera-State would show how the 'Camera-State' state variable is defined in the intent specification.

= Idle			
Previous Value of <u>Camera-State</u> in state Off	*	F	F
<u>Turn-On-Camera-Command</u> was Received	T	*	*
Previous Value of <u>Power-Bus-State</u> in state Powered	T	T	T
Time Since <u>Camera-State</u> Last Entered Ready \geq 10 seconds	F	T	F
Previous Value of <u>Camera-State</u> in state Ready	F	T	T
<u>Go-Idle-Camera-Command</u> was Received	*	F	T

Figure 14. Example *And/Or* Table from Camera State Transition Logic

In the example described in Figure 14 the camera is only able to transition into *Idle* mode if: 1) the Camera was previously *Off*, the ‘Turn-On-Camera-Command’ was received, and the power bus is delivering power to the camera; or 2) the camera has been in *Ready* mode for at least 10 seconds and the power bus is delivering power to the camera; or 3) the camera has been in *Ready* mode for less than 10 seconds, the ‘Go-Idle-Camera-Command’ was received, and the power bus is delivering power to the camera.

The *and/or* tables used in the blackbox models describe the conditions for transitioning between states and the values of inputs and outputs. Visualizations for black box models are also used in SpecTRM as shown Figure 15. Process model visualizations show all of the inputs, outputs, control modes, inferred state variables, and other controllers or devices necessary for control of the camera. Each state variable, input, and output has a model described in part by an *and/or* table in level 3 of the intent specification. Level 3 formally defines the control system behavior and includes the transitions between values of an inferred state variable and control modes. It also includes timing constraints, descriptions, state variable macros, and functions for the value calculation of continuous state variables.

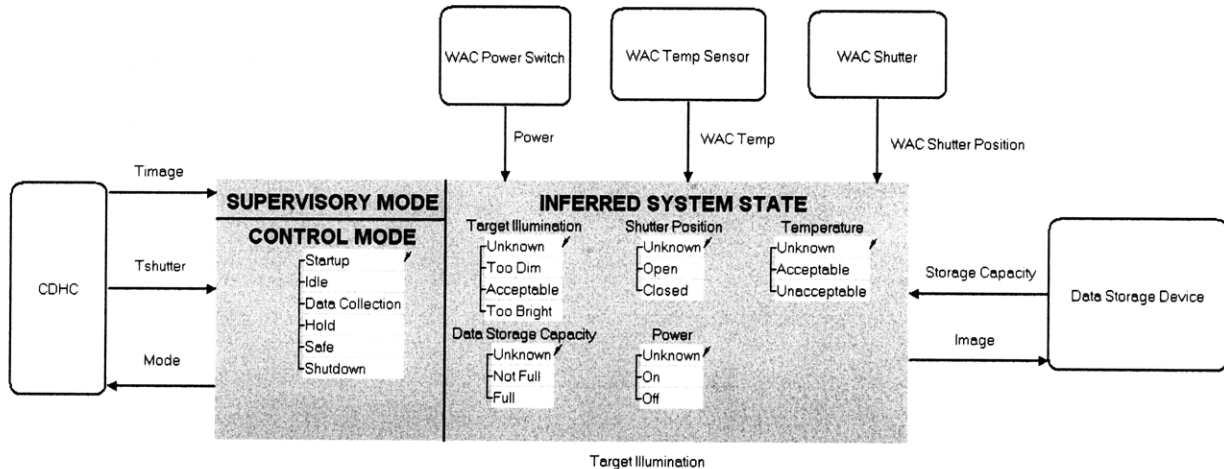


Figure 15. SpecTRM-RL Camera Mode Control Process Model

2.5 Literature Review

Intent specifications, STAMP, STPA and SpecTRM-RL, are all appropriate for the safety-driven system engineering process because each technique possesses the required support for the implementation of the process. A literature survey of other possible techniques was conducted and superior substitutes were not found. Intent specifications, STAMP, STPA and SpecTRM-RL were each created to address a need in safety engineering that was not otherwise met by current techniques and methods to prevent system accidents.

Major system accidents have been attributed to requirements and specifications problems [12]. Problems occur because requirements are often inconsistent themselves and incomplete [5]. Furthermore, requirements are difficult to write, implement or understand because relevant design rationale was either not included in the document, or isolated in a requirements sources and rationale table. The process of writing requirements is further confounded when writers cannot identify how their area of responsibility or subsystem relates to the system as a whole. From a stakeholder perspective, traditional requirements do not offer relevant views of the system for each stakeholder. The requirements engineering community has called for both automatic specification generation and the presentation of system specifications in multiple views for different audiences [13]. A better way of writing requirements and specifications was needed and experts recommended a change to traditional specification construction with the addition of embedded rationale, traceability, and the ability to view the specification from the perspective of significant stakeholders [5], [11].

As the result of customer requirement elicitation, traditional requirements and specification generation processes generate several unlinked and separate products: requirements, specifications, operating procedures, and verification and validation plans [14]. Intent specifications are structured to contain all the typical system engineering products, but include them in a way that simplifies writing the specification and makes the system design more comprehensible.

Intent specifications were created as an alternative method of writing, structuring and documenting requirements and specifications. In traditional system engineering, positively stated 'shall statements' were used to describe system needs. Negatively formed requirements, such as constraints, were not permitted in government contracts and so the positive 'shall form' became the standard [5]. This method of writing requirements is often not the most natural form for specifications, and safety engineering in particular is more often concerned with unsafe actions (what the system should not do) than with achieving system goals (what the system should do.) Intent specifications encourage constraint-based requirements to specify system behavior and control hazards [1].

There have been other techniques that encourage constraint-based requirements, including Constraint based approach to Requirements and Safety Analysis (CoRSA). This approach supports the writing of system requirements as constraints so that the requirements can be formally analyzed as a constraint satisfaction problem (CSP). Several techniques from artificial intelligence can be applied to CSPs to prove or assure certain system properties [15], [16]. Unfortunately, CoRSA, like other formal methods for writing requirements, is only tractable for smaller problems, and is not suitable for application to complex, software-controlled systems. Formal methods require mathematical training beyond most system engineers' and have not been successfully applied to large-scale software-controlled systems. For a more detailed discussion about the suitability of formal methods for complex systems see Leveson's System Safety Engineering: Back to the Future [4] and Wedde's "Are formal methods useful for software development?" [30].

Formal models are advantageous. They unambiguously define a system and allow the construction of proofs of system properties as well as prove the specification is complete [20]. Rather than writing the entire specification formally, intent specifications are structured to include a formal model of the system blackbox behavior. SpecTRM, a toolset developed to support the creation of intent specifications, includes support for formal model building. SpecTRM uses a formal mathematical language, SpecTRM-RL, to build the models. Any number of formal modeling methods could have been used to describe the system blackbox behavior; however, SpecTRM-RL was developed to be intuitive for system engineers. Formal modeling methods usually require intense mathematical training, and become too cumbersome for modeling complex systems. SpecTRM-RL, however, can be mastered in minutes and used to review complex systems successfully [17], [18].

One alternative to SpecTRM-RL is executable UML (xUML). xUML models of the system are built at various levels of abstraction and can be simulated, verified and validated, using UML toolsets. xUML models are intended to model the design of the system rather than form the blackbox requirements. In addition, xUML requires more training than SpecTRM-RL to construct models and toolsets that jointly support xUML modeling and intent specifications do not exist [20].

To address the last weaknesses of traditional requirements engineering, intent specifications provides complete traceability, verification and validation support, and multiple stakeholder views of the specification. Others have also developed techniques to address these weaknesses as well. They encourage the use of a requirements repository with computer aided software

engineering (CASE) tools to provide traceability between the requirements and design [13]. Others have constructed integrated development environments (IDEs) to support requirements elicitation, development, verification and validation support, and multiple system views [21]. These IDEs, however, are lacking. The various views provided are not relevant to stakeholder perspectives, but are the convenient result of various analysis tools. For example, a view is provided to see traceability between requirements, but there are not separate views that contain only the information pertinent to each project stakeholder, namely, managers, customers and developers. These alternatives often focus on verification and validation and do not adequately support the requirements and specification development process.

Intent specifications, in combination with SpecTRM-RL, however, is the first to have multiple stakeholder views, support requirements and design development, embed requirement and design rationale within the specification, have complete traceability, be formally analyzable and have automatic code generation capability.

STAMP is an accident causation model that treats safety as a control problem. Thus it provides the basis of writing the specification as a control system that prevents or mitigates hazards. Several other accident causation models exist, most popularly, the chain of events model of accidents. In this model, accidents occur by breaking through a series of barriers; the more barriers, the more likely the accident will not occur. The requirements built from this model focus on end-states (accidents) and preventing them, rather than hazards, or the state conditions that lead to them [4].

Probabilistic Risk Assessment (PRA), Hazard and Operability Analysis (HAZOP) and Fault Trees are hazard analysis techniques based on the chain of events model. These techniques are useful for non-software controlled electro-mechanical systems where failure rate data is available and redundancy can be added to reduce the probability of an accident. PRA, HAZOP and Fault Trees focus on events and event probabilities to calculate the probability of system failure. These techniques were created for conventional systems where the relationship between failures and hazards are clear. For example, the failure rate data for motors is widely available. In a software controlled system, however, the chain of events model cannot be applied: there is not a way to predict the failure of software, because software does not fail [4] [5]. Traditional hazard analysis techniques are even more inappropriate for complex, software-controlled systems for three reasons: 1) it is unlikely that the system structure is known well enough in advance to predict all the types of events that could lead to an accident; 2) they are applied after the fact rather than concurrently with design; and 3) the probabilities of the events are unknown [4] [15].

Rather than attempt to reduce the probability of undesirable events, it is more effective to control hazards and eliminate instances of inadequate control. STPA uses the STAMP model of accidents for the hazard analysis which allows engineers to find control flaws that lead to inadequate control. Once inadequate control actions and control flaws are identified, engineers can eliminate, mitigate, or control all hazards in the system.

The three methods chosen to create an integrated safety-driven system engineering process represent the best alternative in each class: specification writing style, documentation, and hazard

analysis technique. They address many of the problems in writing specifications and performing hazard analyses.

2.6 Summary

Each of the approaches discussed above are intended to produce safety-driven design. STAMP and STPA provide an innovative way to achieve safety-driven design, while intent specifications and SpecTRM-RL provide a unique way of capturing the system design specification allowing increased transparency and fewer errors of omission or loss of information. The use of models at levels 1 and 2 to explicitly state the physical assumptions that drive the design and allows for greater traceability and transparency in the intent specification. The inclusion of models in level two of the intent specification is natural for spacecraft engineers, and includes the engineering basis for design decisions in the specification. Together these approaches are used to define a safety-driven system engineering process.

3. System Engineering Process

The integration of STAMP and STPA with intent specifications has the potential for powerful synergy as a systems engineering method. As the basis for a safety-driven design method, it assists engineers in generating requirements aimed at hazard elimination and mitigation *concurrently* with generating functional requirements and spacecraft specification. Safety is designed into the spacecraft from the beginning of the design process rather than adding on fault protection after the fact.

The integrated design method presented here in the context of an example of a hypothetical NASA mission to explore the moon of an outer planet. The complete example is included in the appendix.

Step 1. Identify Mission Goals and Requirements

The starting point for the process is the definition of *mission goals* that we want or require the mission to achieve, and *requirements* that the mission must meet to achieve its mission goals

For this project, the science goals shown in the outer planet moon mission example were derived from Karla Clark's paper describing a proposed Europa orbiter mission [7]. The goals listed here are generalized below and shown in Figure 16. The example contains mission goals with links across level 1 pointing to high-level requirements. Figure 17 shows an example of a high-level requirement derived from the mission goals, corresponding to a high-level requirement called out in Clark's paper.

Characterize the presence of a subsurface ocean on an icy moon of an outer planet (Clark, 2007). (→[HLR2](#), [HLR4](#), [HLR5](#), [HLR6](#)), (↑[ACC4](#), [ACC5](#))

Characterize the three-dimensional configuration of the icy crust of the icy moon of an outer planet, including possible zones of liquid (Clark, 2007). (→[HLR1](#), [HLR2](#), [HLR3](#), [HLR4](#)), (↑[ACC4](#), [ACC5](#))

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

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

Figure 16. Level 1 Mission Goals

HLR3. The mission shall perform topographic mapping of a representative TBD percentage of the surface of the icy moon of the outer planet at better than 10-m/pixel scale and better than or equal to 1-m/vertical accuracy. (←[G2](#), [G4](#)), (→[S/C-G1](#))

Rationale: This level of horizontal and vertical accuracy is necessary create topographic maps of the icy moon that will be critical for future surface-landing missions.

Figure 17. High Level Requirement

Mission goals and requirements can be drawn from or inspired by a number of standard information sources such as: prior architecture studies, reused mission requirements, and governmental mandates.

Step 2. Define System Accidents or Unacceptable Losses

To derive the safety requirements and design constraints, the engineer first defines system accidents or unacceptable losses. These losses may include loss of life, mission, or damage to the environment. System accidents are documented in level 0 of the intent specification and have links that point to hazards in level 1 of the intent specification. Figure 18 contains accident definitions for the outer planet moon mission example with links pointing to hazards in level 1.

ACC1. Humans and/or human assets on earth are killed/damaged. (↓[H5](#))

ACC2. Humans and/or human assets off of the earth are killed/damaged. (↓[H6](#))

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](#))

Rationale: It's assumed that 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.

ACC4. The scientific data corresponding to the mission goals are not collected. (↑[G1](#), [G2](#), [G3](#), [G4](#), [G5](#), [G6](#), [G7](#)), (↓[H1](#))

Figure 18. System Accidents

Step 3. Define High-level Hazards

Next, the engineer defines the high-level hazards that could lead to system accidents or prevent mission goals and requirements from being met. Figure 19 lists examples of the high-level hazards that were derived using the outer planet moon mission goals in combination with standard system safety engineering principles and analysis of the accidents identified above. System-level hazards are documented in level 1 of the intent specification and point to accidents at level 0. Then, from these high-level hazards, the high-level safety constraints are defined (see Step 4).

- | |
|---|
| H1. Inability of Mission to collect data. (↑ ACC4) |
| H2. Inability of Mission to return collected data. (↑ ACC5) |
| H3. Inability of Mission scientific investigators to use returned data. (↑ ACC5) |

Figure 19. High-level Hazards

Step 4. Define High-level Safety-related Constraints

The safety constraints are requirements that eliminate or mitigate a hazard. The definition of safety constraints involves a simple but important translation from the hazard into an engineering goal. For example, if the hazard is “Subway train leaves the platform with the doors open,” the corresponding safety constraint could be “Subway train must not be capable of leaving with the train door open.” Recently, the Cassini mission experienced a setback when a critical piece of software was not operational during a Saturn moon flyby. During the data collection time, the spacecraft was switching its data collection software to an updated version that was intended to provide the necessary functionality [33]. In this case, the hazard could be “Spacecraft is not operating with the software it requires,” and the corresponding safety constraint could be “Spacecraft must always run the updated (correct) software.” High-level safety constraints are documented in level 1 of the intent specification with links pointing to high-level hazards. An example from the outer planet moon explorer mission is show below in Figure 20.

- | |
|--|
| H1. Inability of Mission to collect data. (↑ ACC4) |
| H2. Inability of Mission to return collected data. (↑ ACC5) |
| H3. Inability of Mission scientific investigators to use returned data. (↑ ACC5) |
| SC1. The mission must have the necessary functionality for data acquisition at the required times. (← H1) |
| SC2. The mission must be able to return data at the required times. (← H2) |
| SC3. Mission scientific investigators must be able to use the data from the mission at the required times. (← H3) |

Figure 20. High-level Hazards and Constraints

Step 5. Identify Environmental Constraints, Customer-derived Constraints and Programmatic Risks

The next step in the process is to identify:

- environmental constraints and assumptions
- customer-derived system design constraints, and
- customer-derived programmatic constraints (e.g., budgets, etc.).
- programmatic risks

Environmental assumptions and constraints describe and model the both the natural and manmade environment of the system. Engineers should include assumptions that will inform or constrain the design. Given a goal of the mission to explore the moon of an outer planet, information regarding lighting conditions, existing space infrastructure, radiation environment, atmospheric pressure, gravity, etc. would be documented in this section. In addition, environmental information is documented for other environments that the mission will encounter before and after the primary mission at the icy moon. Examples of environmental assumptions can be found in Figure 21.

EA.1 Gravitational Effects: Characterization of the Europa's gravity field is necessary in order to do detailed orbital planning (e.g. whether it is possible to use "frozen orbits" which are more energy efficient to maintain than alternative orbits, but require precise gravity field mapping).

EA.2 Particle Radiation: Characterization of Europa's particle radiation environment will provide key insight for future missions. The icy moon's radiation environment is a critical unknown determining mission life. The harsh environment induced by radiation trapped by Jupiter is limiting factor to mission life and onboard data storage options. Furthermore, the radiation activity on the icy moon could provide one of the critical ingredients for life.

....

EA.8 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 mission.

Rationale: It is possible for the 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).

Figure 21. Example Environmental Assumptions

Environmental assumptions and constraints are documented in level 1 of the intent specification. Non-textual models of key environmental state variables that drive design should be included e.g., surface temperature of the icy moon; ephemeris state of the sun, the outer planet, and the icy moon. Later steps and iterations of the process will revisit the environmental assumptions when more detailed requirements and constraints have been derived, and when system engineers have a better understanding of what level of fidelity is required.

Figure 22 shows a more complete example of a Jupiter radiation model. A general description of the model is given, including sample output in Figure 23, a link to the software implementation of the model as well as rationale as for why the model is included in the intent specification.

EA.3 Jupiter Radiation Model:

The radiation environment near Jupiter has been measured by several spacecraft (Pioneer 10 and 11, Voyager 1 and 2, and Galileo missions), results of which led to the creation of the Galileo Interim Radiation Electron Model (GIRE).

The GIRE model is available for public download here:
<http://www.openchannelfoundation.org/projects/GIRE/>

JPL has used the GIRE model to calculate that a 3.4 Mrad Si environment behind 100 mils of Aluminum equivalent will be required to withstand the expected radiation doses for a 90 day mission.

Different radiation sources dominate the radiation environment on Europa at different depths. An output from the GIRE model is shown in Figure 23.

Rationale for inclusion in the intent specification: The degree to which increasing shield thicknesses will be able to withstand the expected radiation doses will determine what level of shielding is chosen to protect various spacecraft components.

Figure 22. Jupiter Radiation Model

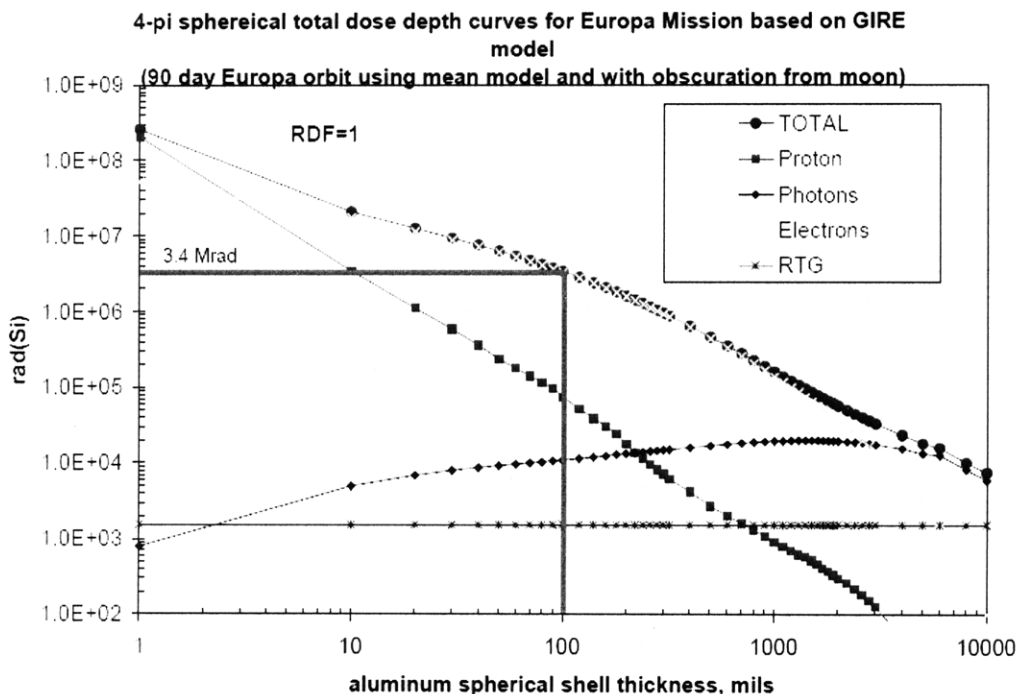


Figure 23. GIRE Output for Various Radiation Sources on Europa [31]

Customer-derived programmatic constraints are typically constraints on budget and schedule and will influence the design of the entire system. While these constraints should not be violated in efforts to achieve mission goals, it is often the case that they cannot all be satisfied. It is helpful for engineers to analyze trades between the constraints and use the design trades, programmatic

and safety risks to choose between mission performance and satisfying programmatic requirements. Figure 25 shows an example of customer programmatic constraints. Customer programmatic constraints, like mission goals and requirements, can be drawn from or inspired by a number of standard information sources such as: governmental mandates, corporate policies, laws, and standard system safety practices. Customer programmatic constraints are documented in level 1 of the intent specification.

Customer-derived system design constraints are constraints on the design of the system that are technical in nature. Typically, they involve how the system must interact with existing resources, engineering mandates, or initiatives the customer wishes to implement. Figure 24 shows an example of customer-derived system design constraints. Customer-derived system design constraints are documented in level 1 of the intent specification.

Violations of customer-derived design constraints could be considered an accident or unacceptable loss. If so, the accident list at level 0 of the intent specification should be updated and the customer-derived design constraints and accidents should be linked.

<p>DC1. The memory allowable on board the spacecraft is TBD. (←EA.2) <i>Rationale: Radiation hard memory beyond TBD is not available.</i></p> <p>DC2. The mission must utilize and be compatible with the current Deep Space Network (DSN) as well as with modifications currently under consideration for communication beyond earth orbit. <i>Rationale: The DSN is NASA's primary resource for ground communication with spacecraft operating beyond earth orbit. The salient modification to the DSN is the use of arrays of smaller antennas rather than single 70 meter antennas.</i></p>

Figure 24. Examples of Customer-Derived Design Constraints

<p>PC1. The mission must not cost more than TBD dollars total and/or TBD dollars for any given fiscal year. (↑PR1)</p> <p>PC2. The mission must launch in the year 2015. (↑PR2)</p>

Figure 25. Examples of Customer-Derived Programmatic Constraints

The violations of programmatic constraints that would not be considered to be an accident should be treated as programmatic risks. Programmatic risks are documented in level 0 of the intent specification with links pointing to programmatic constraints. An example of a programmatic risk is shown in Figure 26. Engineers may consider programmatic risks when considering architecture or design trades. If two particular architectures or designs offer similar performance, but the cost of one could be more expensive, the engineers may want to choose the design with the more certain cost estimate. Engineers may even choose to scale back performance requirements in order to achieve certain budget and schedule risks.

<p>PR1. Mission costs exceed TBD dollars total and/or TBD dollars for any given fiscal year. (↓PC1)</p>

Figure 26. Example of a Programmatic Risk

Step 6. Perform High-level Functional Decomposition

After the goals and external constraints are defined and documented, the next step in the process is to perform a high-level functional decomposition to define the system functions and assign functions to high-level system components.

The usual next step in systems engineering, after definition and definition of the goals and external constraints, is to perform a high-level functional decomposition to define the system functions and assign functions to high-level system components. The assignment of functions to components has a huge impact on safety and should involve an analysis to assist in making safety-related decisions. For example, if, for business reasons, management decides to use radio-isotopic thermoelectric generators (RTGs), this decision will introduce a hazard of dispersion of radioactive materials in Earth's atmosphere. In order to incorporate safety from the beginning of the design process we recommend following a risk-based architectural approach, such as that described in "Incorporating Safety in Early System Architecture Trade Studies" [8].

Physical and informational coupling across functional components of complex systems has often been cited as a major factor in the accidents that occur in complex systems [10]. Therefore, once all high-level functions and physical interactions are recorded, functions should be assigned to individual functional elements in a manner that minimizes coupling across the functional elements. While a functional analysis can be performed in various ways, Design-Structure Matrices (DSMs)² [9] was found useful during the application of this safety-driven process to an outer planet explorer mission, included in section 4. As functions necessary to meet the system's requirements and constraints were identified, physical and informational interactions between these functions (e.g., energy exchanges, information exchanges, and/or material exchanges) were also identified and recorded in the DSMs. DSMs are particularly useful for functional decomposition because they can be analyzed and functions can be clustered to minimize physical and informational coupling across functional components. Once these functional elements are identified, requirements and constraints are derived for them. Later steps in the process discuss how lower-level functional elements are iteratively identified.

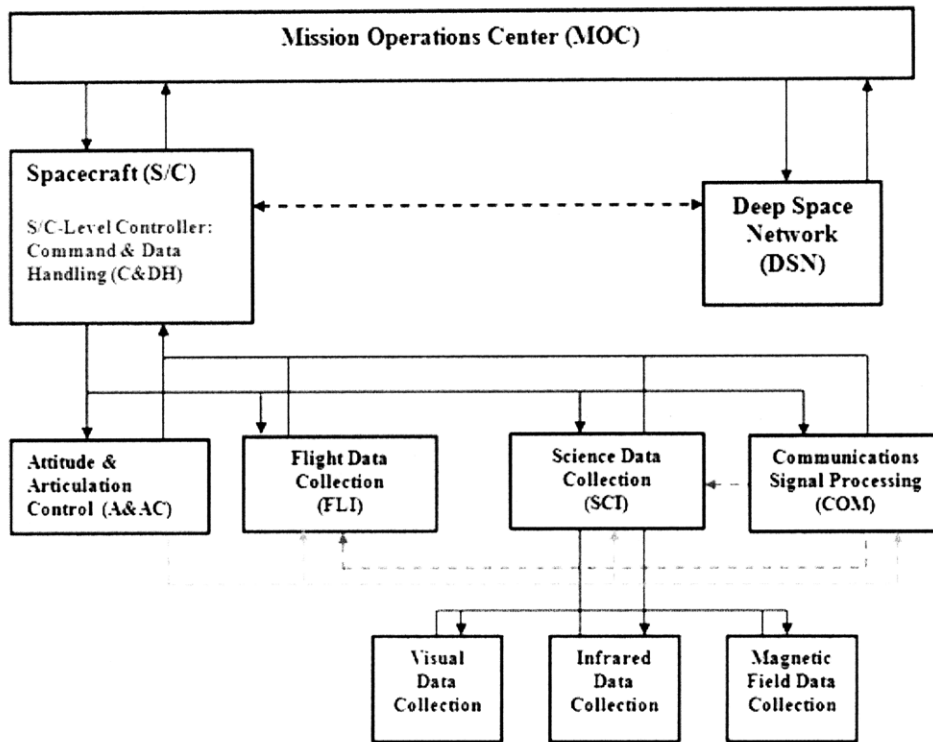
Step 7. Design High-level System Control Structure

Another important aspect of high-level design is designing the system control flow. The control structure is a graphical representation of the control flow between the system functional elements. In this step of the design process, engineers should start to define the control hierarchy of the system and document it in the intent specification. At each level of functional decomposition, each functional element is assigned responsibility for the control of the functional interactions within the element while one hierarchically superior element is assigned responsibility for control of the interactions across elements. Note that these assignments are not necessarily a description of the software and hardware architecture, but a representation of the functions the system must perform and how the functions are related to each other. Using the results of the functional analysis, a high-level system control structure is designed. An example

² Design Structure Matrices are also referred to as N-Square Diagrams, Dependency Structure Matrices, Incidence Matrices, Dependency Maps, Interaction Matrices, Design Precedence Matrices, etc. in the literature.

system control structure for a spacecraft is shown in Figure 27. In the example (and in current standard spacecraft architectures), interactions between spacecraft functional elements are controlled by the spacecraft command and data handling functional element (C&DH) while interactions between functional elements of the Attitude and Articulation Control (A&AC) functional element are controlled by the A&AC command and data handling functional element (AC&DH).

The iteration section after Step 12 discusses how the control structure can be evolved iteratively to capture lower-level interactions and inform the lower-level design.



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
<div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 0 auto;"> Functional Element Name Functional Element Level Controller (if applicable) </div>	Functional Element with the controller of its internal interactions (i.e., the functional element-level interactions)

Figure 27. Control Structure and Legend

Step 8. Perform Preliminary Hazard Analysis

Using the information obtained in Steps 1 through 7, a preliminary hazard analysis using STPA is performed and the system hazard log is created.

After high-level design is created, STPA is used to identify inadequate control actions that would allow the existence of hazardous states in the system and control flaws and inadequate control executions that could instantiate an inadequate control action. As discussed previously, the engineer has several options after identifying the control flaws and inadequate control executions and will either modify or create new safety constraints or design until all hazards are eliminated, mitigated, or controlled.

STPA is performed as described in the background section 2.3. The results of STPA are recorded in the hazard analysis section of the intent specification, in level 1. It is worth reiterating from section 2.3 that in the initial phase, not much of the design information is known and the STPA process will focus on safety constraint refinement and architecture selection. STPA is an iterative process and in later iterations, STPA will involve more design refinement to enforce the safety constraints.

A partial result of an STPA hazard analysis from the Outer planet moon mission example is shown below in

Figure 28. The referenced hazards and safety constraints can be found in section 4. The hazard log is not meant to be read stand-alone. The hazard log is a record of the STPA process and is used to discover the reason certain safety constraints were generated. If a reader of the specification wishes to discover what control flaws in the design led to a particular safety constraint they would reference the hazard log. The STPA process is performed as usual and recorded as follows: Each inadequate control action is recorded once, and the relevant safety constraints and hazards are listed. For each inadequate control action the related control flaws and inadequate control executions are listed. The STPA process may lead the engineer to the discovery of C&DH-ICA1 by analyzing any of the hazard and safety constraint combination from the hazards and safety constraints below, but it is not relevant in a top-down presentation of the analysis to denote which safety constraint first leads to C&DH-ICA1.

The associated design decision column shows all of the design decisions related to the control flaw and associated inadequate control action. It's important to record the associated design decision because the engineer may decide to modify the original design to enforce the constraints. In the far right column new requirements or constraints or refined requirements or constraints are listed.

The control structure is a useful aid to performance of STPA. Each branch can be analyzed for inadequate control actions and control flaws. Control flaws at a particular level of control can be addressed on that level of control with safety constraint and design that eliminates (or mitigates) the control flaw at that level, or can a safety constraint can be refined and assigned to functional elements at higher or lower-levels of control.

An example of a control flaw at one layer of control resulting in a safety constraint at a higher level of control is shown below:

The inadequate control action:

S/C-ICA1: The spacecraft does not maintain the science orbit to within TBD degrees and the data is either not collected, not returned to earth, or the orbit degrades and resources are wasted or the orbiter unintentionally crashes into the outer planet moon.

The inadequate control action S/C-ICA1 can occur due to the control flaw:

S/C-CF1.1: The spacecraft does not make orbit correction maneuvers as often as required. (Around once every 24 hours.)

The resulting safety constraint:

C&DH-SC9: The C&DH must command the A&AC to perform orbital correction maneuvers to maintain the science orbit to within TBD degrees.

Rationale: Low, circular, near polar orbits left uncontrolled will degrade and impact the surface of the moon within tens of days.

The safety constraints generated with STPA will directly generate safety-driven design. In later steps, each safety constraint is either enforced in design or refined and then enforced in design. Design in level 2 can be written directly, without STPA, but using STPA brings safety into the design process in a rigorous fashion.

Inadequate Control Actions, Control Flaws, and Inadequate Executions of Control Actions	Relevant High-level Hazard(s)	Associated Design Decision	Resulting Safety Constraint(s) or Requirements
<p>S/C-ICA1 The spacecraft does not maintain the science orbit to within TBD degrees and the data is either not collected, not returned to earth, or the orbit degrades and resources are wasted or the orbiter unintentionally crashes into The outer planet moon .</p>	<p>H1. Inability of Mission to collect data H2. Inability of Mission to return collected data. H4. Contamination of Outer Planet Moon with biological agents of Earth origin on mission hardware.</p>	<p>S/C-2.1. The spacecraft’s science orbit will be low altitude (between 100 and 500 km), near circular, and near polar (within TBD degrees). <i>Rationale: The science instruments require a low, circular, polar orbit for surface mapping fidelity.</i></p>	
<p>S/C-CF1.1. The spacecraft does not make orbit correction maneuvers as often as required. (Around once every 24 hours.)</p>			<p>C&DH-SC9. The C&DH must command the A&AC to perform orbital correction maneuvers to maintain the science orbit to within TBD degrees. <i>Rationale: Low, circular, near polar orbits left uncontrolled will degrade and impact the surface of the moon within tens of days.</i></p>
<p>S/C-ICA2 The spacecraft is not able to transmit the data collected back to Earth.</p>	<p>H2. Inability of Mission to return collected data.</p>	<p>SCI-2.1.1. High-rate science data (from the WAC and IRC) is collected,</p>	

<p>S/C-CF2.1. The SCI collects high-rate data during non-communication periods. (Co-ordination control flaw between SCI and C&DH.)</p>		<p>compressed in hardware, packetized and buffered on the science mass memory before transmission to the DSN during Communication periods on command from the C&DH. <i>Rationale: High-rate data cannot be taken during non-communication periods due to scarce memory resources.</i></p>	<p>C&DH-SC12. The C&DH must not command SCI to collect data during non-communication periods. SCI-SC10. The SCI must not collect any high-rate data during non-communication periods. <i>Rationale: High-rate data collected during non-communication periods would quickly fill up the science mass memory, and consequently be overwritten and lost. The science mass memory is intended to act as a high-rate data buffer before transmission to the MOC.</i></p>
<p>S/C-CF2.2. The center of mass shifts due science boom flexibility.</p>			<p>A&AC-SC5. The A&AC must be robust to disturbances from instrument mechanisms and science booms within a TBD range.</p>
<p>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)</p>	<p>H1. Inability of Mission to collect data H2. Inability of Mission to return collected data. H4. Contamination of Outer Planet Moon with biological</p>	<p>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</p>	

<p>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.</p>	<p>agents of Earth origin on mission hardware. H5. Exposure of Earth life or human assets on Earth to toxic, radioactive, and/or energetic elements of mission hardware. H6. Exposure of Earth life or human assets off Earth to toxic, radioactive, and/or energetic elements of mission hardware. H7. Inability of other space exploration missions to use shared space exploration infrastructure to collect, return, and/or use data.</p>	<p>state, generates a schedule for directive execution and/or delegates them to the appropriate functional elements.</p>	<p>C&DH-SC1. The C&DH must have the capability to reason about the state of the spacecraft and plan the execution of MOC directives so that the initial conditions of a directive are valid.</p>
--	---	--	---

Figure 28. Partial STPA Hazard Analysis

Creation of the hazard log follows STPA. For each high-level hazard, the functional element pertaining to the hazard is listed as well as the relevant operation or mission phase. The causal factors shown in the hazard log are pointers to the control flaws identified in the STPA analysis. The hazard log also captures other information such as the hazard severity and type of potential loss resulting from the hazard. An example of the hazard log is shown below in Figure 29. The hazard log is documented in level 1 of the intent specification.

Discussion regarding further iterations of STPA will be discussed later in this section.

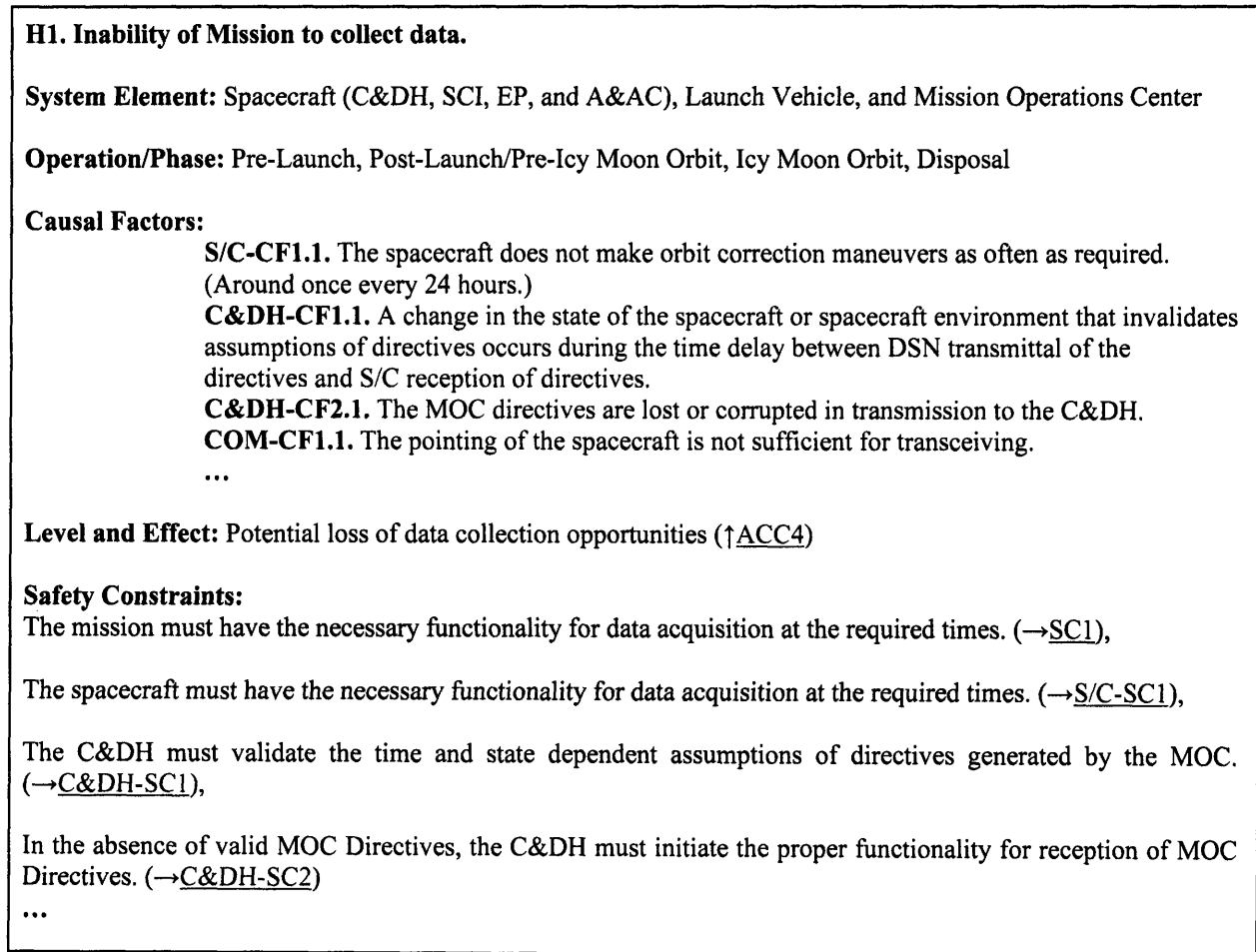


Figure 29. Partial Hazard Log Example

Step 9. Define Lower-level level 1 Specifications

For each functional element identified in the high-level functional decomposition and control structure, identify system-element goals, assumptions, requirements, design constraints and safety constraints using system-level goals, requirements and constraints. Figure 30 and Figure 31 are examples of system-element level 1 specifications with links shown between subsystem goals, requirements, assumptions, and constraints.

The definition of level 1 specifications for system elements is iterative, and will be discussed in more depth near the end of this process description. The first time step 9 is performed the

specification of system elements will be fleshed out. Subsequent iterations will involve the definition of goals, assumptions, requirements, and constraints on lower-level functional elements defined by further iterations of steps 9 through 12.

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 manage the interactions between the lower-level functional elements that the C&DH controls (Flight Data Collection, Science Data Collection, Communications Signal Processing, and Attitude and Translation Control) so that spacecraft goals are met. (←S/C-G1) (→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)

C&DH-G2. To transmit the data required to fulfill spacecraft goals and ensure that the MOC has spacecraft health and status state information that is no older than TBD seconds during comm times. (←S/C-G1) (→C&DH-R1, C&DH-R8, C&DH-R9)

C&DH-G3. To prioritize, schedule, and execute MOC directives so that spacecraft goals are met. (←S/C-G1) (→C&DH-R1, C&DH-R2, C&DH-R4, C&DH-R6, C&DH-R8)

Rationale: There is a significant time delay between Earth and Europa and some on-board execution scheduling ability will allow the mission to take advantage of scientific opportunities.

Spacecraft Command & Data Handling (C&DH) Requirements

C&DH-R1. The C&DH shall create and revise mission plans in accordance with Spacecraft health, Science data collection needs and MOC directives. (←C&DH-G1, C&DH-G2, C&DH-G3, C&DH-G4)

C&DH-R2. The C&DH shall issue science data collection, storage and transmission related directives to the SCI in accordance with the mission plan. (←C&DH-G1, C&DH-G3)

C&DH-R3. The C&DH shall monitor feedback measurements from the SCI and revise its mission plan accordingly. (←C&DH-G1)

Rationale: The C&DH must know the health and status of the spacecraft.

Figure 30. Level 1 Outer Planet Moon Mission Example

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

C&DH-DC1. The C&DH must be able to receive and process directives from the MOC. (←CS1)

C&DH-DC2. Due to the low availability of radiation hard memory, no data will be re-transmitted. (←EA.2)
(→C&DH-SC8)

Rationale: A new data collection and transmission can be initiated on request but data will not be stored onboard the spacecraft. High rate data will be taken during comm periods and immediately processed and transmitted to earth.

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

C&DH-SC1. The C&DH must have the capability to reason about the state of the spacecraft and plan the execution of MOC directives so that the initial conditions of a directive are valid. (←C&DH-CF1.1)

C&DH-SC1.1. The C&DH mission planner and executor must be able to generate plans that re-orient the spacecraft within TBD seconds so that spacecraft initial conditions are compatible with MOC directives.

Rationale: During the time delay between flight data status downlink and receipt of MOC directives, the MOC directives may not be compatible with current mission state. In this case new directives can be sent, or the onboard mission planner and executor (part of the C&DH) can generate a plan to make spacecraft state compatible with the initial conditions specified by the MOC directives within TBD seconds.

C&DH-SC1.2. The C&DH must ask for a new set of directives if the current state of the spacecraft is incompatible and the onboard mission planner and executor (part of the C&DH) cannot find a new plan and execute it so that the current state is compatible with the directives within TBD seconds.

Rationale: For example if the spacecraft is damaged or low on power such that a requested re-orientation is not possible, then a request for new directives would be appropriate. This situation could arise if the spacecraft is damaged in the time delay between the MOC receipt of health and status from the spacecraft and receipt of the new set up directives by the C&DH.

Figure 31. Level 1 Constraints Outer Planet Moon Explorer Mission Example

Step 10. Define Lower-level Design

The lower-level requirements and constraints in level 1 and the hierarchy in control structure are implemented with design in level 2. An example of design decisions that implement the C&DH level 1 requirements and constraints is shown in Figure 32. The first time step 10 is performed, the system element level 2 design specifications will be recorded. Subsequent iterations through step 10 will specify specifications for lower-level functional elements identified in subsequent iterations through 9-12.

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, generates a schedule for directive execution and/or delegates them to the appropriate functional elements. (↑C&DH-C1), (←S/C-2.1), (↓C&DH-ICA1, C&DH-ICA2) (↑C&DH-CF1.1, C&DH-CF2.1)

C&DH-2.1.1. The C&DH generates new mission plans in the event of off-nominal safety-related states or science opportunities.

Rationale: The C&DH should schedule and execute MOC directives except when the spacecraft has detected an unsafe state or fault mode, (such as high temperature or unresponsive reaction wheels) or a high-priority science opportunity arises (such as the discovery of an unexpectedly hot spot on the European surface).

Many faults can be diagnosed and treated on-board the spacecraft without waiting for a new plan from the MOC. During such a delay, the spacecraft state could further deteriorate and new directives from the MOC could be inappropriate for the evolving state onboard. Generation of new mission plans onboard prevents asynchronous evolution between the MOC and the spacecraft.

Similarly, if the science collection functional elements discover a predefined, high-priority science scenario, the spacecraft should immediately investigate it, rather than proceeding with lower-priority data collection. A hot spot on the European surface may mean the discovery of new life, and waiting for the spacecraft to downlink the data and for relevant new MOC directives could mean an intolerable loss of investigation time or an altogether missed investigation opportunity. (→The scientist's model for predicted infrared readings on the icy surface)

C&DH-2.1.1.1 If the current set of directives from the MOC are incompatible with spacecraft state, and the C&DH is unable to generate a plan to transition the spacecraft state to be compatible with the MOC directives, the C&DH will request new directives from the MOC and downlink current and projected spacecraft state to the MOC. (↑ C&DH-SC1.2)

C&DH-2.1.1.2 Whenever the spacecraft has finished executing all available MOC directives and no off-nominal health or science events have occurred the spacecraft maintains its orbit and collects low-rate science data. (↑C&DH-SC3)

Rationale: The low-rate science data can be collected for TBD hours before becoming too large to be stored on the science mass memory.

C&DH-2.1.1.3 After TBD days, if attempts to communicate with the MOC have failed and power resources are below TBD, the C&DH will generate a mission plan to send the spacecraft on a self-destruct orbit. (↑C&DH-SC4) (→A&AC-2.1)

Figure 32. Level 2 Intent Specification

At this point in the process, any detailed models that were used to derive the design (such as discussed in 2.1.1) should be documented in level 1 or 2 of the intent specification. As iterations through the design progresses these models may be used again during design trades. Or, the inclusion may be required in order to provide design rationale. For example, models of the radiation environment and radiation shielding properties of materials chosen to house data collection instruments should be included. This information is used in the level 2 design for spacecraft mass calculations. An example of a key environmental model is shown in Figure 22 and Figure 23.

Step 11. Define and Design System Operational Behavior

In this step, the system engineer documents design decisions pertaining to the control system. This information serves as the informal description of the control system and helps in the creation of the formal blackbox models.

For example, using the control structure and the system design documented so far, the design specification of how the C&DH controller interacts with other functional is shown below in Figure 33. The design presented in Figure 33 is a high-level description of the C&DH controller behavior that is documented formally in level 3.

C&DH-2.1.2. The C&DH receives state information and sends directives to the spacecraft subsystems and the MOC. The C&DH does not consider any delegated task complete until either a status message is returned from a lower-level functional element and/or it reads a measurement proving that the task was completed. (↑A&AC-CF1.1)

See the ↑Control Structure for functional elements and components connected to the C&DH.

C&DH → MOC

New Directives Request: Feedback to the MOC asking for new directives.

Mission Update: Notifies the MOC of new mission plan and includes current and projected spacecraft state.

MOC → C&DH

Directives: Set of directives from the MOC.

C&DH → A&AC

Orbital Adjustment: Command to adjust the spacecraft's trajectory using thrusters. Command is sent as necessary at periods greater than 24 hours. (↑C&DH-SC11)

Reaction Wheel Desaturation: Reaction wheels are used to maintain pointing of the spacecraft from DSN communications and science data collection. They must be desaturated every TBD hours.

A&AC → C&DH:

Reaction Wheel Measurement: Current state of reaction wheel saturation and position.

Spacecraft Attitude Measurement: Current state of spacecraft attitude.

Spacecraft Trajectory Measurement: Current state of spacecraft trajectory.

Trajectory Adjustment Status: Measurement notifying the C&DH when the next orbital adjustment will be required to maintain desired orbit.

Off-nominal Attitude or Trajectory: Measurement to C&DH that the A&AC has detected an off-nominal attitude or trajectory state.

Figure 33. Outer Planet Moon Explorer Mission Example of System Operational Behavior

Step 12. Develop Formal Models of the System

In this step, the system engineers design and specify blackbox models of the control system using SpecTRM-RL. (Refer to Figure 35 for an example). Engineers use level 1 requirement and constraints, the control structure and level 2 control system design to create the blackbox models. For instance, there will often be safety constraints listed in level 1 for the maximum time allowed between safety-critical measurement readings. This information is used to specify the transition of a measurement from *valid* to *obsolete* in the SpecTRM-RL process model. Depending on the state variable, an obsolete measurement may, in turn, cause the estimate of a state variable to become UNKNOWN.

DEFINITION

= New Data for Health and Status				
	Health and Status was Received			T
= Previous Value of Health and Status				
	Health and Status was Received			F
	Time Since Health and Status was Last Received ≤ TBD seconds			T
= Obsolete				
	System Start		T	
	Health and Status was Never Received		T	
	Time Since Health and Status was Last Received > TBD seconds			T

Figure 34. Example *And/Or* Table

In summary, the formal control system design can be created according to the following guidelines:

1. The hierarchy of control modeled at level 3 should reflect the control structure described in level 2.
2. Control system behavior and the process model should reflect design described in level 2.
3. Control system design must enforce constraints and requirements documented in level 1.

Although there are other ways of creating the formal control system design, process model sketches can be used to help create the formal control system models. The process model sketch in Figure 36 can be used to aid in generation of formal blackbox behavior model. A visualization of the formal control system design of the Science Functional Element is shown in Figure 35. The design of a controller must include:

1. The state variable being controlled by this element of the control system (in this example, this state variable is the Science Opmode).
2. All of the affecting state variables of the state variable being controlled by this element of the control system, which would be considered process inputs in the generic control loop shown in Figure 6. The controller in Figure 35 uses the “Communication Interface,” “Active Instrument Pointing,” “Memory,” “Temperature,” “Wide Angle Camera,” “Magnetometer,” and “Infrared Camera” states.

3. All of the measurements in the state influence diagram affected by the state variable being controlled by this element of the control system, and other state variables directly affecting these measurements. The controller in Figure 35 uses the “Power,” “Radiation,” and “Communications Pointing,” measurements.

The state variables referred to in 1 and 2 are the relevant state variables needed for the control system to choose control modes. The measurements referred to in 3 are required for the control system to infer the value of the state variables in 1 and 2 and thus infer the state of the process to be controlled.

However the formal models are generated, they are written in SpecTRM-RL and can be used for traceability, completeness analysis, and automatic code generation. In the SpecTRM-RL model of the controller, the process model of the controlled system’s state variables will always have an “Unknown” state. If, for example, a measurement was not received, the controller may not be able to infer the current value of a state variable and the controller’s model of that state variable would transition to “Unknown.” For a complete executable model, physical components being controlled must be specified as well. Physical components can be specified in SpecTRM-RL directly, or the SpecTRM-RL controllers’ components can be put into a simulator harness that contains the physical components. Note that specification of physical components in SpecTRM-RL does not include an “unknown” state because it is specification of the actual component, rather than the controller’s process model.

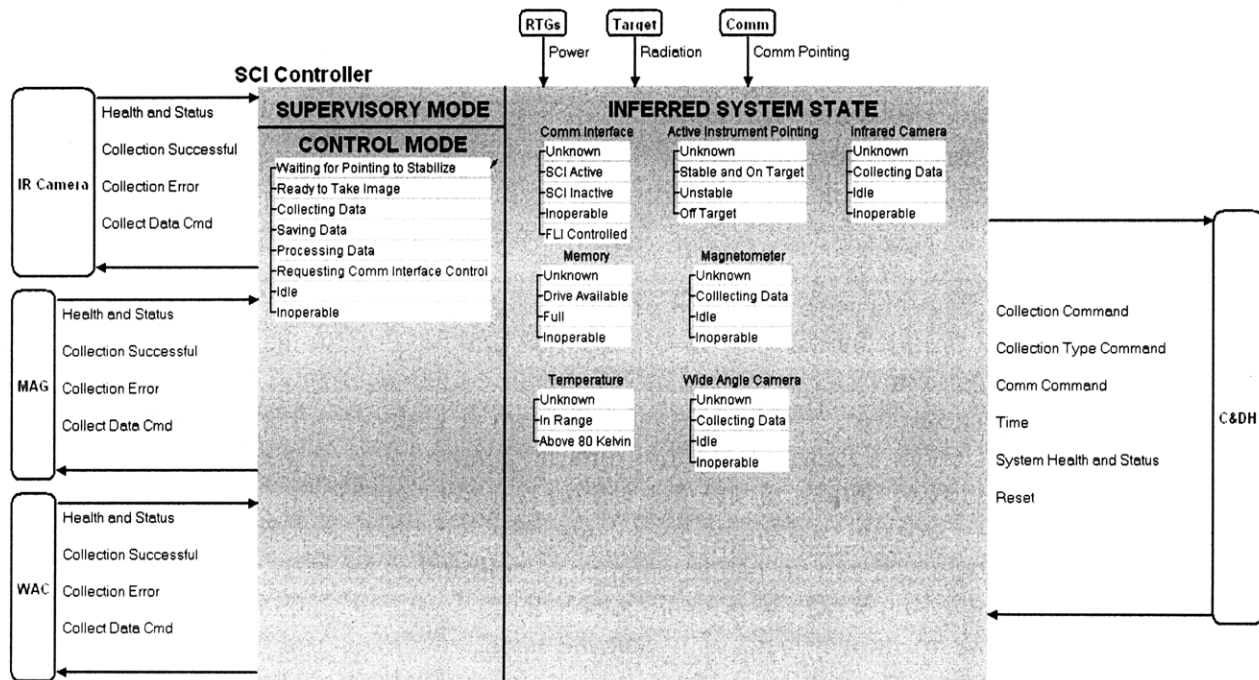


Figure 35. Outer Planet Moon Explorer Mission Example of Science Functional Element Controller

Iteratively Refine the System Design and Continue to Perform STPA

It is important to note that the process steps are iterative and STPA is performed simultaneously with the creation of design and lower-level design steps: As new design is created and new control flaws and inadequate control executions are found, new constraints are generated and new design is created in turn to implement them. Naturally, the lower-level design steps will be performed iteratively as the design is refined for each subsystem and component. Repetition of lower-level design steps may also change high-level artifacts in the intent specification. Feedback to the higher levels of the intent specification can occur as engineers create new requirements and constraints as a result of STPA; if the hazard analysis inspires engineers to modify level 1 goals or level 2 design decisions. Iterations through the design process are finished when the design is set and all hazards are eliminated, mitigated, or controlled.

The process is an iterative one, with each subsystem design leading to further refinement of the requirements and constraints, further application of STPA, and further system design. Some design decisions will stem from the enforcement of safety constraints as result of STPA and others will enforce requirements and constraints already documented in level 1. Design decisions can pertain to the software control system or the physical structure of the system or any other aspect of the system.

In parallel to the performance of STPA, products completed at a high-level in steps 6 and 7 are iterated on to refine and inform the lower-level design. Another iterative activity done along with the process steps is to refine the graphical system design tools. The three high-level design tools, the functional decomposition, control structure and the state variable diagrams will also evolve as more design is created. However, these inputs are an aid in the design process (as well as provide a visualization of the design) and need only be represented in as much depth as the designers think is useful. The information contained in each is represented in the intent specification, although these graphical tools describing the coupling of the system should aid in the STPA analysis.

Functional Decomposition:

The identification and decomposition of lower-level functional elements must be performed in tandem with STPA and the creation of level 1 specifications. As new or lower-level requirements and constraints are generated, new and lower-level functions within the elements will be identified in the DSM. Additionally, the new functional elements will each be decomposed with a DSM.

Control Structure:

The control structure is another critical element to inform the design process. As more of the specification is completed, the control structure will be fleshed out with more detail, which in turn should aid the STPA hazard analysis. The control structure evolves iteratively to capture lower-level interactions and informs the lower-level design.

Repetition through the steps of the process may even change products from steps 1 through 5. Feedback to the higher-levels of the process can occur as engineers create new requirements and

constraints as a result of STPA or if the hazard analysis inspires engineers to modify system-level goals, constraints or programmatic considerations. Furthermore, other artifacts from steps 1 to 5 can change if new constraints or modified design (perhaps modified as a result of STPA) results in elimination of a high-level hazard and associated safety constraint. Iteration through the process is finished when the design is set and all hazards are eliminated, mitigated, or controlled.

Using Diagrams to aid in this safety-driven system engineering process

Examination of the intent specification, including diagrams can aid in performance of STPA. Representing the relationships between system state variables graphically may be helpful in design creation. Such diagrams allow engineers to brainstorm and identify process inputs and disturbances. For instance, many inadequate control actions stem from poor controller behavior due to the controller's incorrect process model. Examination of the recorded state influence diagram (or any other graphical aid engineers have used during system design) may help in the discovery of previously unnoticed process inputs or disturbances. These missing parts of the process model can be added and STPA performed on the resulting design. These graphical design representations can be used to aid the STPA process and do not need to be included in the final intent specification.

In the diagram shown in Figure 36, engineers have sketched out relevant sources of disturbances on the image taking process, as well as necessary process inputs and control inputs. These kinds of sketches can be helpful to system engineers performing STPA in order to brainstorm control flaws related to each of these or inadequate control executions. For example, an engineer looking at this graph might think along the lines of "what kind of radiation problems can happen to the SCI?" Engineer may consider radiation effects on the SCI data collection mode without the diagram, but the externalizing the engineer's mental model of the system on paper helps free up cognitive resources for looking for complex interactions between state variables that may lead to inadequate control.

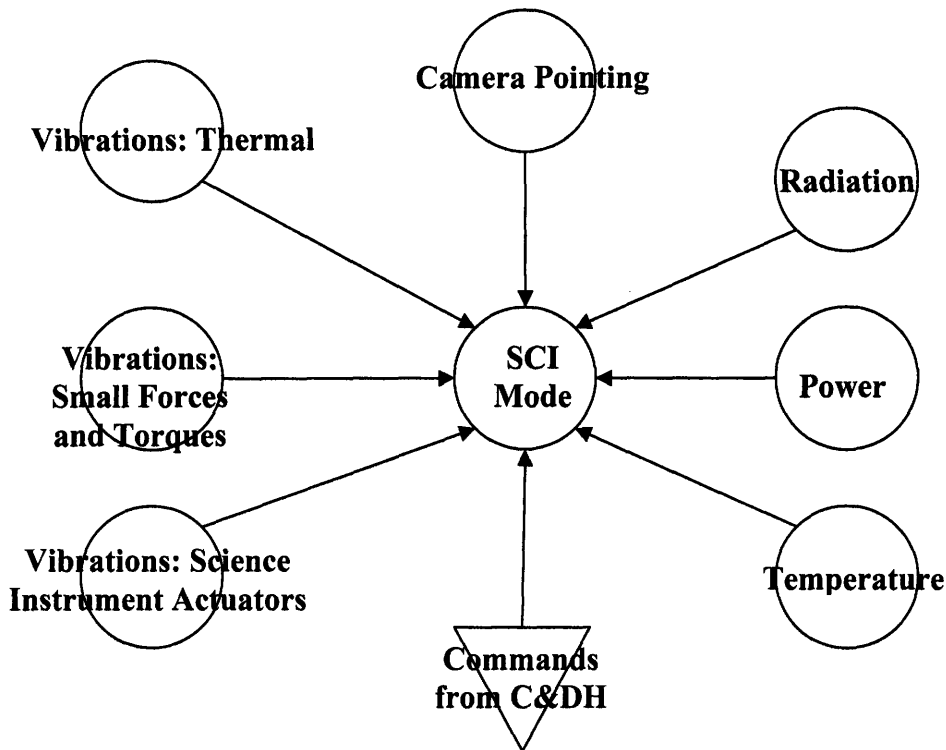


Figure 36. System States Influencing SCI Data Collection

Step 13. Perform Validation Tests

A commercial toolset for creating intent specifications, SpecTRM has several tools for validation. SpecTRM-RL blackbox behavior models are executable and analyses can be performed on them (completeness, robustness, consistency, etc.) to evaluate and identify errors and omissions. If validation tests fail, they will provide an entry point back into modification of the design of the system.

Step 14. Generate Designs and Software Code

The final design of the system including the implementation of the control system in software code and hardware are the ultimate end-products of the process. Physical component designs can be generated from the models, and software code can be generated either manually or automatically.

3.1 Partial Safety-driven System Engineering Process Map

Figure 37 shows a partial map of the safety-driven system engineering process. Several potential feedback discussed in the step descriptions above were omitted for the sake of clarity. It is worth noting that the process is not a linear, “cookbook” process. This process is intended to support the natural opportunistic and iterative kind of design that good engineers typically

follow, rather than trying to confine the design process into a rigid series of steps, which is often not followed and presents an encumbrance to the engineer.

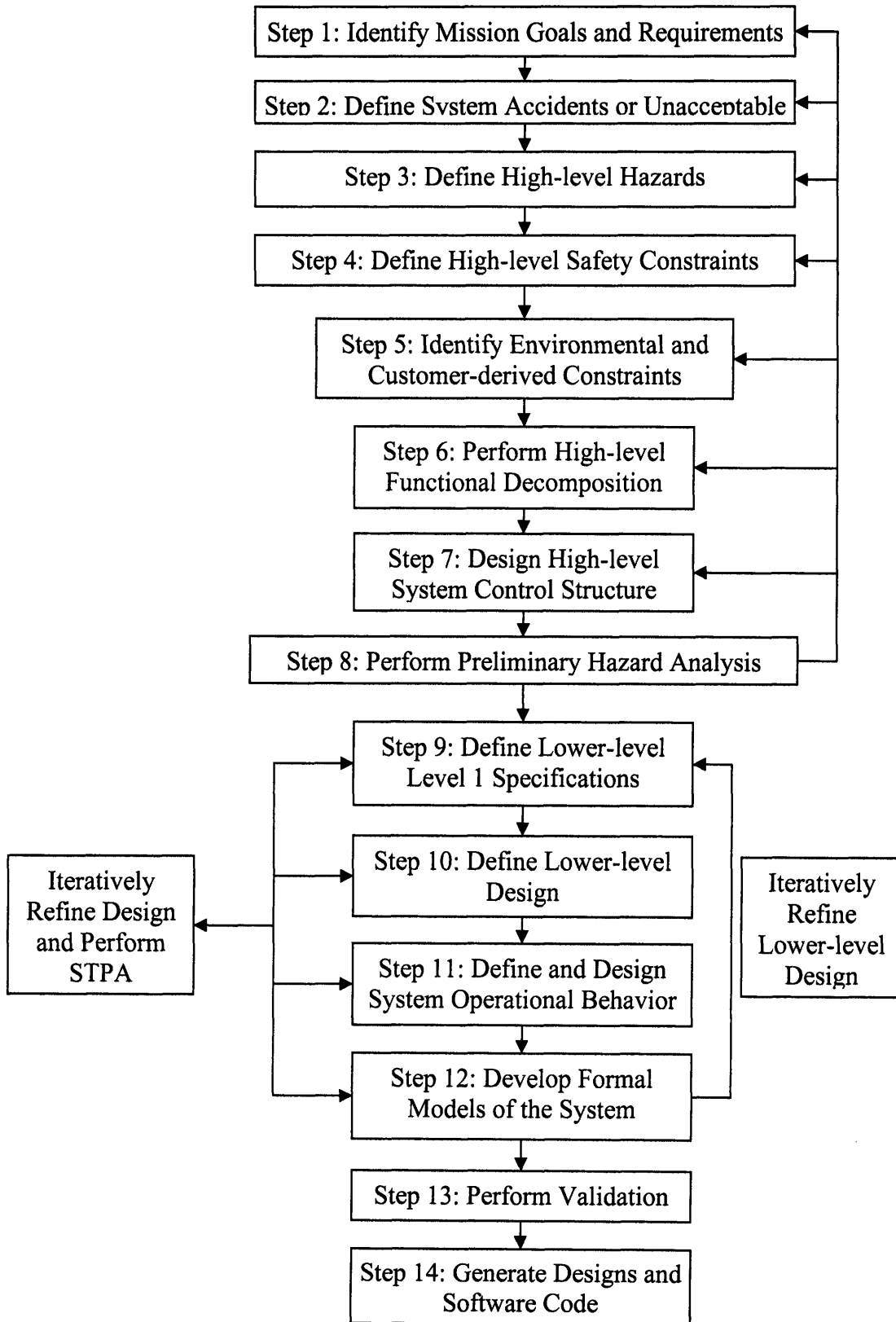


Figure 37. Partial Map of the Safety-driven System Engineering Process

3.2 Process Summary

1. Identify Mission Goals, Requirements and Constraints.
Products: Level 1 intent specification of mission goals and constraints
2. Define System Accidents or Unacceptable Losses
Products: Level 0 intent specification documenting the accidents.
3. Define High-level Hazards.
Products: Level 1 intent specification documenting high-level hazards.
4. Define High-level Safety Constraints
Products: Level 1 intent specification documenting safety constraints.
5. Identify Environment and Customer Constraints
 - environmental assumptions
 - customer-derived system design constraints, and
 - customer programmatic constraints (e.g., budgets, etc.).
 - programmatic risksProducts: Level 1 intent specification of environmental assumptions, customer-derived system design constraints, customer programmatic constraints.
Level 0 intent specification documenting programmatic risks
6. Perform High-level Functional Decomposition
Products: Level 1 intent specification documenting the functional decomposition.
7. Design High-level System Control Structure
Products: Level 1 intent specification documenting the high level control structure.
8. Perform Preliminary Hazard Analysis
Products: Level 1 intent specification documenting the STPA hazard analysis and hazard log
9. Define Lower-level Level 1 Specifications
Products: Level 1 intent specification documenting goals, requirements, design constraints and safety constraints for each subsystem or functional element.
10. Define Lower-level Design
Products: Level 2 intent specification documenting design decisions made to implemented the requirements and constraints on level 1.
11. Define and Design System Operational Behavior
Products: Level 2 intent specification documenting high-level system operation design.

12. Develop Formal Models of the System

Products: Level 3 intent specification documenting the formal blackbox behavior of the system

Iterate: Design and STPA

Products: More complete or modified intent specification of levels 0, 1, 2 and 3.

13. Perform Validation Tests

Products: Test results

14. Generate Designs and Software Code

Products: Design specifications and software code.

4. Application of Process to a Outer Planet Moon Exploration Spacecraft

An application of the process described above is presented in the appendix as a partial intent specification. The intent specification is a top-down product, and does not explicitly show the process of how each design decision was made, nor the order in which they were made. As mentioned previously, the requirements and design process is not linear, and so appending a timeline to each item in the specification would only confuse the engineer.

The intent specification of an outer planet moon exploration spacecraft highlights the traceability in the intent specification, the embedded rationale and the total integration of the hazard analysis throughout the spacecraft design.

5. Discussion of Safety-driven System Engineering Process Application and Future Work

Examination of the structure of the intent specification that was produced by applying the safety-driven system engineering process to an outer plane moon exploration mission supports a major claim of this thesis: that the resultant design is safety-driven. Evaluation of the direct links between items in the intent specification example, led to the creation of the intent specification traceability structure shown in Figure 38. The links between specification items also show the numerous paths available to create the specification. For instance, high-level safety constraints are first created after high-level hazards have been identified or after inadequate control actions and control flaws have been found using the control structure. Then high-level safety constraints can be iterated upon or modified. Each link in the diagram represents a transitive influence. For instance, while inadequate control actions are not linked directly to design decisions, they do influence design: the identification of inadequate control actions leads to the identification of control flaws in the design. The identification of control flaws leads to the creation of safety constraints which are then enforced by new design decisions. It follows that closed cycles in the

intent specification traceability structure represent possible iterations in the intent specification creation process.

While the structure of the intent specification allows for the creation of the design without using STPA, the safety-driven process should motivate the use of STPA as well as make STPA the primary driver of the design process. Figure 38 shows seven intent specification items coupled to three hazard analysis artifacts: inadequate control actions, inadequate control executions and control flaws.

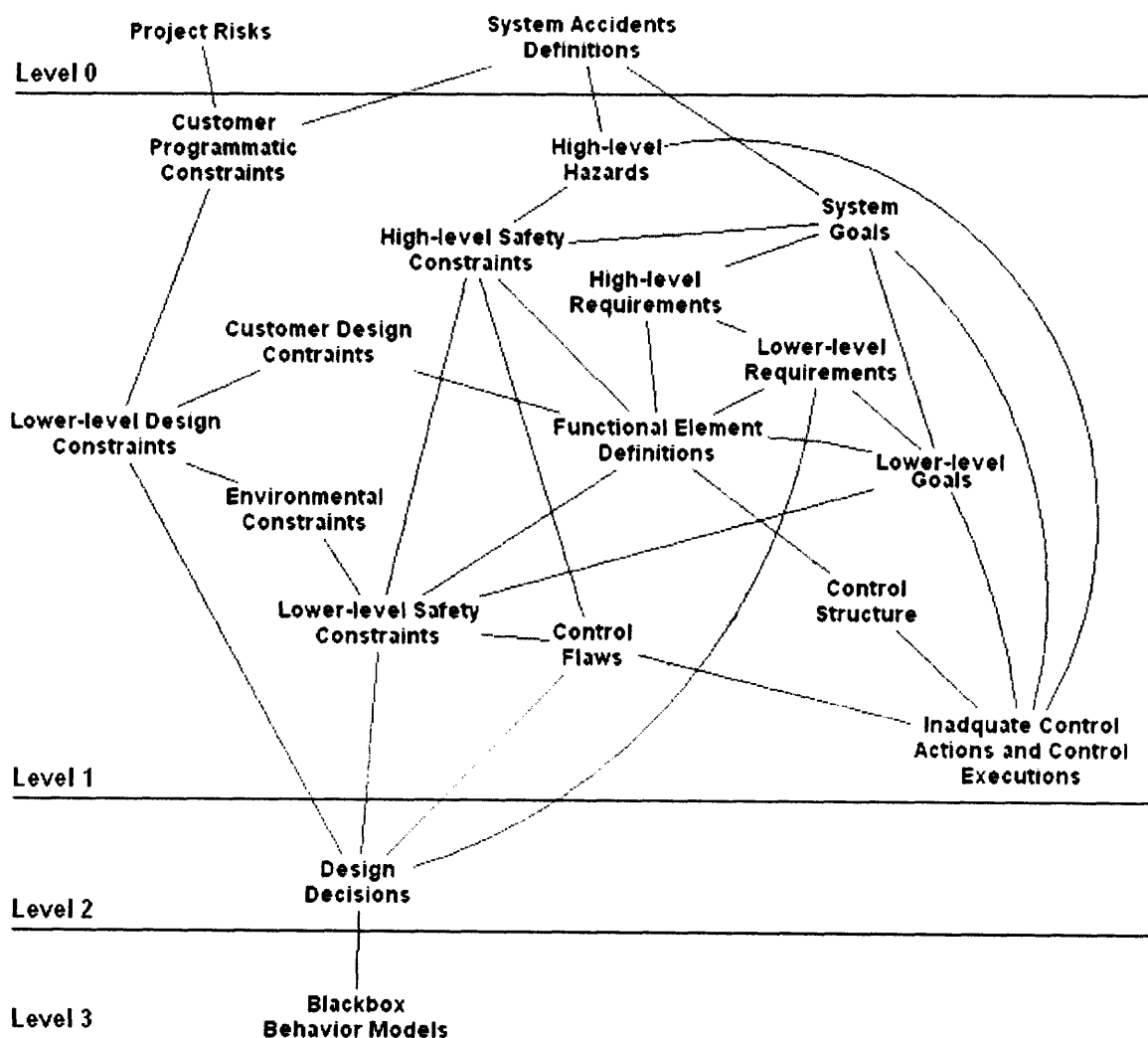


Figure 38. Traceability Structure of the Intent Specification: Levels 0-3.

The structure of the intent specification also would make the creation of tools to aid in engineering or programmatic trade studies very effective. Given that the intent specification is fully traceable, engineers can use the coupling represented in the specification to aid in their

design process. For example, engineers contemplating a design choice may examine the resultant coupling of the design across functional elements. As high coupling has been cited as an indicator of safety risk and a source of accidents, engineers can consider the resultant coupling given by each design choice when designing the system. The system design can be created to minimize the impact of potential design and requirements changes on the rest of the system as well. A tool in the SpecTRM toolset that created coupling graphs for possible design choices is required to make full use of the traceability. This tool would also allow the specification structure to be analyzed for the impact of requirements or design changes. Traceability is also useful to examine the safety impacts in design trades. The creation of design that is linked to multiple control flaws may be further analyzed to consider alternative design options. A design with several control flaws may be adequate, as control flaws can be eliminated with proper safety constraints, but the severity of the control flaws could be used as an indicator for a design that should be reexamined.

The hazard log is the safety engineer's point of entrance to the system. It is used to ensure that each hazard is understood. Similarly, the hazard analysis created with STPA shows how the design addresses each hazard. For these products to be useful to engineers, a tool is necessary to create links between causal factors, hazards, associated design principles and resulting safety constraints that exist elsewhere in the intent specification. In particular, to be understandable, each hazard, safety constraint, etc, must be fully written out, so that engineers are not required to click to another part of the document. Specification readers can easily lose sight of the big picture and become lost after a few jumps. For example, for a particular hazard, an engineer should understand both how the hazard could arise and how the hazard is controlled in the design. It would be ideal if intent specification creators were not required to repeatedly write the same intent specification item (such as a safety constraint) in each of the spots in the intent specification where the item should be listed. A tool should be created to allow mapping of an intent specification item (such as a safety constraint) to all instances of itself within the specification. Furthermore, it would be useful for hazard analysis reviewers to have a tool that links hazard analysis artifacts to the control structure and allows information hiding and exposure.

The safety-driven process could be used to implement the new NASA software safety standard [32], MIL-STD-882, or a similar system safety standard. The NASA standard requires complete traceability between requirements, design, implementation, test and hazard throughout the software life cycle. The standard also requires that the safety analysis is part of a closed-loop feedback path in system design process. In the process, the hazard analysis is folded into the design so that the safety goals of the standard can be attained rigorously, and without needless documentation. The complete traceability of the intent specification aids in several design analyses, as previously discussed in this section.

Applying the safety-driven process and creating the intent specification in the appendix highlights the intuitive nature of this approach in an engineering sense. The hazard analysis brought rigor to the safety design without stifling creativity as in other design processes, and the control theory approach to safety, as used in STAMP, helped apply an engineer's perspective to an otherwise amorphous problem. Using visualizations of the system design to implement the creation of the formal blackbox behavior models was valuable. The diagrams aided the creation

of the controller design and helped determine required control inputs, process inputs, and characterize the effect of disturbances.

The addition of traceability tools to the SpecTRM toolset would aid in the application of the safety-driven process. Other areas of future work should include using the STPA hazard analysis results in design trades. A tool should also be created to allow engineers to use the hazard log to understand the how various design choices impact safety. These tools would allow engineers to integrate safety into all aspects of the design process.

6. Conclusions

Spacecraft engineers have typically considered safety in respect to human and pre-launch safety. By regarding safety as assuring mission success, however, and using safety-driven design, a host of mission failures and accidents could be avoided. This thesis presents an improved system engineering framework to heighten the ability to assure the success of future missions. Implementing this process creates a safer design without unnecessary documentation. The rigor of the process is achieved by reevaluating the creation of typical system engineering specifications and using hazard analysis proactively to inform the system design.

This safety-driven system engineering process defines a rigorous approach to complex system design and addresses the increasing complexity of spacecraft systems. The resulting specification is structured and provides complete traceability. Most critically, the STPA process folds the hazard analysis directly into the design process. Integration of STAMP, STPA, and intent specifications allows system engineers, software engineers and hardware engineers to share a common specification document to describe the motivation and rationale for design decisions and provides access to models used in the creation of the design.

7. References

- [1]. Leveson, Nancy G. (2000), "Intent Specifications: An Approach to Building Human-Centered Specifications, *IEEE Transactions on Software Engineering*, Vol. 26, No. 1, pp. 15-35.
- [2]. Leveson, Nancy G. (2004), "A New Accident Model for Engineering Safer Systems," *Safety Science*, Vol. 42, No. 4, pp. 237-270.
- [3]. Weiss, K., Dulac, N., Chiesi S., Daouk, M., Zipkin, D., Leveson, N. (2006), "Engineering Spacecraft Mission Software using a Model-Based and Safety-Driven Design Methodology," *AIAA Journal of Aerospace Computing, Information, and Communication*, Vol. 3, No. 11, pp. 562-586.
- [4]. Leveson, Nancy (2008), <http://sunnyday.mit.edu/book2.pdf>
- [5]. Leveson, Nancy (1995), *Safeware: System Safety and Computers*, Addison-Wesley Publishing Company. ISBN 0-201-11972-2.

- [6]. Ingham, M., Rasmussen, R., Bennett, M., and Moncada, A. (2006), "Generating Requirements for Complex Embedded Systems using State Analysis", *Acta Astronautica*, Vol. 58, No. 12, pp. 648-661.
- [7]. Clark, Karla B. (2007), "Europa Explorer—An Exceptional Mission Using Existing Technology," *2007 IEEE Aerospace Conference Proceedings*, March 3-10, Big Sky, MT, paper #1417.
- [8]. 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.
- [9]. Browning, Tyson R. (2001), "Applying the Design Structure Matrix to System Decomposition and Integration Problems: A Review and New Directions," *IEEE Transactions on Engineering Management*, Vol. 48, No. 3, pp. 292-306.
- [10]. Perrow, Charles (1999), *Normal Accidents: Living with High-Risk Technologies*, 1999 Edition, Princeton University Press, Princeton, NJ.
- [11]. Hooks, Ivy (1990), "Why Johnny can't write requirements," *Proceedings of the AIAA Conference*, September 25-28, Huntsville, AL,
- [12]. Weiss, K., Leveson, N.G., Lundqvist, K., Farid, N., and Stringfellow, M. (2001), "An Analysis of Causation in Aerospace Accidents," *Proceedings of the Digital Aviation Systems Conference*, October 14-18, Daytona, FL, pp. 137-147.
- [13]. Firesmith, D. (2003), "Modern Requirements Specification" *Journal of Object Technology*, Vol. 2, No. 2, pp. 53-64.
- [14]. Grady, Jeffery (2006), *System Requirements Analysis*, McGraw-Hill, Inc., New York, NY.
- [15]. Hollingworth, K., Saeed, A. (1998), "CoRSA – A Constraint Based Approach to Requirements and Safety Analysis," *Proceedings of the 17th International Conference on Computer Safety, Reliability and Security, SAFECOMP'98*, October 5-7, Heidelberg, Germany.
- [16]. Riff, Maria-Cristina and Zuniga, Marcos (2007), "Towards and immune system that solves CSP," *IEEE Congress on Evolutionary Computation*, September 25-28, Singapore.
- [17]. Leveson, N., Reese, J., Heimdahl, M., "SpecTRM: A CAD System for Digital Automation," *Digital Avionics System Conference*, October 31 – November 6, 1998.

- [18]. Dulac, Nicolas (2003), *Empirical evaluation of design principles for increasing reviewability of formal requirements specifications through visualization*, S.M. Thesis, Aeronautics and Astronautics, Massachusetts Institute of Technology.
- [19]. Wing, J. M. (1990), "A specifier's introduction to formal methods," *Computer*, Vol. 23, No. 9, pp. 8, 10-22, 24
- [20]. Raistrick, C., Francis, P., Wright, J., Carter, C., Wilkie, I. (2004), *Model driven architecture with Executable UML*, Cambridge University Press, Cambridge, England.
- [21]. Koo, S.R., et al. (2004), "An Integrated Environment of S/W Specification and V&V for Safety-Critical Systems," *Proceedings of Software Engineering* February 17-19, Innsbruck, Austria.
- [22]. Sterman, John (2000), *Business Dynamics*, McGraw-Hill, Inc., New York, NY
- [23]. Bruza, P.D. and van der Weide, T. (1993), "The Semantics of Data Flow Diagrams," *Proceedings of the International Conference on Management of Data*, May 25-28, Washington D.C., USA
- [24]. Owens, B., Stringfellow, M., Dulac, N., Leveson, N., Ingham, M., Weiss, K. (2008), "Application of a Safety-Driven Design Methodology to an Outer Planet Exploration Mission," *Proceedings of the 2008 IEEE Aerospace Conference* March 7-14, Big Sky, MT
- [25]. HAREL, D., (1987), "Statecharts: a visual formalism for complex systems," *Science of Computer Programming* Vol. 8, pp. 231-274
- [26]. Larkin, Jill and Herber, Simon (1987) "Why a Diagram is (Sometimes) Worth Ten Thousand Words," *Cognitive Science*, Vol. 11, No. 1, January-March, pp. 65-100
- [27]. Cheng, P., Lowe, R., Scaife, M. (2001), "Cognitive Science Approaches to Understanding Diagrammatic Representation," *Artificial Intelligence Review* Vol. 15 pp. 79-94.
- [28]. Leveson, Nancy (2004), "The Role of Software in Spacecraft Accidents," *AIAA Journal of Spacecraft and Rockets* Vol. 41, No. 4.
- [29]. Weiss, Kathryn (2003), *Component-based systems engineering for autonomous spacecraft*, S.M. Thesis, Aeronautics and Astronautics, Massachusetts Institute of Technology.
- [30]. Wedde, H.F., Cheng, B.H.C., Gries, D., Shankar, N., Lin, K.-J., Ardis, M. (1992), "Are formal methods useful for software development?," *Proceedings of the Sixteenth Annual International Computer Software and Applications Conference* Chicago, Illinois, September 21-25, pp. 2-9, 21-25.

- [31]. Clark, Karla (2007), "Europa Explorer—An Exceptional Mission Using Existing Technology," *IEEE Aerospace Conference Proceedings*, March 3–10, Big Sky, MT.
- [32]. National Aeronautics and Space Administration, NASA (2004), Software Safety Standard, NASA-STD-8719.13B.
- [33]. Dunham, Will (2008), "Software "hiccup" undermines trip past Saturn moon," *Reuters*, March 14.
<http://www.reuters.com/article/scienceNews/idUSN1220873520080314?pageNumber=1&virtualBrandChannel=0>
- [34]. National Aeronautics and Space Administration, NASA (2007), Science Plan, http://nasascience.nasa.gov/about-us/science-strategy/Science_Plan_07_summary.pdf

Appendix

Outer Planet Moon Explorer Intent Specification Outline

Level 0

Project Risks

Accident Definitions

Level 1

System Goals

Introduction

Environmental Description, Assumptions and Constraints

Customer Design Constraints

Customer Programmatic Constraints

List of Inadequate Control Actions and Control Flaws

Hazard List and Hazard Log

High-Level Safety Constraints

High-Level Requirements

Functional Elements and Components

System Control Structure

Spacecraft Goals

Spacecraft Requirements

Spacecraft Safety Constraints

C&DH Goals

C&DH Requirements

C&DH Design Constraints

C&DH Safety Constraints

FLI Goals

FLI Requirements

FLI Design Constraints

FLI Safety Constraints

SCI Goals

SCI Assumptions

SCI Requirements

SCI Design Constraints

SCI Safety Constraints

WAC Goals

WAC Assumptions

WAC Requirements

WAC Design Constraints

WAC Safety Constraints

IRC Goals

IRC Assumptions

IRC Requirements

IRC Design Constraints

IRC Safety Constraints

MAG Goals

MAG Assumptions

MAG Requirements

MAG Design Constraints

MAG I Safety Constraints

A&AC Goals

A&AC Requirements

A&AC Design Constraints

A&AC Safety Constraints

COM Goals

COM Requirements

COM Design Constraints

DSN Safety Constraints

MOC Goals

MOC Safety Constraints

Level 2

Design Decisions

Level 3

Blackbox Models

Outer planet explorer

Level 0: Program Management Information

Project Risks

PR1. Mission costs exceed TBD dollars total and/or TBD dollars for any given fiscal year. (↓PC1)

PR2. Mission launch is delayed beyond 2015. (↓PC2)

Accident Definition

ACC1. Humans and/or human assets on earth are killed or damaged. (↓H5)

ACC2. Humans and/or human assets off of the earth are killed or damaged. (↓H6)

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)

Rationale: It's assumed that 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.

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

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)

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)

Rationale: 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.

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. (↓H4, H5, H6, H7)

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). (→HLR2, HLR4, HLR5, HLR6), (↑ACC4, ACC5)

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). (→HLR1, HLR2, HLR3, HLR4), (↑ACC4, ACC5)

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

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

G5. Characterize the magnetic field and radiation environment of the icy moon of an outer planet (Clark 2007). (→HLR5, HLR6, HLR7), (↑ACC4, ACC5)

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). (→HLR2), (↑ACC4, ACC5)

Introduction

The priority of an outer planet moon mission is high for NASA. This specification will use the planet Jupiter's Europa as a hypothetical candidate for such a mission. Water, one of the key ingredients of life may exist on Europa in substantial quantities. Scientists believe subterranean oceans exist on Europa twice the size of Earth's oceans. Nearby Jupiter has created a radiation intense environment which has created substantial amounts of radiation chemistry on Europa's surface. The radioactive environment in combination with an ocean creates an analogous environment to the life-sustaining hydrothermal vents deep in the Earth's ocean. Characterization of the radiation environment on Europa will provide insight into whether future missions should explore the possibility of life on Europa [34].

“Although oceans may exist within many of the solar system's large icy satellites, Europa's is extremely compelling for astrobiological exploration. This is because Europa's geology provides evidence for recent communication between the icy surface and ocean, and the ocean might be supplied by above and/or below with the chemical energy necessary to support microbial life.”

A mission to Europa would ideally perform a high-precision gravity field characterization and global surface mapping. From these global maps, the mission would then coverage on a few selected targets to investigate to existence of an ocean and should it find one, the interaction between ocean and surface elements.

Environment Description, Assumptions and Constraints

Several key features of the environment have significant impact on the design and structure of the mission. Furthermore, these features are also important to the mission's scientific inquiry.

EA.1. Gravitational Effects: Characterization of the Europa's gravity field is necessary in order to do detailed orbital planning (e.g. whether it is possible to use “frozen orbits” which are more energy efficient to maintain than alternative orbits, but require precise gravity field mapping).

EA.2. Particle Radiation: Characterization of Europa's particle radiation environment will provide key insight for future missions. The icy moon's radiation environment is a critical unknown determining mission life. The harsh environment induced by radiation trapped by Jupiter is limiting factor to mission life and onboard data storage options. Furthermore, the radiation activity on the icy moon could provide one of the critical ingredients for life. (→DC1.1) (→C&DH-DC2)

Jupiter Radiation Model:

The radiation environment near Jupiter has been measured by several spacecraft (Pioneer 10 and 11, Voyager 1 and 2, and Galileo missions), results of which led to the creation of the Galileo Interim Radiation Electron Model (GIRE).

The GIRE model is available for public download here:
<http://www.openchannelfoundation.org/projects/GIRE/>

JPL has used the GIRE model to calculate that a 3.4 Mrad Si environment behind 100 mils of Aluminum equivalent will be required to withstand the expected radiation does for a 90 day mission.

Different radiation sources dominate the radiation environment on Europa at different depths. An output from the GIRE model is shown in Figure 39.

Rationale: The degree to which increasing shield thicknesses will be able to withstand the expected radiation doses will determine what level of shielding is chosen to protect various spacecraft components.

In the radiation of model of Europa it is found that a TBD Mrad (Si) dose of radiation will be accumulate behind 100 mils of Aluminum equivalent.

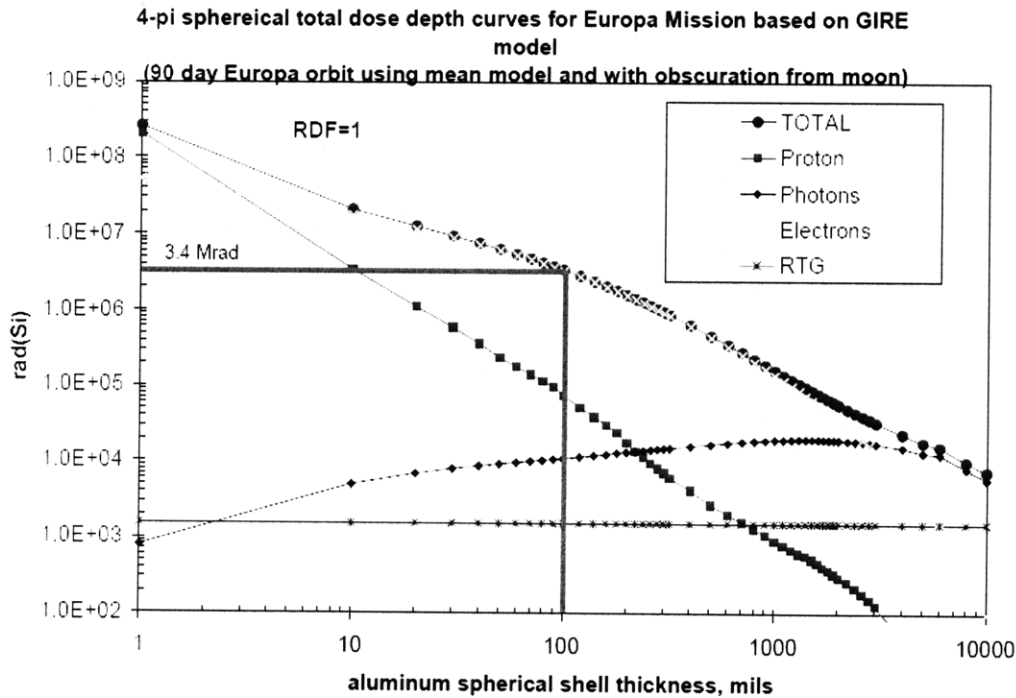


Figure 39. GIRE Output For Various Radiation Sources on Europa (Klark 2007)

EA.3. Thermal Radiation: Characterization of the Europa's thermal radiation will provide key insight for future missions into potential exploration site and the existence of a subsurface ocean.

EA.4. Magnetic Flux: Characterization of the Europa's magnetic flux environment will provide insights into the physical composition of the moon and the existence of an ocean.

EA.5. Communications Occulting: Data transmission times of the mission are driven by communications occulting. The Earth is not visible from Europa for up to 37 percent of each European day. Therefore, a 100 km orbit with a period of 2.1 hours would be occulted for 0.78 hours during which time communications would not be possible. In addition, Jupiter occults Earth every European orbit (every ~3.55 days) and lasts for about 2.5 hours.

EA.6. Translation: The translation and rotation of Europa with respect to the Sun and Jupiter will be relatively stable over the mission and thus predictable.

EA.7. Surface Conditions: The average surface temperature on Europa is minus162 degrees Celsius and as an atmospheric pressure of 10^{-7} bar.

EA.8. 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 mission.

Rationale: It is possible for the 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).

EA.9. 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).

Rationale: In order to stay within the budget and risk profile designated for this mission, new technology shall not be demonstrated.

Customer Design Constraints

DC1. The memory allowable on board the spacecraft is TBD. (←EA.2)

Rationale: Radiation hard memory beyond TBD is not available.

DC2. The mission must utilize and be compatible with the current Deep Space Network (DSN) as well as with modifications currently under consideration for communication beyond earth orbit. (←EA.8)

Rationale: The DSN is NASA's primary resource for ground communication with spacecraft operating beyond earth orbit. The salient modification to the DSN is the use of arrays of smaller antennas rather than single 70 meter antennas.

Customer Programmatic Constraints

PC1. The mission must not cost more than TBD dollars total and/or TBD dollars for any given fiscal year. (↑PR1)

PC2. The mission must launch in the year 2015. (↑PR2)

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
S/C-ICA1 The spacecraft does not maintain the science orbit to within TBD degrees and the data is either not collected, not returned to earth, or the orbit degrades and resources are wasted or the orbiter unintentionally crashes into Europa.	H1, H2, H4	S/C-2.2	

S/C-CF1.1. The spacecraft does not make orbit correction maneuvers as often as required. (Around once every 24 hours.)			C&DH-SC9
S/C-ICA2 The spacecraft is not able to transmit the data collected back to Earth.	H2	SCI-2.6	
S/C-CF2.1. The SCI collects high-rate data during non-communication periods. (Coordination control flaw between SCI and C&DH.)			C&DH-SC12, SCI-SC10
S/C-CF2.2. The center of mass shifts due science boom flexibility.			A&AC-SC5
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.			C&DH-SC1
C&DH-ICA2. The C&DH does not receive an expected 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 MOC directives are lost or corrupted in transmission to the C&DH.			C&DH-SC1
COM-ICA1. The COM does not send or receive commands to/from the MOC.	H1, H2	A&AC-2.1	
COM-CF1.1. The pointing of the spacecraft is not sufficient for transceiving.			A&AC-SC1
A&AC-ICA1 The A&AC moves the spacecraft to the correct attitude for the next science data collection target before current data collection has finished.	H1,H3	C&DH-2.2.1, SCI-2.8	

A&AC-CF1.1. The C&DH receives an incorrect measurement from the SCI that the current data collection task has finished.			SCI-SC11
A&AC-ICA2 The A&AC does not maintain the pointing of the spacecraft sufficiently well for the science data collection instruments.	H1, H3	A&AC-2.1, C&DH-2.1.3	
A&AC-CF2.1. The ability of the A&AC to sufficiently maintain pointing is deteriorated due to disturbances from actuator nonlinearities, thermally induced vibrations, instrument mechanisms, etc.			A&AC-SC4, A&AC-SC5, A&AC-SC6, A&AC-SC7, A&AC-SC8,
FLI-ICA1 The FLI cannot transmit data to Earth at the required time.	H2	C&DH-2.1.4, C&DH-2.1.5, FLI-2.2,	
FLI-CF1.1. The SCI has control of the MTIF to the COM. Rationale: The FLI computer collects health and status data about the spacecraft, and will communicate this to the ground. The inability to communicate after detection of a spacecraft safety-critical fault is detected would be catastrophic.			SCI-SC1, FLI-SC1 C&DH-SC7
SCI-ICA1 The SCI cannot collect the required data at the required times.	H1	SCI-2.1	
SCI-CF1.1. The ability of the SCI to collect data is undermined due to disturbances from actuator nonlinearities, thermally induced vibrations, instrument mechanisms, etc.			A&AC-SC4, A&AC-SC5, A&AC-SC6, A&AC-SC7,
SCI-CF1.2. Radiation causes a single bit upset which corrupts the relevant science data.			SCI-SC5
SCI-CF1.3. Radiation causes a single bit upset which corrupts the instructions sent to the SCI.			SCI-SC5

SCI-CF1.4. The rotation of the Earth starts to occlude the line-of-sight to the spacecraft.			DSN-SC3
SCI-ICA2 The SCI cannot collect Visual data at the required times.	H1	C&DH-2.2	
SCI-CF2.1. The A&AC orients the spacecraft such that the pointing of the spacecraft is incorrect for data collection.			A&AC-SC1, A&AC-SC2, A&AC-SC7, A&AC-SC8,
SCI-CF2.2. The FLI computer is using the SCI's MTIF for data downlink and the SCI does not collect data unless its MTIF is free.		FLI-2.2	SCI-SC1, FLI-SC1 C&DH-SC7
SCI-CF2.3. The WAC's field of view is obstructed by space debris.		WAC-2.1	NONE. Risk of Control Flaw is accepted
SCI-ICA3 The SCI cannot collect Infrared data at the required times			
See SCI-CF2.1. SCI-CF2.2. SCI-CF2.3.			
SCI-ICA4 The SCI cannot collect Magnetic Field data at the required times			
See SCI-CF2.1. SCI-CF2.2. SCI-CF2.3.			
MOC-ICA1. The MOC sends the directives to the spacecraft later than the expected time.	H1, H2, H3	MOC-2.1, DSN-2.2	
MOC-CF1.1. A higher priority mission (e.g. a crewed mission) requires resources used by the Europa mission, e.g. the DSN.			MOC-SC1, C&DH-SC3
MOC-ICA2 The MOC stops sending commands.	H1, H2, H3, H4, H5, H6,	MOC-2.1	

<p>MOC-CF2.1. The mission may be unexpectedly aborted by an unforeseen disaster. Rationale: There cannot be a safety constraint that will constrain the MOC to continue to operate the mission in the event of a disaster, but there can be safety constraints on other functional elements to address this lack of control.</p>	H7		N/A Risk of Control Flow Accepted
<p>MOC-ICA3 The MOC cannot use the returned data.</p>	H3	A&AC-2.1	
<p>MOC-CF3.1. The C&DH executes a mission plan with orbital correction frequency greater than once per 24 hours. (In order to locate an ocean on the surface, the MOC needs to accurately reconstruct the orbit with Doppler tracking. Accurate Doppler tracking is not possible with thrusting more frequent than once per 24 hours.)</p>			C&DH-SC11, MOC-SC2
<p>MOC-CF3.2. The C&DH does not maintain orbital fidelity to within TBD degrees and the imaging tracks cannot be properly interleaved for mapping.</p>	H3	A&AC-2.1	C&DH-SC11
<p>MOC-CF3.3. The IRC temperature goes above 80 degrees Kelvin.</p>	H1	IRC-2.1	SCI-SC7
<p>MOC-CF3.4. The SCI electronics are irradiated and the data is corrupted.</p>	H1, H3	SCI-2.7	SCI-SC6
<p>MOC-CF3.5. The SCI memory becomes full and the data buffered and transmitted to the MOC.</p>	H1, H2	SCI-2.5	SCI-SC8
<p>DSN-ICA1. The DSN sends directives to the spacecraft later than the expected time.</p>			
<p>See MOC-CF1.1.</p>			

Hazard List and Hazard Log

H1. Inability of Mission to collect data.

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

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

Causal Factors:

S/C-CF1.1. The spacecraft does not make orbit correction maneuvers as often as required. (Around once every 24 hours.)

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.

C&DH-CF2.1. The MOC directives are lost or corrupted in transmission to the C&DH.

COM-CF1.1. The pointing of the spacecraft is not sufficient for transceiving.

A&AC-CF1.1. The C&DH receives an incorrect measurement from the SCI that the current data collection task has finished.

A&AC-CF2.1. The ability of the A&AC to sufficiently maintain pointing is deteriorated due to disturbances from actuator nonlinearities, thermally induced vibrations, instrument mechanisms, etc.

SCI-CF1.1. The ability of the SCI to collect data is undermined due to disturbances from actuator nonlinearities, thermally induced vibrations, instrument mechanisms, etc.

SCI-CF1.2. Radiation causes a single bit upset which corrupts the relevant science data.

SCI-CF1.3. Radiation causes a single bit upset which corrupts the instructions

sent to the **SCI-CF1.4.** The rotation of the Earth starts to occlude the line-of-sight to the spacecraft.

SCI-CF2.1. The A&AC orients the spacecraft such that the pointing of the spacecraft is incorrect for data collection.

SCI-CF2.2. The FLI computer is using the SCI's MTIF for data downlink and the SCI does not collect data unless its MTIF is free.

SCI-CF2.3. The WAC's field of view is obstructed by space debris.

MOC-CF1.1. A higher priority mission (e.g. a crewed mission) requires resources used by the Europa mission, e.g. the DSN.

MOC-CF2.1. The mission may be unexpectedly aborted by an unforeseen disaster.

Rationale: There cannot be a safety constraint that will constrain the MOC to continue to operate the mission in the event of a disaster, but there can be safety constraints on other functional elements to address this lack of control.

MOC-CF3.3. The IRC temperature goes above 80 degrees Kelvin.

MOC-CF3.4. The SCI electronics are irradiated and the data is corrupted.

MOC-CF3.5. The SCI memory becomes full and the data buffered and transmitted to the MOC.

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

Safety Constraints:

C&DH-SC1, C&DH-SC2, C&DH-SC3, C&DH-SC7, C&DH-SC9, SCI-SC1, SCI-SC5, SCI-SC6, SCI-SC7, SCI-SC8, FLI-SC1, SCI-SC11, A&AC-SC1, A&AC-SC2, A&AC-SC4, A&AC-SC5, A&AC-SC6, A&AC-SC7, A&AC-SC8, DSN-SC3, MOC-SC1

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.

System Element: Spacecraft (C&DH, COM, and A&AC), and DSN.

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

Causal Factors:

S/C-CF1.1. The spacecraft does not make orbit correction maneuvers as often as required. (Around once every 24 hours.)

S/C-CF2.1. The SCI collects high-rate data during non-communication periods. (Co-ordination control flaw between SCI and C&DH.)

S/C-CF2.2. The center of mass shifts due science boom flexibility.

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.

C&DH-CF2.1. The MOC directives are lost or corrupted in transmission to the C&DH.

COM-CF1.1. The pointing of the spacecraft is not sufficient for transceiving.

FLI-CF1.1. The SCI has control of the MTIF to the COM.

Rationale: The FLI computer collects health and status data about the spacecraft, and will communicate this to the ground. The inability to communicate after detection of a spacecraft safety-critical fault is detected would be catastrophic.

MOC-CF1.1. A higher priority mission (e.g. a crewed mission) requires resources used by the Europa mission, e.g. the DSN.

MOC-CF2.1. The mission may be unexpectedly aborted by an unforeseen disaster.

Rationale: There cannot be a safety constraint that will constrain the MOC to continue to operate the mission in the event of a disaster, but there can be safety constraints on other functional elements to address this lack of control.

Level and Effect: Potential loss of collected data (↑ACC5)

Safety Constraints:

C&DH-SC1, C&DH-SC2, , C&DH-SC3, C&DH-SC7, C&DH-SC9, SCI-SC10, C&DH-SC12, SCI-SC1, SCI-SC8, , FLI-SC1, A&AC-SC1, A&AC-SC5, MOC-SC1

Analyses Performed:

Actions Taken:

Status:

Verification:

Final Disposal (Closeout Status):

Responsible Engineer:

Remarks:

H3. Inability of mission scientific investigators to use returned data.

System Element: Mission Operations Center

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

Causal Factors:

A&AC-CF1.1. The C&DH receives an incorrect measurement from the SCI that the current data collection task has finished.

A&AC-CF2.1. The ability of the A&AC to sufficiently maintain pointing is deteriorated due to disturbances from actuator nonlinearities, thermally induced vibrations, instrument mechanisms, etc.

MOC-CF1.1. A higher priority mission (e.g. a crewed mission) requires resources used by the Europa mission, e.g. the DSN.

MOC-CF2.1. The mission may be unexpectedly aborted by an unforeseen disaster.

Rationale: There cannot be a safety constraint that will constrain the MOC to continue to operate the mission in the event of a disaster, but there can be safety constraints on other functional elements to address this lack of control.

MOC-CF3.1. The C&DH executes a mission plan with orbital correction frequency greater than once per 24 hours. (In order to locate an ocean on the surface, the MOC needs to accurately reconstruct the orbit with Doppler tracking. Accurate Doppler tracking is not possible with thrusting more frequent than once per 24 hours.)

MOC-CF3.2. The C&DH does not maintain orbital fidelity to within TBD degrees and the imaging tracks cannot be properly interleaved for mapping.

MOC-CF3.4. The SCI electronics are irradiated and the data is corrupted.

Level and Effect: Potential loss of returned data and failure to establish scientific return from the mission. (↑ACC5)

Safety Constraints:

C&DH-SC3, C&DH-SC11, SCI-SC6, SCI-SC11, A&AC-SC4, A&AC-SC5,
A&AC-SC6, A&AC-SC7, A&AC-SC8, MOC-SC1, MOC-SC2

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

H4. Contamination of Outer Planet Moon with biological agents of Earth origin on mission hardware.

System Element: Spacecraft (C&DH, EP, and A&AC)
Operation/Phase: Post-Launch/Pre-Icy Moon Orbit, Icy Moon Orbit, Disposal
Causal Factors:

S/C-CF1.1. The spacecraft does not make orbit correction maneuvers as often as required. (Around once every 24 hours.)

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.

C&DH-CF2.1. The MOC directives are lost or corrupted in transmission to the C&DH.

MOC-CF2.1. The mission may be unexpectedly aborted by an unforeseen disaster.

Rationale: There cannot be a safety constraint that will constrain the MOC to continue to operate the mission in the event of a disaster, but there can be safety constraints on other functional elements to address this lack of control.

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) or to fail to collect and/or use the data corresponding to its mission goals because of the moon's contamination. (↑ACC7)

Safety Constraints:
C&DH-SC1, C&DH-SC9

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.

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:

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.

C&DH-CF2.1. The MOC directives are lost or corrupted in transmission to the C&DH.

MOC-CF2.1. The mission may be unexpectedly aborted by an unforeseen disaster.

Rationale: There cannot be a safety constraint that will constrain the MOC to continue to operate the mission in the event of a disaster, but there can be safety constraints on other functional elements to address this lack of control.

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:

C&DH-SC1

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.

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

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

Causal Factors:

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.

C&DH-CF2.1. The MOC directives are lost or corrupted in transmission to the C&DH.

MOC-CF2.1. The mission may be unexpectedly aborted by an unforeseen disaster.

Rationale: There cannot be a safety constraint that will constrain the MOC to continue to operate the mission in the event of a disaster, but there can be safety constraints on other functional elements to address this lack of control.

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:

C&DH-SC1

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:

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.

C&DH-CF2.1. The MOC directives are lost or corrupted in transmission to the C&DH.

MOC-CF2.1. The mission may be unexpectedly aborted by an unforeseen disaster.

Rationale: There cannot be a safety constraint that will constrain the MOC to continue to operate the mission in the event of a disaster, but there can be safety constraints on other functional elements to address this lack of control.

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:
C&DH-SC1

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, and must collect data at the required times. (←H1) (→S/C-SC1)

SC2. The mission must return data at the required times. (This constraint can conflict with SC9). (←H2) (→S/C-SC2)

SC3. Mission scientific investigators must be able to use the data from the mission at the required times. (←H3)

SC4. All physical elements of the mission must not unintentionally move along a collision course with an outer planet moon. (←H4) (→S/C-SC3)

SC5. All physical elements of the mission that intentionally collide with an outer planet moon must be sterile. (←H4) (→S/C-SC4)

SC6. All physical elements of the mission must not unintentionally move along a collision course with Earth. (←H5, H7) (→S/C-SC5)

SC7. All physical elements of the mission that intentionally collide with the Earth must not cause damage to humans or human assets. (←H5, H7) (→S/C-SC6)

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) (→S/C-SC7)

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 can conflict with SC2. Resolution: SC9 does not apply with space asset governors determine that this mission is higher priority than competing mission). (←H7)

High-Level Requirements

HLR1. The mission shall monochromatically image TBD% of the surface of the icy moon of the outer planet at a TBD-m/pixel scale. (←G2, G4), (→S/C-G1)

Rationale: Visual data of this resolution is necessary for characterization of icy crust and identification of candidate sites for exploration.

HLR2. The mission shall perform multispectral global mapping of the icy moon of the outer planet with a minimum of 3 colors, including IR, at better than TBD-m/pixel scale. (←G1, G2, G3, G4, G6), (→S/C-G1)

Rationale: The radiation emitted by a mass is a function of its temperature and thermal properties. Imaging in IR will provide insights into the physical composition of the icy moon's surface and the location of heat sources that would not be apparent using just the visual spectrum. Imaging in the remaining 2 spectrums will provide evidence of the chemical composition of the surface.

HLR3. The mission shall perform topographic mapping of a representative TBD percentage of the surface of the icy moon of the outer planet at better than 10-m/pixel scale and better than or equal to 1-m/vertical accuracy. (←G2, G4), (→S/C-G1)

Rationale: This level of horizontal and vertical accuracy is necessary create topographic maps of the icy moon that will be critical for future surface-landing missions.

HLR4. The mission shall identify dielectric or physical interfaces related to the current or recent presence or water or brine diapiers by probing the upper TBD km of the icy surface with spatial resolution on the order of 1km and depth resolution of TBD% of the probing depth and uniform global spatial sampling. (←G1, G2), (→S/C-G1)

Rationale: Measurements of this kind is necessary for confirming the presence of a subsurface ocean.

HLR5. The mission shall determine the global gravity field of Europa to identify regions of density contrast within the ice crust by taking horizontal scales of order 100 km. (←G1, G5), (→S/C-G1)

Rationale: These measurements are necessary to characterize the icy moon's gravity field. These measurements are also critical for establishing efficient orbits for current and future missions.

HLR6. 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)

Rationale: These measurements are necessary to characterize the magnetic field of the icy moon of the outer planet. An understanding of the icy moon's magnetic field provides insights in the physical composition of the moon and the existence of an ocean.

HLR7. The mission shall measure high and low energy ions in the ambient magnetosphere to characterize the radiation environment of the space surrounding the icy moon of the outer planet (altitude TBD to altitude TBD). (←G5), (→S/C-G1)

Rationale: These measurements are necessary to characterize the radiation environment of the icy moon of the outer planet. An understanding of the icy moon's radiation

environment is a critical unknown in to mission life and will be critical data for future exploration mission. Furthermore, the radiation activity on the icy moon could provide one of the critical ingredients for life.

Functional Elements and Components:

1. Spacecraft (S/C) (→S/C-G1)

S/C1. Spacecraft Command and Data Handling (C&DH) functional element (→C&DH-G1)

Functions Performed: Health & Status Data Collection for spacecraft; Management of Flight and Science Collection; Evaluation of Flight and Science computation health; Interface management between spacecraft functional elements; Generation of baseline mission plans, storage and execution; Process and Management of MOC directives, Spacecraft MOC Directive Storage and Execution.

S/C2. Flight Data Collection (FLI) functional element (→FLI-G1) (→C&DH-R4)

Functions Performed: Data Packetization, Control of Engineering Mass Memory, and Control of FLI MSAP telecom interface (MTIF).

S/C3. Science Data Collection (SCI) functional element (→SCI-G1) (→C&DH-R2)

Functions Performed: Science Data Collection; Control of the WAC, IR and Magnetometer instruments; Science Data compression; Flight telemetry integration; Data Packetization; Control of Science Mass Memory; Control of SCI MSAP telecom interface (MTIF).

SCI1. Wide Angle Camera (WAC) Controller (→WAC-G1) (→SCI-DC1)

Functions Performed: Management of operation and sensor

SCI2. Infrared Mapping Spectrometer Camera (IRC) Controller (→IRC-G1) (→SCI-DC2)

Functions Performed: Management of operation and sensor

SCI3. Magnetometer Controller (→MAG-G1) (→SCI-DC3)

Functions Performed: Management of operation and transducer

S/C4. Attitude and Translation Control (A&AC) functional element (→A&AC-G1) (→C&DH-R6)

Functions Performed: Spacecraft Pointing, Spacecraft Translation, Directive Receptions, Storage,

S/C5. Communications Signal Processing (COM) functional element (→COM-G1) (→C&DH-R8)

Functions Performed: Spacecraft Data Modulation, Spacecraft MOC Directive Demodulation, RF Transmission/Reception of Data

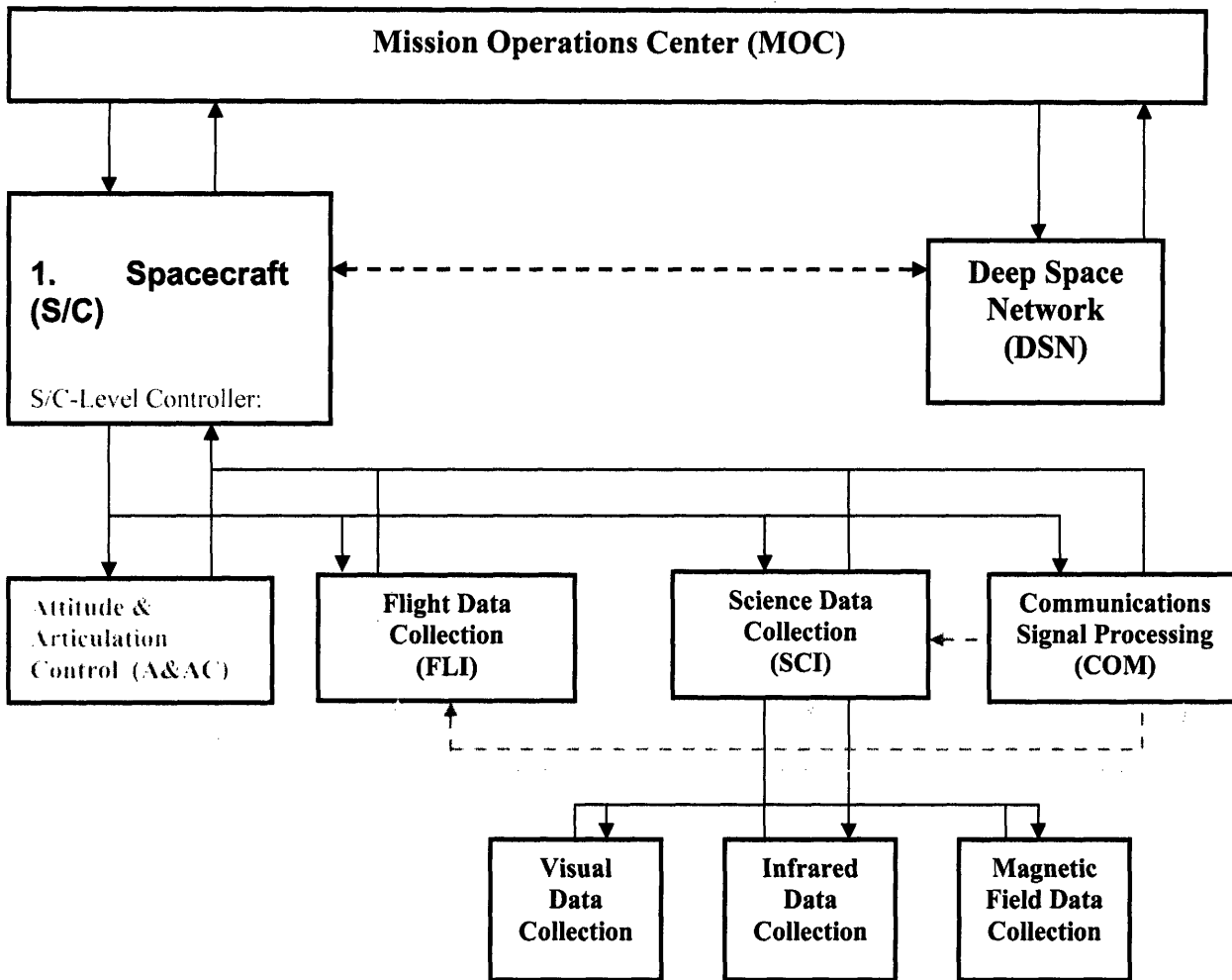
2. Deep Space Network (DSN) (→DSN-G1) (→S/C-R6)



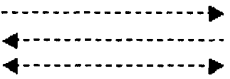
Functions Performed: Transmission of data between the Mission Operations Center and the spacecraft.

3. Mission Operations Center (MOC) (→MOC-G1) (→S/C-R5)
 Functions Performed: Mission planning and operation

System Control Structure:

CS-Diagram1. (→C&DH-DC1), (↓C&DH-2.2.1, FLI-2.4, SCI-2.9)



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
<div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 0 auto;"> <p style="text-align: center;">Functional Element Name</p> <p style="text-align: center;">Functional Element-Level Controller (if applicable)</p> </div>	Functional Element with the controller of its internal interactions (i.e., the functional element-level interactions)

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 HLR7 and collect other data as scientific opportunities arise and transmit that data to the MOC. (←HLR1, HLR2, HLR3, HLR4, HLR5, HLR6, HLR7), (→S/C-R1, S/C-R2, S/C-R3, S/C-R4, S/C-R5, S/C-R6) (→C&DH-G1, C&DH-G2, C&DH-G3, C&DH-G4, C&DH-G5, A&AC-G1, A&AC-G1, A&AC-G3, COM-G1)

Spacecraft (S/C) Requirements

S/C-R1. After deployment from the launch vehicle, the spacecraft shall enter an initial orbit around Europa for approximately TBD days. (←S/C-G1) (↓S/C-2.3, S/C-2.4, S/C-2.5, S/C-2.6)

Rationale: The initial orbit is intended to collect data on 1) The health and status of the spacecraft itself and 2) The gravity field around Europa prior to science orbit insertion. The gravity field data from the initial orbit will be used to determine the optimal science orbit.

S/C-R2. After completion of diagnostics and gravity field measurements the spacecraft must enter a science orbit maintained to TBD degrees for a period of 90 days. (←S/C-G1) (↓S/C-2.2, S/C-2.5, S/C-2.6)

Rationale: It's expected that the mission will require 90 days to collect the required data. The mission could, but is not required, to enter into an extended mission phase after 90 days.

S/C-R3. The spacecraft shall collect the data specified in HLR1 through HLR7 for 90 days. (←S/C-G1)(↓S/C-2.1, S/C-2.4, S/C-2.5, S/C-2.6, S/C-2.7)

S/C-R4. The spacecraft shall communicate with the MOC during non-occultation periods. (←S/C-G1, S/C-2.7)

S/C-R5. The spacecraft shall execute MOC directives. (←S/C-G1) (↓S/C-R5, S/C-2.6)
Rationale: The spacecraft is not expected to fulfill science mission objectives autonomously.

S/C-R6. The spacecraft shall packetize and transceive data to and from the MOC via the DSN, meeting DSM communication requirements. (←S/C-G1) (↓S/C-2.4, S/C-2.5, S/C-2.7)

Spacecraft (S/C) Safety Constraints

S/C-SC1. The spacecraft must have the necessary functionality for data acquisition at the required times, and must collect data at the required times. (←SC1) (↓S/C-2.1, S/C-2.2, S/C-2.4, S/C-2.5, S/C-2.6)

S/C-SC2. The spacecraft must return data at the required times. (←SC2) (↓S/C-2.1, S/C-2.7)

S/C-SC3. All physical elements of the spacecraft must not unintentionally move along a collision course with an outer planet moon. (←SC4) (↓S/C-2.1, S/C-2.6)

S/C-SC4. All physical elements of the spacecraft that intentionally collide with an outer planet moon must be sterile. (←SC5) (↓S/C-2.1, S/C-2.6)

S/C-SC5. All physical elements of the spacecraft must not unintentionally move along a collision course with Earth. (←SC6) (↓S/C-2.1, S/C-2.6)

S/C-SC6. All physical elements of the spacecraft that intentionally collide with the Earth must not cause damage to humans or human assets. (←SC7) (↓S/C-2.1, S/C-2.6)

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). (←SC8) (↓S/C-2.1, S/C-2.6)

S/C-SC8. Given the current radiation model, the availability of radiation hard memory and electronics, and a desire to minimize shielding mass, the spacecraft must have a radiation design factor of 2. (←EA.2) (→SCI-SC6)

Rationale: A radiation design factor of 2 means that the spacecraft parts must be able to withstand radiation of twice that predicted by the radiation model for the mission duration.

S/C-SC9. For proper operation of the science instruments, the spacecraft must maintain a low and circular science orbit within TBD degrees. (↑SCI-DC.1.1, SCI-DC.2.2, SCI-DC.3) (↓S/C-2.2, S/C-2.6)

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 manage the interactions between the lower level functional elements that the C&DH controls (Flight Data Collection, Science Data Collection, Communications Signal Processing, and Attitude and Translation Control) so that spacecraft goals are met. (←S/C-G1) (→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) (→C&DH-SC1)

C&DH-G2. To transmit the data required to fulfill spacecraft goals and ensure that the MOC has spacecraft health and status state information that is no older than TBD seconds during communication times. (←S/C-G1) (→C&DH-R1, C&DH-R8, C&DH-R9)

C&DH-G3. To prioritize, schedule, and execute MOC directives so that spacecraft goals are met. (←S/C-G1) (→C&DH-R1, C&DH-R2, C&DH-R4, C&DH-R6, C&DH-R8) (→C&DH-SC1.2)

Rationale: There is a significant time delay between Earth and Europa and some on-board execution scheduling ability will allow the mission to take advantage of scientific opportunities.

C&DH-G4. To maintain basic spacecraft operations when MOC directives are unavailable so that spacecraft goals are met (as much as possible). (←S/C-G1) (→C&DH-R1) (→C&DH-SC1.1, C&DH-SC2)

C&DH-G5. To revise missions plans as required to meet spacecraft goals given MOC directives and real-time spacecraft health and science data. (←S/C-G1) (→C&DH-R1) (→C&DH-SC1.1, C&DH-SC1.3, C&DH-SC3)

Rationale: While the C&DH is not expected to achieve all goals autonomously; an on-board mission planner and executor as part of the C&DH is necessary. This will allow the automation of routine functions, reduce the number of commands sent from the MOC which can be corrupted, and enable the spacecraft to respond to faults and arising science opportunities. Removing the long time delay in responding to health and status issues is crucial as the proper safe mode transition behavior must be initiated within milliseconds.

Spacecraft Command & Data Handling (C&DH) Requirements

C&DH-R1. The C&DH shall create and revise mission plans in accordance with Spacecraft health, Science data collection needs and MOC directives. (←C&DH-G1, C&DH-G2, C&DH-G3, C&DH-G4)

C&DH-R2. The C&DH shall issue science data collection, storage and transmission related directives to the SCI in accordance with the mission plan. (←C&DH-G1, C&DH-G3) (↓C&DH-2.1.5)

C&DH-R3. The C&DH shall monitor feedback measurements from the SCI and revise its mission plan accordingly. (←C&DH-G1) (↓C&DH-2.1.5)

Rationale: The C&DH must know the health and status of the spacecraft.

C&DH-R4. The C&DH shall issue flight data collection, storage and transmission related directives to the FLI in accordance with the mission plan. (←C&DH-G1, C&DH-G3) (↓C&DH-2.1.4) (→FLI-G1)

C&DH-R5. The C&DH shall monitor feedback measurements from the FLI and revise its mission plan accordingly. (←C&DH-G1) (↓C&DH-2.1.4)

Rationale: The C&DH must know the health and status of the spacecraft.

C&DH-R6. The C&DH shall issue attitude and translation directives to the A&AC in accordance with the mission plan. (←C&DH-G1, C&DH-G3) (↓C&DH-2.1.3)

C&DH-R7. The C&DH shall monitor feedback measurements from the A&AC and revise its mission plan accordingly. (←C&DH-G1) (↓C&DH-2.1.3)

Rationale: The C&DH must know the health and status of the spacecraft.

C&DH-R8. The C&DH shall issue data transceive directives to the COM in accordance with the mission plan. (←C&DH-G1, C&DH-G2, C&DH-G3) (↓C&DH-2.2)

C&DH-R9. C&DH-R9. The C&DH shall monitor feedback measurements from the COM and revise its mission plan accordingly. (←C&DH-G1, C&DH-G2) (↓C&DH-2.2)

Rationale: The C&DH must know the health and status of the spacecraft.

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

C&DH-DC1. The C&DH must be able to receive and process directives from the MOC. (←SC1) (↓C&DH-2.1, C&DH-2.2.1)

C&DH-DC2. Due to the low availability of radiation hard memory, no data will be re-transmitted. (←EA.2) (↓C&DH-2.2.1)

Rationale: A new data collection and transmission can be initiated on request but data will not be stored onboard the spacecraft. High rate data will be taken during communication periods and immediately processed and transmitted to earth.

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

C&DH-SC1. The C&DH must have the capability to reason about the state of the spacecraft and plan the execution of MOC directives so that the initial conditions of a directive are valid.

(←C&DH-CF1.1) (←S/C-SC1) (←C&DH-G1) (→FLI-SC2, FLI-SC3, SCI-2, SCI-3)
(↓C&DH-2.1.1) (→A&AC-SC2)

C&DH-SC1.1. The C&DH mission planner and executor must be able to generate plans that re-orient the spacecraft within TBD seconds so that spacecraft initial conditions are compatible with MOC directives. (←C&DH-G4, C&DH-G5) (↓C&DH-2.1.1) (→A&AC-SC1)

Rationale: During the time delay between flight data status downlink and receipt of MOC directives, the MOC directives may not be compatible with current mission state. In this case new directives can be sent, or the onboard mission planner and executor (part of the C&DH) can generate a plan to make spacecraft state compatible with the initial conditions specified by the MOC directives within TBD seconds.

C&DH-SC1.2. The C&DH must ask for a new set of directives if the current state of the spacecraft is incompatible and the onboard mission planner and executor (part of the C&DH) cannot find a new plan and execute it so that the current state is compatible with the directives within TBD seconds. (←S/C-SC1) (←C&DH-G3) (↓C&DH-2.1.1.2)

Rationale: For example if the spacecraft is damaged or low on power such that a requested re-orientation is not possible, then a request for new directives would be appropriate. This situation could arise if the spacecraft is damaged in the time delay between the MOC receipt of health and status from the spacecraft and receipt of the new set up directives by the C&DH.

C&DH-SC1.3. The C&DH must have the ability to initiate communications with the MOC and request directives and/or updates. (←S/C-SC1) (←C&DH-G5) (↓C&DH-2.1.1.2)

Rationale: Directives sent from the MOC could be lost or corrupted before reaching the spacecraft and would require a retransmission request from the C&DH. Unscheduled communication with the MOC should also be initiated if off-nominal spacecraft health has been detected, or if the C&DH has aborted the current set of MOC directives due to a high priority science opportunity.

C&DH-SC2. The C&DH must have the capability to generate mission plans without directives from the MOC to allow orbital maintenance and low-rate science and flight data collection. (←C&DH-CF2.1.) (←S/C-SC1) (↓C&DH-2.1.1.3)

Rationale: The spacecraft is not expected to perform the mission autonomously, but it is expected to continue to maintain orbit and take low-rate science data that can be stored on the science memory mass.

C&DH-SC3. The C&DH must be capable of creating and scheduling a mission plan within TBD ms if a predetermined SCI event occurs. (←MOC-CF1.1.) (←S/C-SC1) (→SCI-2, SCI-3)
(↓C&DH-2.1.1)

Rationale: The MOC will include scientifically interesting, prioritized events that will require onboard scheduling and minor mission planning to ensure time-critical science opportunities are not missed.

C&DH-SC4. After TBD days, if attempts to communicate with the MOC have failed and power is below TBD, the spacecraft must enter a destructive orbit. (→A&AC-SC1) (↓ C&DH-2.4) (←S/C-SC1) (↓C&DH-2.1.1.4) (→A&AC-SC3)

Rationale: The mission must not accidentally contaminate the icy moon by falling into a haphazard degenerative, uncontrolled trajectory.

C&DH-SC5. During data collection and Earth-communication times, the C&DH must execute directives to the A&AC that provide sufficient capability to both functions. (←A&AC-CF1.1.) (←S/C-SC1) (↓C&DH-2.1.3) (→A&AC-SC1)

Rationale: The HGA and the science instruments both have strict pointing requirements and the A&AC must fulfill those as well as fulfilling its orbital requirements.

C&DH-SC6. The C&DH must not command the A&AC to move while data collection is ongoing unless the C&DH wishes to abort the current data collection. (←A&AC-CF1.1.) (↓C&DH-2.5) (←MOC-CF3.4) (←S/C-SC1) (↓C&DH-2.1.3) (→A&AC-SC7)

Rationale: The C&DH is responsible for coordination of the spacecraft's data collection and articulation and transition needs.

C&DH-SC7. The C&DH must abort SCI control of the MTIF if the FLI has higher priority health data to communicate. (←FLI-CF1.1.) (←SCI-CF2.2) (←MOC-CF3.3) (←S/C-SC1) (→SCI-SC1) (↓C&DH-2.2) (↓FLI-SC1)

Rationale: The current design of the FLI and SCI requires the use of a shared MTIF. To reduce coupling the higher level controller must manage use of this shared resource.

C&DH-SC8. The C&DH must have enough memory to store flight and science data while in non-communication periods. (←EA.2, EA.5) (←C&DH-DC2) (←DC.1.1)(→SCI-SC1) (←MOC-CF3.5) (←S/C-SC1)

Rationale: Communication with Earth is not possible during occultation periods, and it is expected that the mission control will require flight and other low-rate science data taken during occultation periods.

C&DH-SC9. The C&DH must command the A&AC to perform orbital correction maneuvers to maintain the science orbit to within TBD degrees. (This constraint can conflict with C&DH-SC11). (↑S/C-SC9) (↑S/C-CF1.1.) (←S/C-SC1) (↓C&DH-2.1.3) (→A&AC-SC8)

Rationale: Low, circular, near polar orbits left uncontrolled will degrade and impact the surface of the moon within tens of days.

C&DH-SC10. The C&DH software must be impervious to single event upsets. (↓C&DH-2.5) (←S/C-SC1) (→SCI-SC5) (↓C&DH-2.2.2)

C&DH-SC11. The C&DH must not perform orbital correction maneuvers with thrusters more than once per 24 hours.(→MOC-SC2)(↓C&DH-2.4) (←MOC-CF3.1) (←MOC-CF3.2) (←S/C-SC1) (↓C&DH-2.1.3)

Rationale: Use of the thrusters greater than one time per 24 hours will degrade the ability of the SCI to collect data. (This constraint can conflict with C&DH-SC9).

C&DH-SC12. The C&DH must not command SCI to collect data during non-communication periods. (←S/C-CF1.1.) (↓SCI-2.6) (←S/C-SC1)

Level 1.1.1.1: Flight Data Collection (FLI) Goals, Requirements, and Constraints

Flight Data Collection (FLI) Goals

FLI-G1 To collect spacecraft health and status data. (←C&DH-R4)

Flight Data Collection (FLI) Requirements

FLI-R1. Flight data collection will be performed every TBD sec for flight critical instruments. (←C&DH-SC1, C&DH-SC3) (↓C&DH-2.2.1) (↓S/C-2.4) (↓FLI-2.1)

FLI-R2. The flight data must be packetized and compressed for transmission to the MOC. (←FLI-G1) (↓C&DH-2.2.1) (↓FLI-2.2)

FLI-R3. The FLI must execute directives from the C&DH to initiate and regulate data collection. (←C&DH-R4, C&DH-R5) (↓C&DH-2.2.1)

Flight Data Collection (FLI) Design Constraints

FLI-DC1. The FLI must be able to receive and process directives from the C&DH. (←C&DH-R4, C&DH-R5) (↓C&DH-2.2.1)

Flight Data Collection (FLI) Safety Constraints

FLI-SC1. The FLI must relinquish control of the SCI MTIF within TBD ms when commanded to do so by the C&DH. (←FLI-CF1.1.) (←SCI-CF2.2) (←C&DH-SC7) (↓FLI-2.2.1, FLI-2.3))

FLI-SC2. The FLI must send health and status updates to the C&DH every TBD seconds. (←C&DH-SC1) (↓C&DH-2.2.1) (↓FLI-2.4)

FLI-SC3. The FLI must send health and status interrupt if a safety critical measurement was received within TBD ms. (←C&DH-SC1) (↓C&DH-2.2.1) (↓FLI-2.4)

Level 1.1.1.2: Science Data Collection (SCI) Goals, Requirements, and Constraints

Science Data Collection (SCI) Goals

SCI-G1. To collect the science data specified in HLR 1 through HLR7 and collect other data as scientific opportunities arise. (←HLR1, HLR2, HLR3, HLR4, HLR5, HLR6, HLR7), (→S/C-R1, S/C-R2) (←C&DH-R2, C&DH-R3)

Science Data Collection (SCI) Assumptions

SCI-A1. The data required to fulfill HLR1 through HLR7 will amount to approximately TBD Gbits of science data acquired per Earth-day.

Science Data Collection (SCI) Requirements

SCI-R1. The science data collection functional element will collect monochromatic images of the surface. (←SCI-G1) (↓C&DH-2.2.1) (↓SC-2.1)

SCI-R2. The science data collection functional element will collect infrared images of the surface. (←SCI-G1) (↓C&DH-2.2.1) (↓SC-2.1)

SCI-R3. The science data collection functional element will collect data to characterize the magnetic field from the surface. (←SCI-G1) (↓C&DH-2.2.1) (↓SC-2.1)

SCI-R4. The high-rate science data must be compressed and packetized before transmission to the MOC. (←C&DH-DC2) (↓C&DH-2.2.1) (↓SC-2.1)

SCI-R5. Low-rate science data must be packetized and stored on the science memory until sent to the MOC. (←C&DH-DC2) (↓C&DH-2.2.1) (↓SC-2.1)

SCI-R6. The SCI must execute directives from the C&DH to initiate and regulate data collection. (←C&DH-R3) (↓C&DH-2.2.1) (↓SC-2.1)

Science Data Collection (SCI) Design Constraints

SCI-DC1. A wide angle camera (WAC) will be used to collect data in the visual range. (↓SCI-2.10)

SCI-DC2. An infrared camera (IRC) will be used to collect data in the infrared range. (↓SCI-2.11)

SCI-DC3. A Magnetometer (MAG) will be used to collect European magnetosphere data. (↓SCI-2.12)

SCI-DC4. The SCI must be able to receive and process directives from the C&DH. (←C&DH-R2, C&DH-R3)

SCI-DC5. COM bandwidth is limited to TBD kbps so packetized flight telemetry and science data must not exceed TBD kbps.

Science Data Collection (SCI) Safety Constraints

SCI-SC1. The SCI must relinquish control of the MTIF within TBD ms when commanded to do so by the C&DH. (←FLI-CF1.1.) (←SCI-CF2.2) (←C&DH-SC3, C&DH-SC6, C&DH-SC7, C&DH-SC8)

SCI-SC2. The SCI must send health and status updates to the C&DH every TBD seconds. (←C&DH-SC1, C&DH-SC3) (↓SCI-2.3, SCI-2.4)

SCI-SC3. The SCI must send health and status update if a safety critical measurement was received within TBD ms. (←C&DH-SC1, C&DH-SC3) (↓SCI-2.3, SCI-2.4)

SCI-SC4. The SCI must be able to compress high-rate data instruments in hardware. (←C&DH-DC2)

Rationale: The science mass memory is not large enough for compression in software.

SCI-SC5. The SCI software must be impervious to single event upsets. (↓SCI-2.2) (←SCI-CF1.2.) (←SCI-CF1.3.) (←C&DH-SC10) (↓SCI-2.7, SCI-2.8)

SCI-SC6. The SCI instruments must be protected from radiation so that electronics are not exposed to TBD rads over the course of the mission as predicted using the radiation model. (↓SCI-2.4) (←MOC-CF3.4.) (←S/C-SC8) (↑EA2) (→WAC-SC3, IRC-SC3, MAG-SC3)

Rationale: This safety constraint conflicts with the need to conserve mass. Every gram allocated to shielding is a gram that could have been used for greater spacecraft functionality.

SCI-SC7. The SCI must maintain the temperature of the IRC to below 80 degrees Kelvin for proper operation. (↓IRC-2.1) (←MOC-CF3.3.) (↓SCI-2.6.1) (→IRC-SC4)

SCI-SC8. The SCI must compress the data enough so that the science mass memory can be used as a buffer transmission to the MOC. (↓SCI-2.5) (←MOC-CF3.5.)

SCI-SC9. The SCI must not compress the data so much that it is unusable to fulfill science goals. (↓SCI-2.5)

SCI-SC10. The SCI must not collect any high-rate data during non-communication periods. (←S/C-CF1.1.)

Rationale: High-rate data collected during non-communication periods would quickly fill up the science mass memory, and consequently be overwritten and lost. The science

mass memory is intended to act as a high-rate data buffer before transmission to the MOC.

SCI-SC11. The SCI must not send 'Data Collection Successful' message until receipt of a 'Data Collection Successful' message from all instruments taking data at a fixed point. (←A&AC-CF1.1.)

Level 1.1.1.2.1: Wide Angle Camera Data Collection (WAC) Goals, Requirements, and Constraints

Wide Angle Camera Data Collection (WAC) Goals

WAC-G1. To collect monochromatic images of TBD% of the European surface at a TBD-m/pixel scale. (→SCI-R1)

Wide Angle Camera Data Collection (WAC) Assumptions

WAC-A1. The wide angle camera is a high-rate scientific instrument and its data must be compressed. (←SCI-DC1)

WAC-A2. The wide angle camera is a high-rate scientific instrument and its data must be both collected and transmitted to the MOC during communication periods. (←SCI-R4)

Wide Angle Camera Data Collection (WAC) Requirements

WAC-R1. The WAC must execute directives from the SCI to initiate and regulate data collection. (←WAC-G1) (↓SCI-2.9, SCI-2.10) (↓WAC-2.1)

Wide Angle Camera Data Collection (WAC) Design Constraints

WAC-DC1. The WAC must be able to receive process directives from the SCI. (↓SCI-2.9)

WAC-DC2. The WAC requires TBD lux of illumination. (↓WAC-2.1)

Wide Angle Camera Data Collection (WAC) Safety Constraints

WAC-SC1. The WAC must have the necessary functionality for data acquisition at the required times. (←WAC-R1)

WAC-SC2. The WAC must be able to send data to the SCI at the required times. (←WAC-R1)

WAC-SC3. The WAC sensor must withstand a TBD dose of radiation per day. (↑EA2) (←SCI-SC6)

WAC-SC4. WAC data must be written to the internal frame buffer from the CCD sensor within 2 seconds. (↑EA2)

Rationale: Data on the CCD is susceptible to radiation noise which can corrupt the image.

WAC-SC5. For proper WAC operation the WAC pointing must be accurate within TBD mrad and must have TBD mrad stability over TBD seconds. (←A&AC-SC8) (←C&DH-SC9)

WAC-SC6. The WAC requires a near circular orbit between 100 and 500 km for mapping the European surface. (↑S/C-SC9) (←C&DH-SC9)

Rationale: The ability to use WAC data is dependent on orbit fidelity. The WAC data swaths must be interleaved for map creation.

Level 1.1.1.2.2: IR Data Collection (IRC) Goals, Requirements, and Constraints

IR Camera Data Collection (IRC) Goals

IRC-G1. To collect infrared images of the European surface at better than TBD-m/pixel scale infrared images of the European surface from TBD degrees latitude to TBD degrees latitude. (→IRC-G1) (→IRC-R1)

IR Camera Data Collection (IRC) Assumptions

IRC-A1. IR data is collected by a high-rate scientific instrument and its data will need to be compressed. (←SCI-DC2)

IRC-A2. IR data is collected by a high-rate scientific instrument and its data must be both collected and transmitted to the MOC during communication-periods. (←SCI-R4)

IR Camera Data Collection (IRC) Requirements

IRC-R1. The IRC must execute directives from the SCI to initiate and regulate data collection. (←IRC-G1) (↓SCI-2.9, SCI-2.11) (↓IRC-2.1)

IR Camera Data Collection (IRC) Design Constraints

IRC-DC1. The IR must be able to receive and process directives from the SCI. (↓SCI-2.9)

IR Camera Data Collection (IRC) Safety Constraints

IRC-SC1. The IRC must have the necessary functionality for data acquisition at the required times. (←IRC-R1)

IRC-SC2. The IRC must be able to send data to the SCI at the required times. (←IRC-R1)

IRC-SC3. The IRC must withstand a TBD dose of radiation per day. (↑EA2) (←SCI-SC6)

IRC-SC4. The IRC detector must be cooled about 80 degrees Kelvin.(←SCI-SC7) (↓IRC-2.2)

IRC-SC1. For proper IRC operation the IRC pointing must be accurate within TBD mrad and must have TBD mrad stability over TBD seconds.(←A&AC-SC8) (←C&DH-SC9)

Level 1.1.1.2.3: Magnetic Data Collection (MAG) Goals, Requirements, and Constraints

Magnetic Data Collection (MAG) Goals

MAG-G1. To collect infrared images of the European surface at better than TBD-m/pixel scale infrared images of the European surface from TBD degrees latitude to TBD degrees latitude. (→MAG-R1)

Magnetic Data Collection (MAG) Assumptions

MAG-A1. Magnetic field data is collected by a low-rate scientific instrument during both communication and non-communication periods, and its data will need to be compressed in software by the SCI. (←SCI-DC3) (←SCI-R5)

MAG-A2. Magnetic field data is transmitted to the MOC during communication-periods. (←SCI-R5)

Magnetic Data Collection (MAG) Requirements

MAG-R1. The MAG must execute directives from the SCI to initiate and regulate data collection. (←MAG-G1) (↓SCI-2.9) (↓SCI-2.12) (↓MAG-2.1)

Magnetic Data Collection (MAG) Design Constraints

MAG-DC1. The MAG must be able to receive and process directives from the SCI. (↓SCI-2.9)

Magnetic Data Collection (MAG) Safety Constraints

MAG-SC1. The MAG must have the necessary functionality for data acquisition at the required times. (←MAG-R1) (↓MAG-2.1)

MAG-SC2. The MAG must be able to send data to the SCI at the required times. (←MAG-R1) (↓SCI-2.9)

MAG-SC3. The MAG must withstand a TBD dose of radiation per day. (↑EA2) (←SCI-SC6)

Level 1.1.2: Spacecraft Attitude and Articulation Control (A&AC) Goals, Requirements, and Constraints

Spacecraft Attitude and Articulation Control (A&AC) Goals

A&AC-G1. The A&AC must maintain the orbit fidelity to within TBD degrees. (←S/C-R1)
Rationale: For both data science data accuracy and to conserve mission resources, the orbit must be strictly maintained.

A&AC-G2. The A&AC must maintain pointing of the spacecraft to within TBD degrees. (←S/C-R1)
Rationale: Science and communication instruments have strict pointing requirements.

A&AC-G3. The A&AC must follow planned spacecraft trajectories to within TBD. (←S/C-R1)
Rationale: Excess slip from the planned trajectory is inefficient and will waste mission resources.

Spacecraft Attitude and Articulation Control (A&AC) Requirements

A&AC-R1. The A&AC shall provide functionality for following mission trajectories, orbit insertion, orbit maintenance, and vehicle disposal for the mission to and at the outer planet and ice moon. (←A&AC-G1, A&AC-G2, A&AC-G3) (↓S/C-2.6)

A&AC-R2. The A&AC shall provide pointing of the main spacecraft structure to TBD degrees as directed by the C&DH. (←A&AC-G2), (↓A&AC-2.5) (↓A&AC-2.1)
Rationale: The Science Instruments and HGA require pointing of the spacecraft be maintained within specified envelopes for data collection and transceiving.

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

A&AC-DC1. 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) (↓S/C-2.6)

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

A&AC-SC1. The A&AC must have the necessary functionality for performing velocity changes and propulsive actions at the required times. (←COM-CF1.1.) (←SCI-CF2.1) (←C&DH-SC1.1, C&DH-SC5) (↓A&AC-2.2)

A&AC-SC2. The A&AC must be able execute maneuvers at the required times. (←SCI-CF2.1)(←C&DH-SC1)

A&AC-SC3. The A&AC must be able to calculate a self-destruct orbit that will not contaminate Europa. (←C&DH-SC4) (↓A&AC-2.1)

A&AC-SC4. The A&AC must be robust to disturbances from thermally, induced vibrations within a TBD range. (←A&AC-CF2.1.) (←SCI-CF1.1)

A&AC-SC5. The A&AC must be robust to disturbances from instrument mechanisms and science booms within a TBD range. (←S/C-CF2.2) (←A&AC-CF2.1.) (←SCI-CF1.1)

A&AC-SC6. The center of mass accelerations from non-gravitation disturbance forces must be controlled to within TBD m/s^2 . (←WAC-SC5, IRC-SC5) (←A&AC-CF2.1.) (←SCI-CF1.1)

Rationale: This constraint exists because the science instruments require precise pointing.

A&AC-SC7. The A&AC must use reaction wheels to maintain attitude rather than thrusters due to the center of mass instability thruster use would cause. . (←WAC-SC5, IRC-SC5) (C&DH-2.2.1, C&DH→A&AC, A&AC→C&DH). (←A&AC-CF2.1.) (←SCI-CF1.1) (←SCI-CF2.1)

Rationale: This constraint exists because the science instruments require precise pointing.

A&AC-SC8. For proper science instrument operation the A&AC pointing must be must be accurate within TBD mrad and must have TBD mrad stability over TBD seconds. (←WAC-SC5, IRC-SC5) (←A&AC-CF2.1.) (←SCI-CF2.1) (←C&DH-SC6, C&DH-SC9) (↓A&AC-2.2)

Level 1.1.3: Spacecraft Communications Signal Processing (COM) Goals, Requirements, and Constraints

Spacecraft Communications Signal Processing (COM) Goals

COM-G1. To transmit all compressed and packetized flight and science data to Earth. (←S/C-G1)

Spacecraft Communications Signal Processing (COM) Requirements

COM-R1. The COM must execute directives from the C&DH to initiate, transmit and receive data to and from the DSN. (←COM-G1) (↓S/C-2.7) (↓COM-2.1)

COM-R2. The COM functional element will modulate and demodulate data to onto and from signals sent to and from the DSN. (←COM-G1) (↓S/C-2.7) (↓COM-2.2)

Spacecraft Communications Signal Processing (COM) Design Constraints

COM-DC1. The spacecraft cannot transceive data with the DSN for 0.78 hours every European day when the Earth is not visible. (↑EA.5)

Rationale: Earth is occulted for 37% of the European day.

COM-DC2. The spacecraft transceive with the DSN every 3.55 days for 2.1 hours. (↑EA.5)

Rationale: Earth is occulted by Jupiter every 3.55 days.

COM-DC3. The COM functional element must be able to receive packetized H&S data or packetized science data from the FLI's MTIF upon command from the C&DH. (↑C&DH-2.1.2)

COM-DC4. The COM functional element must be able to receive packetized H&S data or packetized science data from the SCI's MTIF upon command from the C&DH. (↑C&DH-2.1.2)

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

Deep Space Network (DSN) Safety Constraints

DSN-SC1. The DSN must not stop receipt of data from the spacecraft before all data has been transceived and the scheduled COM period has been completed, unless the DSN resource must be preempted for another mission. (↓ DSN-2.1)

DSN-SC2. The DSN must adhere to directives from the MOC concerning data transceive with the spacecraft. (↓ DSN-2.1.1)

DSN-SC3. As the Earth turns and the LOS to the spacecraft requires a new antenna site the DSN must be able to pass a job from one antenna site to another without a loss of data. (←SCI-CF1.4)

Level 1.3: 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)

Mission Operations Center (MOC) Safety Constraints

MOC-SC1. The MOC shall not schedule high priority communications with the spacecraft during high priority communication times of higher priority mission. (↓ MOC-2.1) (←MOC-CF1.1)

Assumption: This constraint will only mitigate the inadequate control, and further constraints on the spacecraft exist to deal with this inadequate control action.

MOC-SC2. The MOC must be able to accurately reconstruct the European explorer orbit to within TBD degrees in order to accurately determine the location of an ocean on the icy moon. (MOC-2.3) (←C&DH-SC13) (←MOC-CF3.1)

Level 2: System Design Decisions

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, EA1, EA2), (→2.2, 2.3, 2.4, 2.5, S/C-2.1), (↑MOC-G1)

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. The C&DH receives directives generated by the MOC which it uses in combination with onboard state information from the A&AC, COM, FLI and SCI to generate schedules and mission plans to collect data. (↑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), (←2.1), (↓C&DH-G1)

Rationale: Spacecraft state information is used to ensure that initial conditions specified in the MOC directives are met. If the current spacecraft state does not meet the initial conditions in the MOC directives, the C&DH will create a plan to put the spacecraft into the state required by the MOC. Additionally, the C&DH will use spacecraft state information to generate new mission plans in the case of off-nominal health and status states or to take advantage of science opportunities.

S/C-2.2. The spacecraft's science orbit will be low altitude (between 100 and 500 km), near circular, and near polar (within TBD degrees). (↑S/C-SC1, S/C-SC9) (↑S/C-R2) (↑S/C-CF1.1)

Rationale: The science instruments require a low, circular, polar orbit for surface mapping fidelity.

S/C-2.3. The spacecraft's initial orbit will be at around 500 km elliptical orbit. (↑S/C-R1)

Rationale: The initial orbit is intended to collect data on 1) The health and status of the spacecraft itself and 2) The gravity field around Europa prior to science orbit insertion. The gravity field data from the initial orbit will be used to determine the optimal science orbit.

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, generates a schedule for directive execution and/or delegates them to the appropriate functional elements. (↑C&DH-C1), (←S/C-2.1), (↓C&DH-ICA1, C&DH-ICA2) (↑C&DH-CF1.1, C&DH-CF2.1) (↑C&DH-R1)

C&DH-2.1.1. The C&DH generates new mission plans in the event of off-nominal safety-related states or science opportunities. (↑C&DH-SC1, C&DH-SC3)

Rationale: The C&DH should schedule and execute MOC directives except when the spacecraft has detected an unsafe state or fault mode, (such as high temperature or unresponsive reaction wheels) or a high-priority science opportunity arises (such as the discovery of an unexpectedly hot spot on the European surface).

Many faults can be diagnosed and treated on-board the spacecraft without waiting for a new plan from the MOC. During such a delay, the spacecraft state could further deteriorate and new directives from the MOC could be inappropriate for the evolving state onboard. Generation of new mission plans onboard prevents asynchronous evolution between the MOC and the spacecraft.

Similarly, if the science collection functional elements discover a predefined, high-priority science scenario, the spacecraft should immediately investigate it, rather than proceeding with lower-priority data collection. A hot spot on the European surface may mean the discovery of new life, and waiting for the spacecraft to downlink the data and for relevant new MOC directives could mean an intolerable loss of investigation time or an altogether missed investigation opportunity. (→The scientist's model for predicted infrared readings on the icy surface)

C&DH-2.1.1.1 The C&DH uses a rate-monotonic scheduling algorithm for generating and scheduling mission plans. (↑C&DH-R1)

C&DH-2.1.1.1.1 The C&DH uses prioritized interrupts to replan the mission. (↑C&DH-R1, C&DH-R3) (↑C&DH-SC3)

Rationale: If the SCI functional element detects a magnetic field reading greater than TBD tesla, the spacecraft may need to schedule extended magnetic field data collection and re-orient the spacecraft.

C&DH-2.1.1.2 If the current set of directives from the MOC are incompatible with spacecraft state, and the C&DH is unable to generate a plan to transition the spacecraft state to be compatible with the MOC directives, the C&DH will request new directives from the MOC and downlink current and projected spacecraft state to the MOC. (↑C&DH-SC1.2, C&DH-SC1.3)

C&DH-2.1.1.3 Whenever the spacecraft has finished executing all available MOC directives and no off-nominal health or science events have occurred the spacecraft maintains its orbit and collects low-rate science data. (↑C&DH-SC2)

Rationale: The low-rate science data can be collected for TBD hours before becoming too large to be stored on the science mass memory.

C&DH-2.1.1.4 After TBD days, if attempts to communicate with the MOC have failed and power resources are below TBD, the C&DH will generate a mission plan to send the spacecraft on a self-destruct orbit. (↑C&DH-SC4) (→A&AC-2.1)

C&DH-2.1.2. The C&DH delegates tasks in the MOC directives related directly to the transfer of data between the spacecraft and the MOC (via the DSN) to the COM functional elements. The C&DH will use current spacecraft state (including evaluation of tasks in progress) to determine when these directives should be acted on by the COM functional elements.

C&DH-2.1.3. The C&DH provides attitude and translation directives to and receives feedback from the A&AC functional element in accordance with the mission plan. (↑A&AC-CF2.1) (↑C&DH-R6, C&DH-R7) (↑C&DH-SC5, C&DH-SC6, C&DH-SC11)

Rationale: The mission plan generated by the C&DH uses spacecraft state information (in particular, SCI and COM state information) and MOC directives. (↑C&DH-R6, C&DH-R7, C&DH-C1), (↓A&AC-C2)

C&DH-2.1.4. The C&DH provides directives and receives feedback related to telemetry data collection to the FLI functional element in accordance with the mission plan. (↑FLI-CF1.1) (↑C&DH-R4, C&DH-R5)

Rationale: The mission plan generated by the C&DH uses spacecraft state information (in particular, SCI and FLI state information) and MOC directives.

C&DH-2.1.5. The C&DH provides directives and receives feedback related to science data collection to the SCI functional element in accordance with the mission plan. (↑FLI-CF1.1) (↑C&DH-R2, C&DH-R3)

Rationale: The mission plan generated by the C&DH uses spacecraft state information (in particular, SCI and FLI state information) and MOC directives.

C&DH-2.2. The C&DH software is designed to incorporate state information from lower-level functional elements in mission plan generation. State information comes in the form of prioritized interrupts. Interrupts critical to safety are highest priority. If the C&DH receives an interrupt message it will determine the importance of the interrupt against directives that are currently executing and may generate a new plan and send new directives to the A&AC, SCI, FLI and COM functional elements. (↑SCI-CF2.1) (↑C&DH-R8) (↑C&DH-SC7)

C&DH-2.2.1. The C&DH receives state information and sends directives to the spacecraft subsystems and the MOC. The C&DH does not consider any delegated task complete until either a status message is returned from a lower level functional element and/or it reads a measurement proving that the task was completed. (↑A&AC-CF1.1)

See (↑CS-Diagram1) for functional elements and components connected to the C&DH.

C&DH → MOC

New Directives Request: Feedback to the MOC asking for new directives.

Mission Update: Notifies the MOC of new mission plan and includes current and projected spacecraft state.

MOC → C&DH

Directives: Set of directives from the MOC.

C&DH → A&AC

Orbital Adjustment: Command to adjust the spacecraft's trajectory using thrusters. Command is sent as necessary at periods greater than 24 hours. (↑C&DH-SC11)

Reaction Wheel Desaturation: Reaction wheels are used to maintain pointing of the spacecraft from DSN communications and science data collection. They must be desaturated every TBD hours.

A&AC → C&DH:

Reaction Wheel Measurement: Current state of reaction wheel saturation and position.

Spacecraft Attitude Measurement: Current state of spacecraft attitude.

Spacecraft Trajectory Measurement: Current state of spacecraft trajectory.

Trajectory Adjustment Status: Measurement notifying the C&DH when the next orbital adjustment will be required to maintain desired orbit.

Off-nominal Attitude or Trajectory: Measurement to C&DH that the A&AC has detected an off-nominal attitude or trajectory state.

C&DH → COM:

Start SCICom: Directive to the COM functional element to start data transmission from the science mass memory. This is the typical command sent to the COM because the science mass memory is the primary drive for data retrieval by the COM.

Start FLIComm: Directive to the COM functional element to start data transmission from the engineering mass memory. This command is sent to the COM when the science mass memory is unavailable.

Start SCIComm: Directive to the COM functional element to start data transmission.

Abort Com: Directive to the COM functional element to end data transmission.

COM → C&DH:

End of Data: Message to the C&DH that all available data has been transmitted. This is the normal result of a successful data transmission.

Error: Transmission unsuccessful message.

C&DH → FLI:

Start Data Collection: Directive to the FLI to initiate flight telemetry data collection.

Collect Data Type: Directive for which data to collect: health and status or telemetry.

End Data Collection: Directive to the FLI to end flight telemetry data collection.

Packetize Data: Directive to the FLI to packetize the telemetry data for eventual transmission to the DSN.

Transmit Data to SCI: Directive to the FLI to send packetized telemetry data to the science mass memory.

FLI → C&DH:

Data Collection Successful: Measurement to the C&DH that telemetry data collection was successful.

Data Collection Failed: Error measurement to the C&DH that telemetry data could not be collected or saved.

Off-nominal Telemetry: Measurement to C&DH that the FLI has detected an off-nominal telemetry measurement.

C&DH → SCI:

Time: System Time.

Rationale: The directives from the C&DH are timed, so common system clock is required.

System Health and Status: Measurement and status information (e.g. telemetry modes) relevant to SCI software functions (↑SCI-10).

Start High-rate Data Collection, Compression and Packetization: Directive to the C&DH to start high rate science data. High rate science data is compressed in hardware and packetized in software before transmission to the DSN.

Start Low-rate Data Collection: Directive to the C&DH to start low rate science data. Low rate science data is compressed and packetized in software before transmission to the DSN.

Reset: Directive to the SCI to reset its computer.

SCI → C&DH:

Data Collection Successful: Measurement to the C&DH that science data collection was successful.

Data Collection Failed: Error measurement to the C&DH that science data could not be collected or saved.

Fault Detected: Measurement to C&DH that the SCI has detected an off-nominal behavior.

High-Priority Science Event: Measurement to the C&DH That the SCI has detected an unusual and interesting science reading. (Science opportunity.)

C&DH-2.2.2. The C&DH software uses Reed-Solomon for data encoding. (↑C&DH-SC10)
Rationale: Reed-Solomon code is impervious to single event upsets, which is required in this high radiation environment.

S/C-2.4. A flight data collection functional element on the spacecraft collects, stores, retrieves, and packetizes the flight data to be gathered in fulfillment of the mission high-level requirements and goals. (↑S/C-R1, S/C-R3, S/C-R6, S/C-C3, S/C-SC1), (↓C&DH-G1)

FLI-2.1. Flight data collection functional element collects telemetry, health and status data from various spacecraft sensors and stores the data on the Engineering Mass Memory.

FLI-2.2. The FLI packetizes telemetry, health and status data for transmission to the DSN via the SCI's telecommunication interface (MTIF) for small deep-space transponder (SDST) interface. (↑FLI-CF1.1) (↑SCI-CF2.2)

FLI-2.2.1 Upon command from the C&DH the FLI will use its own MTIF (rather than the SCI's MTIF) to transmit its data to the MOC.

FLI-2.3. The C&DH uses the FLI's MTIF for SDST interface during uplink.

FLI-2.4. When determining spacecraft health and status, the FLI reads sensors and if readings are outside predefined ranges, sends a high priority interrupt to the C&DH.

See (↑CS-Diagram1) for functional elements and components connected to the FLI.

FLI → Telemetry Sensor

Request for Health and Status Measurement: Directive to telemetry sensors for health and status measurement.

Request for Telemetry Data: Directive to telemetry sensors for telemetry data collection.

Telemetry Sensors → FLI

Health and Status Measurements: The Sensors give readings for health and status of the telemetry elements.

Telemetry Data Collection Successful: A measurement to the FLI that the telemetry data collection was successful.

Telemetry Data Collection Error: A measurement to the FLI that the telemetry data collection failed.

S/C-2.5. 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-R1, S/C-R2, S/C-R3, S/C-R6, S/C-C3, S/C-G2, S/C-SC1), (↓C&DH-G1)

SCI-2.1. The SCI collects science data on command from the C&DH and is responsible for payload control, command desequencing, internal fault protection, command processing, and science data formatting and compression. (↑SCI-10) (↑SCI-CF1.1, SCI-CF1.2, SCI-CF1.3, SCI-CF1.4)

SCI-2.1.1 High-rate science data (from the WAC and IRC) is collected, compressed in hardware, packetized and buffered on the science mass memory before transmission to the DSN during Communication periods on command from the C&DH. (↑SCI-SC8, SCI-SC9)

Rationale: High-rate data cannot be taken during non-communication periods due to scarce memory resources.

SCI-2.1.2 Low-rate science data is collected and stored on the science mass memory at all times and transmitted to the DSN on command from the C&HD.

SCI-2.2. The SCI receives packetized telemetry data from the FLI and transmits that the DSN on command from the C&DH.

SCI-2.3. When determining spacecraft health and status, the SCI reads sensors and if readings are outside predefined ranges, sends a high priority interrupt to the C&DH.

SCI-2.4. While performing science data collection the SCI will notify the C&DH via a high priority interrupt if a reading of exceptional scientific import is taken.

SCI-2.5. The SCI software uses Reed-Solomon for data encoding. (↑SCI-SC5) (↑MOC-CF3.5)

SCI-2.6. The SCI functional element contains a passive radiator to dissipate heat from the IRC. (↑IRC-SC4). (↑S/C-CF2.1, S/C-CF2.2)

SCI-2.6.1 The radiator is pointed away from the Sun and the surface of the icy moon at all times. Rationale: The radiator cannot perform well if pointed towards a heat source.

SCI-2.7. All science instrument electronics will be housed together in a shielded box. All instruments with a RDF 2 requirement will have require a design point of TBD Mrad (Si) behind 100 mils of Aluminum and parts with a radiation tolerance below 150 krad have a design point

of TBD Mrad Si behind 100 mils of Aluminum equivalent. (↑EA.2) (↑SCI-SC6) (↑MOC-CF3.4)

SCI-2.8. The electronic sensor heads will be housed separately from their processing hardware. (↑EA.2) (↑SCI-SC6) (↑MOC-CF3.4)

Rationale: The science instrument electronics must be protected as much as possible from radiation. The electronics that process the data from the optical heads are sensitive to radiation. Separation from the optical heads allows them to be partially shielded from radiation exposure. Putting all the instruments together conserves the radiation shielding mass.

SCI-2.9. Directives to and measurements from the SCI. (↑A&AC-CF1.1)

See (↑CS-Diagram1) for functional element and components connected to the C&DH.

SCI → WAC

Request for H&S Measurement: Directive to science sensors for health and status measurement.

Request for Telemetry Data: Directive to science sensors for science data collection.

WAC → SCI

Health and Status Measurements: Notification of the health and status of the WAC.

Science Data Collection Successful: Notification of science data collection success.

Science Data Collection Error: Notification of science data collection failure.

SCI → IRC

Request for H&S Measurement: Directive to science sensors for health and status measurement.

Request for Telemetry Data: Directive to science sensors for science data collection.

IRC → SCI

Health and Status Measurements: Notification of the health and status of the IRC.

Science Data Collection Successful: Notification of science data collection success.

Science Data Collection Error: Notification of science data collection failure.

SCI → MAG

Request for H&S Measurement: Directive to science sensors for health and status measurement.

Request for Telemetry Data: Directive to science sensors for science data collection.

MAG → SCI

Health and Status Measurements: Notification of the health and status of the IRC.

Science Data Collection Successful: Notification of science data collection success.

Science Data Collection Error: Notification of science data collection failure.

SCI-2.10. A wide angle camera onboard the spacecraft collects, and compresses visual image data. The scientific data is 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)

WAC-2.1 The WAC faces the surface of the moon and has a conical 30 degree half angle centered field of view. (↑SCI-CF2.3)

SCI-2.11. An infrared camera on board the spacecraft collects, and compresses infrared image data. The scientific data is 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)

IRC-2.1 The IRC faces the surface of the moon and has a conical 30 degree half angle centered field of view.

IRC-2.2 For proper operation the IRC camera requires that its electronics be cooled to 80 degrees Kelvin.

Rationale: The infrared camera uses Mercury- Cadmium-Tellurium (Hg-Cd-Te) diodes in the detector as it is suitable for both long-wave (8-12 μ m) and medium-wave infrared (3-5 μ m) spectroscopy. This material must be cooled to a temperature below 80 Kelvin to function properly. (Detector Material:
<http://www.wipo.int/pctdb/en/wo.jsp?WO=1999%2F36960&IA=WO1999%2F36960&DISPLAY=DESC>)

SCI-2.12. A magnetometer on board the spacecraft collects magnetic field data. The scientific data is 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)

MAG-2.1 The MAG is located on the nadir of the spacecraft.

S/C-2.6. 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-R2, 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 The A&AC will use the flight computer and estimation and control of spacecraft state to calculate thrust and spacecraft attitude changes to achieve attitude and orbital requirements from the C&DH. (←C&DH-2.4) (↑A&AC-SC1) (↑COM-CF1.1, A&AC-CF2.1, MOC-CF3.1, MOC-CF3.2) (↑A&AC-2.1)

A&AC-2.2 The A&AC uses a startracker and a suntracker with TBD accuracy to calculate the attitude and pointing of the spacecraft. These calculations are performed every TBD seconds. (↑A&AC-SC1)

S/C-2.7. A communications functional element on the spacecraft modulates spacecraft data to be transmitted through the DSN, radiates towards the DSN when in line-of-sight contact and demodulates data from signals received from the DSN. (↑S/C-R3, S/C-R4, S/C-R6, S/C-SC2), (↓C&DH-G1, COM-G1, COM-G2, COM-G3, COM-G4)

COM-2.1 The COM takes directives from the C&DH and sends back COM state information to the C&DH.

COM-2.2 The COM utilizes a High Gain Antenna (HGA) for bi-directional communication with Earth via the DSN. The HGA is line-of-sight and at a distance of TBD km from Earth, it must be pointed within TBD degrees of Earth's center to communicate with the MOC.

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

2.2.1 The Spacecraft must format requests for the DSN in terms of desired bandwidth along with communication start and end times.

Rationale: Previous DSN requests were in the form of a specific 70-meter antenna, but the next generation DSN array will have a quality of service architecture, and request for specific antennas will not be honored.

DSN-2.1 The DSN manually switches which antennas are actively communicating with the spacecraft as the Earth rotates. As one transceiving antenna is occluded by the Earth another antenna has been introduced in to the communication link to continue transceiving without any loss of data. (↑DSN-SC1) (↑MOC-CF1.1)

DSN-2.1.1 The DSN receives directives from mission control concerning data transceiving and communication schedules. (↑DSN-SC2)

DSN-2.2 The DSN is a prioritized resource and may be taken over by higher priority missions.

2.3 A facility on earth, the Mission Operations Center (MOC), provides human operators with the capability to issue directives to the spacecraft and monitor telemetry transmitted back to Earth. (↑ 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).

MOC-2.1 The MOC communicates with higher priority mission (e.g. manned missions) in order to schedule space asset use around the higher priority mission. (↑ MOC-SC1) (↑MOC-CF1.1, MOC-CF2.1)

MOC-2.2 The mission plan developed at the MOC contains time sensitive directives.

Rationale: The MOC uses state information from the spacecraft and science and engineering goals from the operations division to create plans for the spacecraft to execute. The plans use time sensitive forecasting and are made such that they must be received by the spacecraft within TBD time.

MOC-2.3 The MOC uses Doppler tracking to reconstruct the European explorer's orbit in order to discover the location of a potential ocean. (←MOC-SC2)

Level 3: Blackbox Behavior

