Goddard Space Flight Center

Rules for the Design, Development, Verification, and Operation of Flight Systems

GSFC – STD – 1000
Revision C
October 30, 2006

Check the GSFC Directives Management System at
http://gdms.gsfc.nasa.gov to verify that this is the correct version prior to use

Goddard Space Flight Center

Rules for the Design, Development, Verification, and Operation of Flight Systems

GSFC – STD – 1000
Revision C
October 30, 2006

Note: GOLD Rules Baseline dated 10 Dec. 04 was signed per signature lines herein.
All subsequent revisions are signed by present authorities

Approved by:

C. J. Scolese
Deputy Director

Richard M. Day
Director of Mission Success

Arthur F. Obenschain
Director of Flight Programs and Projects

Abigail D. Harper
Deputy Director of Systems Safety and Mission Assurance

Michael G. Ryschkewitsch
Director of Applied Engineering and Technology

TABLE OF CONTENTS

Introduction		6
Standards, Processes, and Rules Hierarchy		7
Goddard Open Learning Design (G.O.L.D) Standard Architecture		8
GSFC Project Lifecycle		9
User's Guide		10
GSFC Rules		
1.0 Systems Engineering		
1.01	Requirements Management	11
1.02	Development & Implementation of Mission Operations Concept	12
1.03	Verification of Mission Requirements	13
1.04	System Modes	14
1.05	Single Point Failures	15
1.06	Resource Margins	16
1.07	End-to-End GN&C Phasing	18
1.08	End-To-Testing	19
1.09	Reserved	
1.10	Logistics and Spares	20
1.11	Qualification of Heritage Flight Hardware	21
1.12	Units of Measurement	22
1.13	Performance Demonstration During Qualification Testing	23
1.14	Mission Critical Telemetry	24
1.15	GSE Use at Launch Site	25
1.16	Ground Systems Configuration	26
1.17	Safe Hold Mode	27
1.18	Reserved	
1.19	Initial Thruster Firing Limitations	28
1.20	Manifold Joints of Hazardous Propellants	29
1.21	Overpressurization Protection in Liquid Propulsion Systems	30

1.22	Purging of Residual Test Fluids	31
1.23	Reserved	
1.24	Propulsion System Safety Electrical Disconnect	32
1.25	Reserved	
1.26	Safety Inhibits & Fault Tolerance	33
1.27	Propulsion System Overtemp Fuse	34
1.28	Unintended Propellant Vapor Ignition	35
1.29	Leakage of Hazardous Propellant	36
1.30	Controller Stability Margins	37
1.31	Actuator Sizing Margins	38
1.32	Thruster and Venting Impingement	39
1.33	Polarity Checks of Critical Components	40
1.34	Closeout Photo Documentation of Key Assemblies	41
1.35	Maturity of New Technologies	42
1.36	Block-Redundant Component Failure	43
1.37	Stowage Configuration	44
1.38	Configuration Command Confirmation	45
2.0 Electrical		
2.01	Flight Electronic Hardware Operating Time	46
2.02	EEE Parts Program for Flight Missions	47
2.03	Radiation Hardness Assurance Program	48
2.04	Dedicated Hardware ETU and EGSE	49
2.05	System Grounding Architecture	50
2.06	System Fusing Architecture	51
2.07	End-to-End Test of Release Mechanism for Flight Deployables	52
2.08	Reserved	
2.09	Spectrum Allocation Considerations	53
2.10	Electronic Design for Flight Missions	54
2.11	EMI/EMC Design for Flight Missions	55
2.12	Printed Circuit Board Coupon Analysis	56

2.13	Electrical Connector Mating	57
2.14	Capping of Test Point and Plugs	58
2.15	Flight and Ground Electrical Hardware	59
2.16	Solar Arrays	60
2.17	I&T Development Input	61
3.0 Software		
3.01	Verification+Validation Program for Mission Software Systems	62
3.02	Reserved	
3.03	High Fidelity Interface Simulation Capabilities	63
3.04	T&C System Selection Trade Study for Operations Ground System	64
3.05	Flight / Ground System Test Capabilities	65
3.06	Dedicated ETU for Flight Software (FSW) Testing	66
3.07	Flight Software Margin Warnings	67
3.08	Reserved	
3.09	Software Development Approach	71
3.10	Flight Operations Preparations and Team Development	72
3.11	Long Duration and Failure Free System Level Test of Flight Software	73
3.12	Visibility of Spacecraft State	74
3.13	Operational Software Redundant Element	75
3.14	Command Procedure Changes	76
3.15	Test and GSE Software Interfaces	77
4.0 Mechanical		
4.01	Contamination Control, Planning, and Execution	78
4.02	Reserved	
4.03	Structural Analysis and Design Factors of Safety	79
4.04	Reserved	
4.05	Reserved	
4.06	Validation of Thermal Coatings Properties	80
4.07	Solder Joint Intermetallics Mitigation	81
4.08	Space Environment Effects on Material Selection	82

4.09	Mechanical Test Factors and Duration	83
4.10	Minimum Workmanship	84
4.11	Testing in Flight Configuration	85
4.12	Structural Proof Testing	86
4.13	Modal Survey Characterization	87
4.14	Structural Qualification	88
4.15	Torque Margin	89
4.16	Reserved	
4.17	Reserved	
4.18	Deployment and Articulation Verification	90
4.19	Reserved	
4.20	Fastener Locking	91
4.21	Reserved	
4.22	Precision Component Assembly	92
4.23	Life Test	93
4.24	Mechanical Clearance Verification	94
4.25	Thermal Design Margins	95
4.26	Thermal Design Margins - Unplanned Conditions	96
4.27	Test Temperature Margins	97
4.28	Thermal Design Margin Verification	98
4.29	Thermal-Vacuum Cycling	99
5.0 Instruments		
5.01	Reserved	
5.02	Reserved	
5.03	Reserved	
5.04	Instrument Testing for Multipaction	100
5.05	Fluid Systems GSE	101
5.06	Flight Instrument Characterization Standard	102
5.07	Reserved	
5.08	Laser Development Contamination Control	103

5.09 Cryogenic Pressure Relief 104
Glossary 105
Change History 114

INTRODUCTION

Goddard Space Flight Center (GSFC) Rules are a high-level subset of all the design rules required for safety and mission success for all space flight products. These rules spell out the technical or design requirements that every Goddard project shall meet regardless of its implementation approach. GSFC Rules are not replacements for existing Goddard Procedural Requirements (GPRs) or NASA Procedural Requirements (NPRs). NPRs and GPRs are specific, detailed procedures for implementing NASA and Goddard policies, and as such they often address project management requirements per NASA Procedural Requirement (NPR) 7120.5 that do not fall within the scope of the GSFC Rules. Figure 1 provides a hierarchy of where the GSFC Rules fit within the Center's larger collection of rules. Figure 2 illustrates the role the GSFC Rules play in the Goddard Open Learning Design (G.O.L.D.) approach to knowledge management. GSFC Rules are not intended to serve as a "cookbook" or "how-to" guide, but rather as another tool for assessing overall project risk and assuring mission success.

GSFC Rules are defined and apply in relation to the lifecycle of a mission or project. (See Figure 3.) All products shall be designed, developed, verified and operated in accordance with the GSFC Rules. Exceptions shall be permitted only by formal waiver or deviation, processed and approved in accordance with GPG 8070.4, or by virtue of the requirement's non-applicability to the product, as explicitly stated in the rule. Figure 4 defines the rule structure and explains the difference between the rule principle and rule activities, with respect to project compliance. The Principle states the requirement of each rule, and a formal waiver or deviation is required for non-compliance. Activities are best practices, identified across lifecycle phases. Non-compliance with activities does not require waivers or deviations, but may generate a request for action.

The Office of Mission Success (OMS) shall develop and maintain the GSFC Rules for the Design, Development, Verification, and Operation of Flight Systems. GSFC Rules shall adhere to the following criteria:
a) It is a high-value principle to establish the methodology necessary to consistently and efficiently achieve safety and mission success;
b) It is important enough to require compliance, or formal waivers, for all GSFC projects;
c) The rationale is based on sound engineering practice, systems management principles, or lessons learned; and
d) A system engineering product or other objective verification method is identified at one or more milestones in the project life cycle.

GSFC Rules shall be configuration-controlled and accessible to all GSFC employees. A technical authority designated for each rule will be responsible for validating the principle, rationale, verification requirements, related guidance and lessons learned, and participating in the evaluation of proposed changes, waivers and deviations.

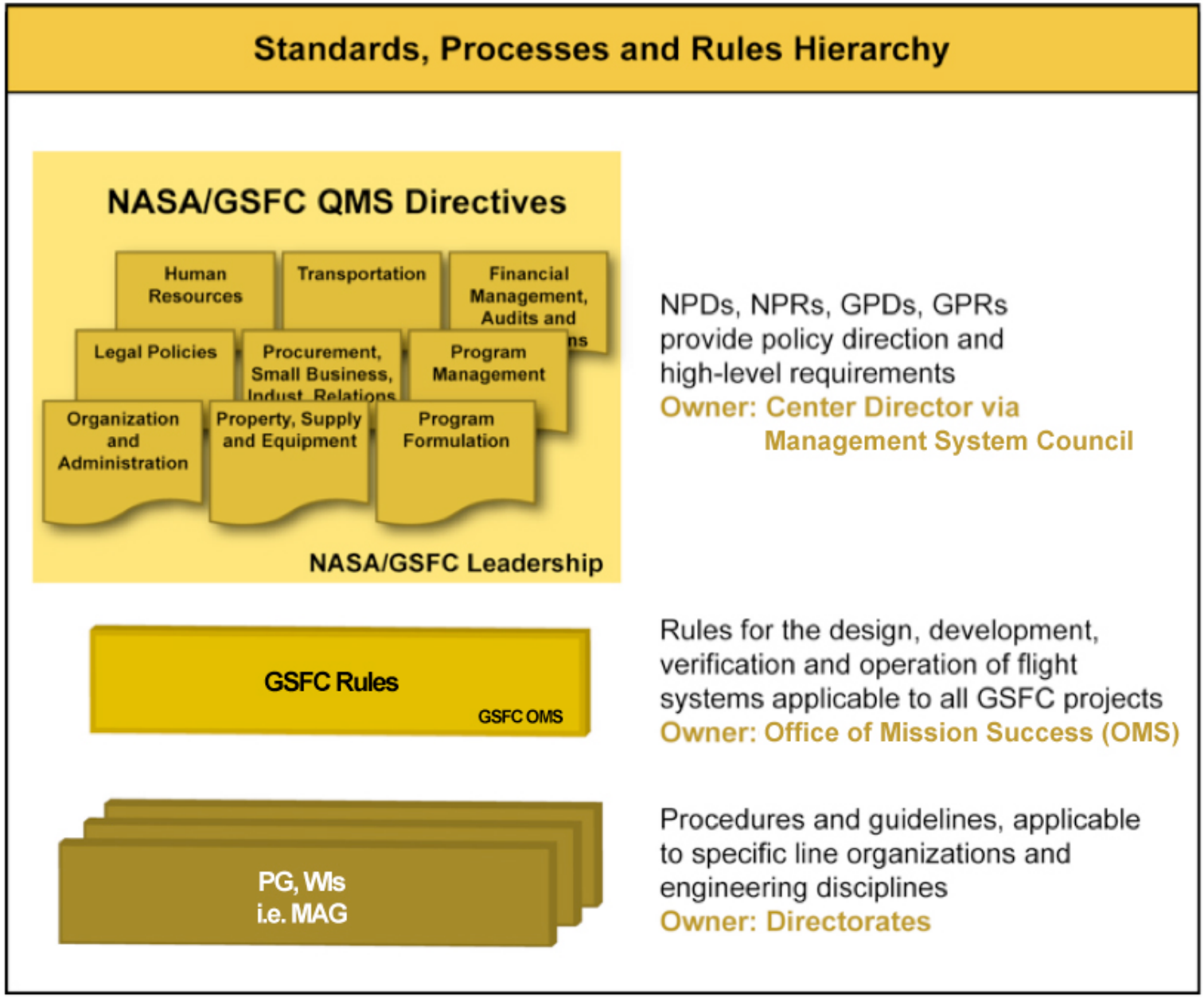
Standards, Processes and Rules Hierarchy
NASA/GSFC QMS Directives
Human Resources
Transportation
Financial Management, Audits and
Legal Policies
Procurement, Small Business,
Program Management
Organization and Administration
Property, Supply and Equipment
Program Formulation
NASA/GSFC Leadership
NPDs, NPRs, GPDs, GPRs provide policy direction and high-level requirements
Owner: Center Director via Management System Council
GSFC Rules
GSFC OMS
Rules for the design, development, verification and operation of flight systems applicable to all GSFC projects
Owner: Office of Mission Success (OMS)
PG, WIs
i.e. MAG
Procedures and guidelines, applicable to specific line organizations and engineering disciplines
Owner: Directorates

Figure 1

* Mission risk classification will be addressed in a future revision.

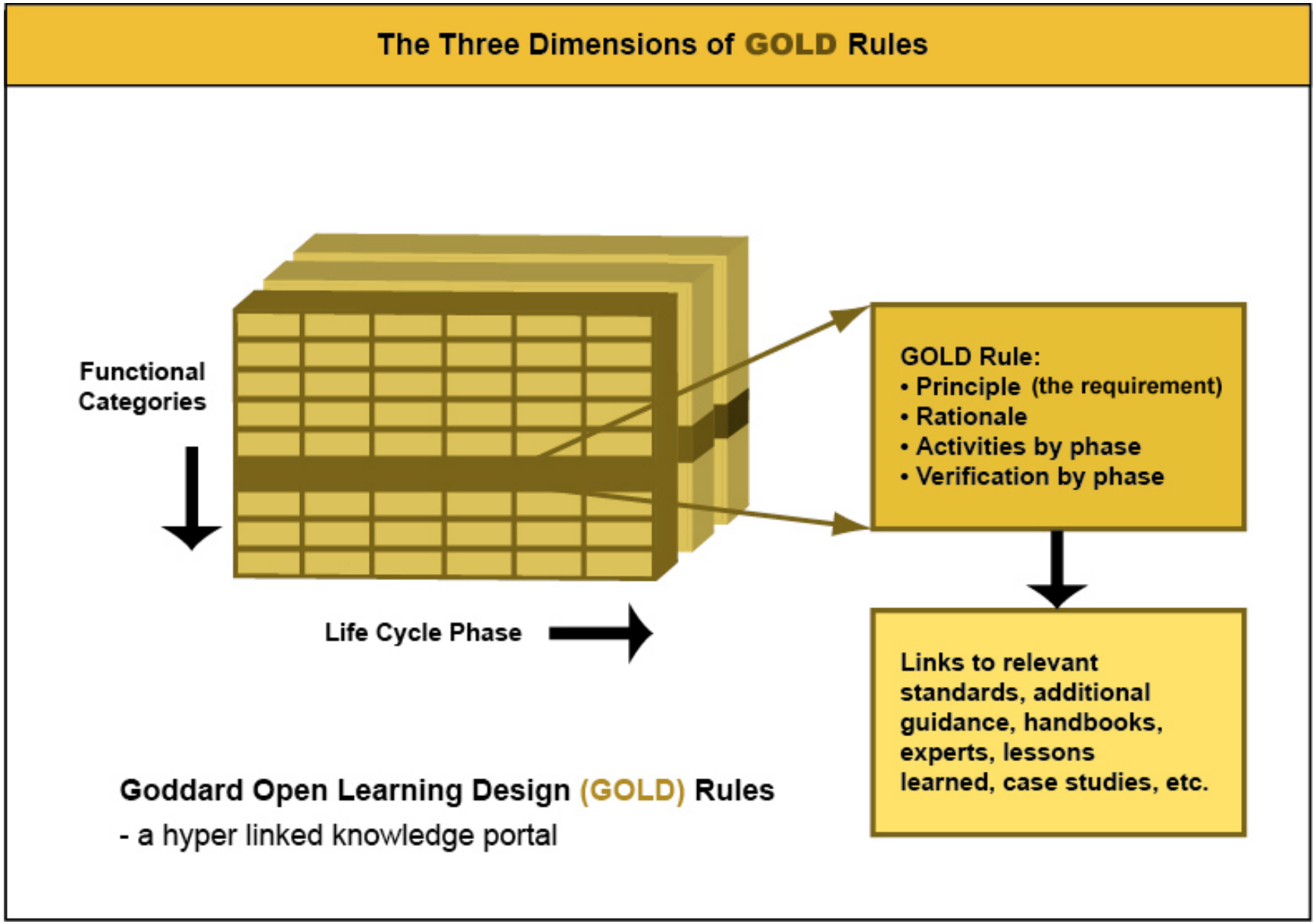

Figure 2

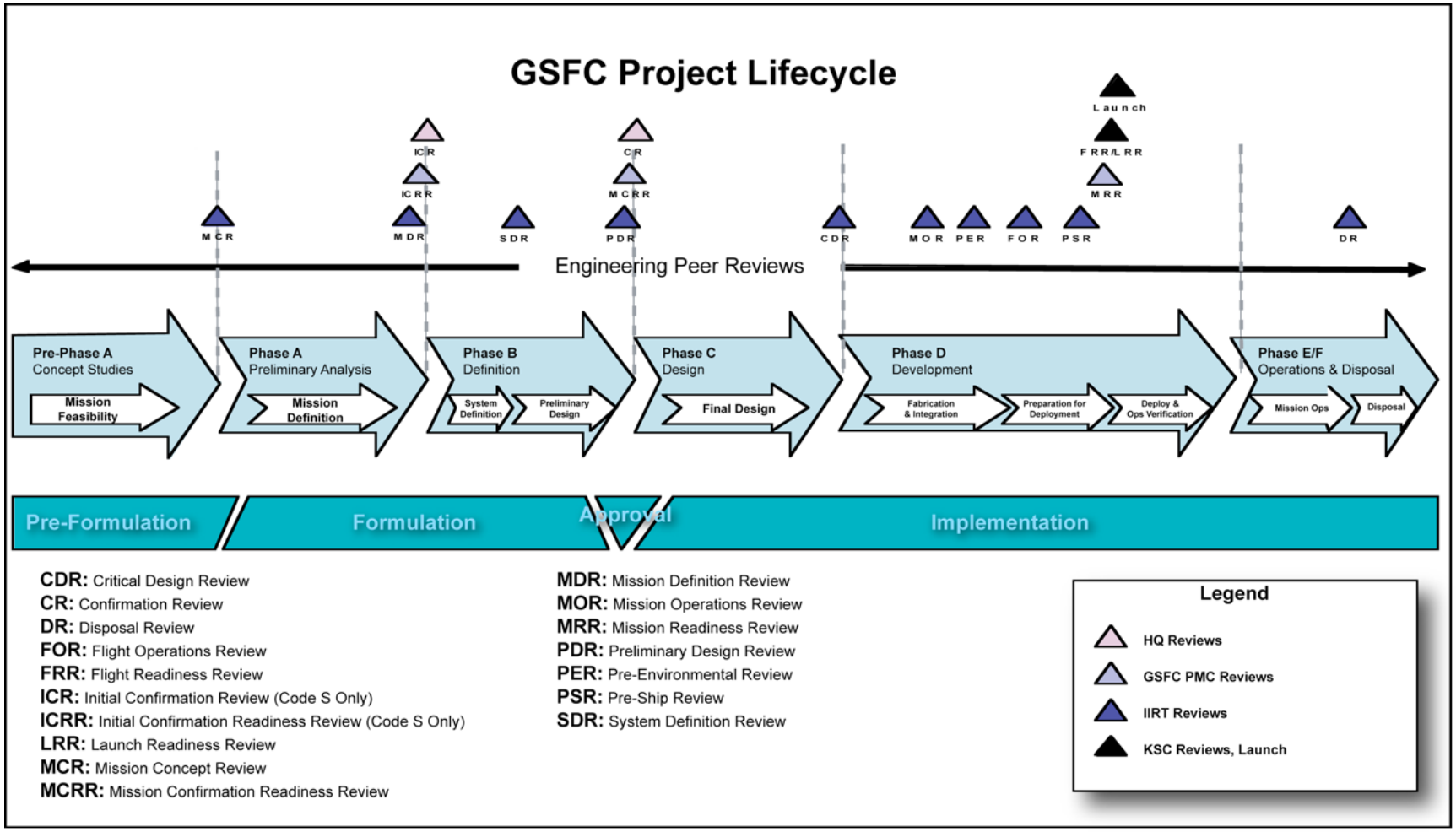
GSFC Project Lifecycle
Launch
FRR/LRR
MRR
ICR
ICRR
CR
MCRR
MCR
MDR
SDR
PDR
CDR
MOR
PER
FOR
PSR
DR
Engineering Peer Reviews
Pre-Phase A
Concept Studies
Mission Feasibility
Phase A
Preliminary Analysis
Mission Definition
Phase B
Definition
System Definition
Preliminary Design
Phase C
Design
Final Design
Phase D
Development
Fabrication & Integration
Preparation for Deployment
Deploy & Ops Verification
Phase E/F
Operations & Disposal
Mission Ops
Disposal
Pre-Formulation
Formulation
Approval
Implementation
CDR: Critical Design Review
CR: Confirmation Review
DR: Disposal Review
FOR: Flight Operations Review
FRR: Flight Readiness Review
ICR: Initial Confirmation Review (Code S Only)
ICRR: Initial Confirmation Readiness Review (Code S Only)
LRR: Launch Readiness Review
MCR: Mission Concept Review
MCRR: Mission Confirmation Readiness Review
MDR: Mission Definition Review
MOR: Mission Operations Review
MRR: Mission Readiness Review
PDR: Preliminary Design Review
PER: Pre-Environmental Review
PSR: Pre-Ship Review
SDR: System Definition Review
Legend
HQ Reviews
GSFC PMC Reviews
IIRT Reviews
KSC Reviews, Launch
Rev. – 8/9/04

Figure 3

USER'S GUIDE

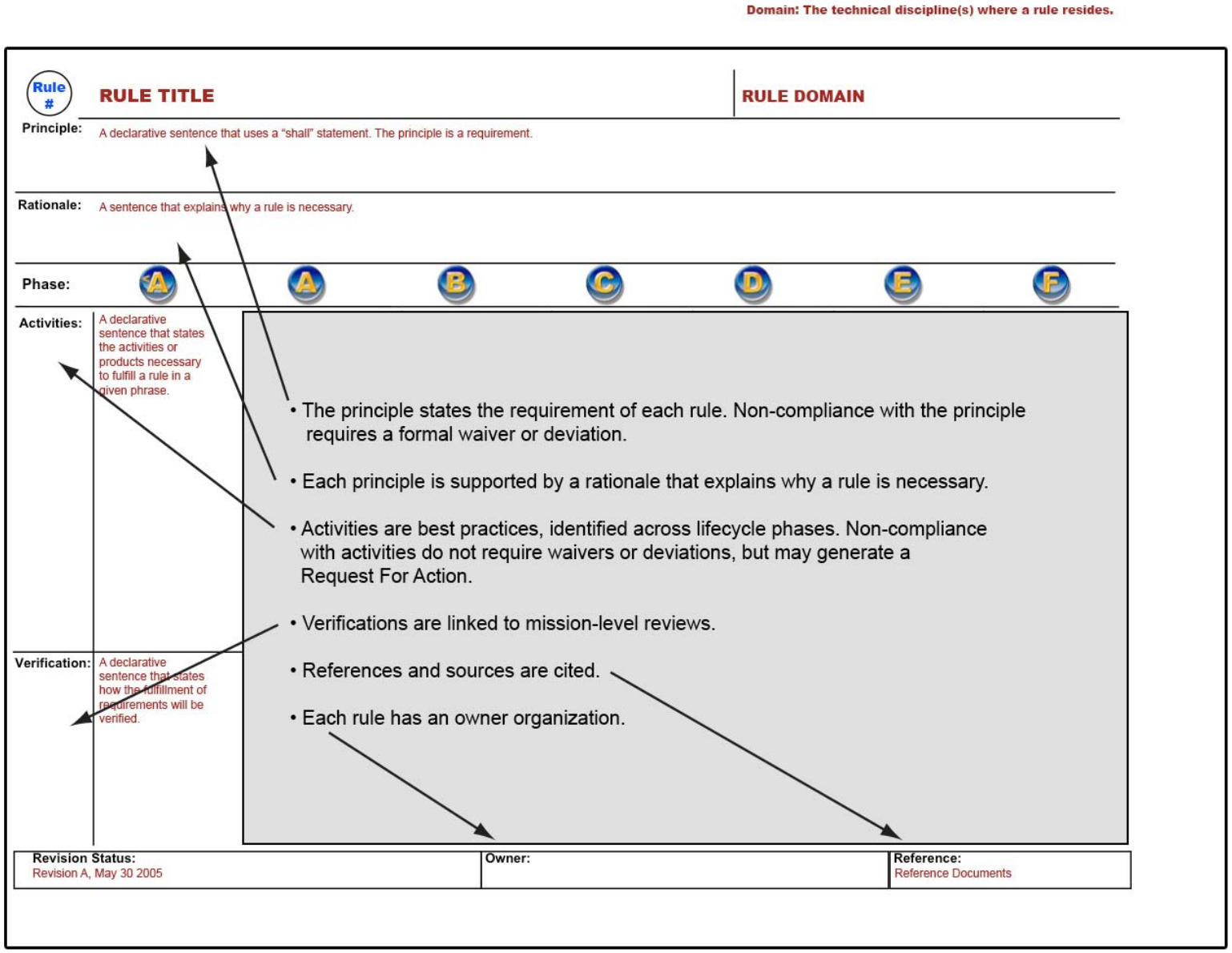

Figure 4

1.01 Requirements Management

Systems Engineering

Principle: A requirements management process shall be developed throughout the lifecycle that includes requirements identification, tracking, and documentation as well as a flow-down and traceability of Level 1 requirements to implementation requirements.

Rationale: Clear, traceable requirements lead to a good understanding of how high level objectives and requirements drive mission design and success.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Develop traceability matrix. 2. Develop draft Mission Requirements Document.	1. Update traceability matrix. 2. Define traceable Level 2 requirements in Mission Requirements Document. 3. Identify requirements management tools for Phases B, C, & D. 4. Validate consistency of requirements from all mission elements.	1. Update Mission Requirements Document and put under CM. 2. Implement requirements management tool. 3. Identify documentation structure required to define implementation of Level 2 requirements, Level 3 requirements, and Level 4 requirements. 4. Define Level 3 and 4 requirements and draft requirement documents. 5. Develop SEMP.	1. Update Mission Requirements Document. 2. Track changes to Level 2 requirements, Level 3 requirements, and Level 4 requirements.	1. Verify consistency of requirements in traceability matrix. 2. Document requirements verification.	1. Verify that mission operations requirements are still valid and make appropriate contingency plans.	1. Verify that disposal requirements are still valid and make appropriate contingency plans.
Verification:	1. Verify through project team concurrence, peer review, and at MCR.	1. Verify at MRR and MDR.	1. Verify at PDR.	1. Verify through peer review and at CDR.	1. Verify through peer review and at PER, MOR, FOR, and PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mission Engineering and Systems Analysis Division (590)	GPR 7120.5A

1.02 Development & Implementation of Mission Operations Concept

Systems Engineering

Principle: The Mission Operations Concept and Plan shall be defined and its implementation shall be verified throughout the lifecycle.

Rationale: The Mission Operations Plan is critical to the development of mission architecture necessary for a successful launch, deployment, commission, operation, and disposal.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Establish and document a concept for operations that incorporates instrument operations concept and accomplishes Level 1 requirements.	1. Identify all mission operation modes and configurations. 2. Update concept for operations. 3. Develop a concept for ground system design.	1. Draft Operations Concept. 2. Identify contingency concepts and safe hold modes. 3. Develop requirements for ground system.	1. Draft Operations Plan. 2. Begin development of operations procedures for ground system.	1. Update Operations Plan and put under CM. 2. Perform mission simulations and testing to verify Operations Plan, utilizing mission elements including ground system operations procedures. 3. Complete operations procedures.	1. Update post-launch changes to Operations Plan and document operational constraints.	1. Perform disposal operations per Operations Plan.
Verification:	1. Verify at MCR.	1. Verify through project team concurrence and at MRR and MDR.	1. Verify through peer review and at PDR.	1. Verify through peer review and at CDR.	1. Verify at MOR, FOR, LRR, and PSR, and ORR.	N/A	1. Verify at DR.

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Mission Engineering and Systems Analysis Division (590)	GPR 7120.5A

1.03 Verification of Mission Requirements

Systems Engineering

Principle: A process that ensures all mission requirements are verified shall be developed.

Rationale: Mission success requires that mission functions can be achieved and that system designs are implemented correctly.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Develop a verification matrix that identifies a verification method for all system functions that are critical to mission success.	1. Update draft verification matrix.	1. Draft a verification plan that identifies items and interfaces as well as functions to be verified, the verification method, and the method of approving results as well as necessary equipment, tools and facilities.	1. Update verification plan to include verification method for all requirements and mission-critical functions. 2. Draft a Comprehensive Performance Test Plan. 3. Put all plans under CM.	1. Prepare verification plans for tests, simulations or inspections. 2. Perform verifications; analyze and document results.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify at SDR and PDR.	1. Verify at CDR.	1. Verify at subsystem peer review, PER, PSR, LRR, and MRR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mission Engineering and Systems Analysis Division (590)	GPR 7120.5A

1.04 System Modes

Systems Engineering

Principle: System and sub-system (e.g., ACS, FSW, EPS, etc.) modes and states shall be properly identified and verified.

Rationale: Proper function of all system and sub-system modes, states, and transitions need to be verified for mission success. If not directly addressed, this verification can easily be overlooked.

Phase:							
Activities:	1. Identify strawman system and sub-system modes and states.	1. Produce preliminary diagram of system and sub-system mode and state transitions.	1. Refine diagram of system and sub-system mode and state transitions. 2. Define tests and analyses that verify system and sub-system modes, states, and mode transitions. 3. Incorporate into verification plan.	1. Update diagram of system and sub-system mode and state transitions. 2. Put document under configuration management control by CDR. 3. Perform detailed design of modes, states, and transitions. 4. Update verification of modes, states and transitions in verification plan.	1. Implement design of modes, states, and transitions. 2. Verify mode and state functionality and performance. 3. Define on-orbit execution of operational modes, states, and transitions.	N/A	N/A
Verification:	1. Verify at Peer review.	1. Verify at end of Phase A: Peer Review, SDR or SRR.	1. Verify at Peer review, PDR, CR.	1. Verify at CDR.	1. Verify at PER, PSR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Pending	Mission Engineering and Systems Analysis Division (590)	

1.05 Single Point Failures

Systems Engineering

Principle: Single point failures that inhibit the ability to fully meet minimum mission success requirements shall be identified, and the risk associated with each shall be characterized, managed, and tracked.

Rationale: Robust design approaches make the elimination of single point failures desirable. From a risk management perspective, it is recognized that the acceptance of some single point failures may be prudent. In these cases, it is essential to understand the attendant risks and receive approval from senior management.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Identify all requirements necessary for minimum mission success. 2. Determine if a breech of any of these requirements will cause the minimum mission to fail.	1. Identify failures that would cause the minimum mission to fail and develop a design strategy to avoid single point failures.	1. Identify failures for all hardware and software that performs mission-critical functions. 2. Develop a design to avoid single point failures.	1. Design mission-critical elements to avoid single point failures.	1. Verify that there are no single string failures in mission elements that are necessary for minimum mission success.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PER and PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mission Engineering and Systems Analysis Division (590)	

1.06 Resource Margins

Systems Engineering

Principle: Resource margins shall be met in accordance with Table 1.06-1.

Rationale: Compliance with these margins improves performance on cost and schedule as well as overall mission performance.
NOTE: Flight software margin warnings are covered in Rule 3.07.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Identify resource margins. 2. Identify the percent of resource that was determined by estimation, calculation or measurement.	1.Update resource margins. 2. Identify the percent of resource that was determined by estimation, calculation or measurement.	1. Update resource margins. 2. Identify the percent of resource that was determined by estimation, calculation or measurement.	1. Update resource margins. 2. Identify the percent of resource that was determined by estimation, calculation or measurement.	1. Update resource margins.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at ICR and MDR.	1. Verify at PDR and confirmation review.	1. Verify at CDR.	1. Verify at PER and PSR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Mission Engineering and Systems Analysis Division (590)	Guidelines for Margins (future)

Table 1.06-1 Technical Resource Margins
All values are assumed to be at the end of the phase

Resource	Pre-Phase A	Phase A	Phase B	Phase C	Phase D	Phase E
Mass	≥30%	≥25%	≥20%	≥15%	0	
Power (wrt EOL capacity)	≥30%	≥25%	≥15%	≥15%	≥10% *	
Propellant	3σ***				3σ	
Telemetry and Command hardware channels**	≥25%	≥20%	≥15%	≥10%	0	
RF Link	3 dB	3 dB	3 dB	3 dB	3 dB	
Margin (in percent)= (Available Resource-Estimated Value of Resource)/Estimated Resource X 100						

*At launch there shall be 10% predicted power margin for mission critical, cruise and safing operating modes as well as to accommodate in-flight operational uncertainties.
** Telemetry and command hardware channels read data from hardware such as thermistors, heaters, switches, motors, etc.
*** The 3 sigma variation is due to the following: 1. Worst-case spacecraft mass properties 2. 3-sigma low launch vehicle performance 3. 3-sigma low propulsion subsystem performance (thruster performance/alignment, propellant residuals) 4. 3-sigma flight dynamics errors and constraints 5. Thruster failure (applies only to single-fault-tolerant systems)

1.07 End-to-End GN&C Phasing

Systems Engineering

Principle: All GN&C sensors and actuators shall undergo end-to-end phasing/polarity testing after spacecraft integration and shall have flight software mitigations to correct errors efficiently.

Rationale: Many spacecraft have had serious on-orbit problems due to inadequate verification of signal phasing or polarity. Component-level and end-to-end phasing tests and flight software mitigations can ensure correct operation.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Define interface requirements of sensors and actuators. 2. Design flight software to include capability to fix polarity problems via table upload.	1. Update ICDs to include polarity definition 2. Review vendor unit-level phasing test plans. 3. Write flight S/W to include capability to fix polarity problems via table upload. 4. Create unit-level & end-to-end phasing test plan.	1. Perform unit-level phasing tests. 2. Test flight S/W for table upload functionality. 3. Perform end to-end phasing test for all sensor-to-actuator combinations. 4. Develop & test contingency flight ops procedures for fixing phasing problems.	N/A	N/A
Verification:	N/A	N/A	1. Verify through peer review and at PDR.	1. Verify through peer review and at CDR.	1. Verify at PSR and LRR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Flight Dynamics Analysis Branch (595)	

1.08 End-to-End Testing

Systems Engineering

Principle: System end-to-end testing shall be performed using actual hardware or simulation, and shall apply from input to instrument(s), through the spacecraft, transmitted to receiving antennas, and through the ground system - reconciled against what is physically achievable before launch, and consistent with associated mission risk.

Rationale: End-to-end testing is the best verification of the system's functionality, and often cannot be fully achieved because of difficulties in closing some of the links. Breaks from a continuous end-to-end test are permitted in such cases, if they are consistent with the associated risks of the mission classification.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Identify end-to-end tests that represent system-level functions.	1.Review and update the list of end-to-end tests and analyses identified in Pre-phase A. 2. Define success criteria for verification and incorporate into verification plan. 3. Review and update verification plan and schedule. 4. Identify facilities required for end-to-end testing.	1. Review and update list of end-to end tests and analyses identified in Phase A. 2. Review and update verification plan and schedule. 3. Identify test plans and facilities that need to be in place for end-to-end testing.	1. Draft final verification plan. 2. Sign off on plan, put under CM test schedule. 3. Identify and schedule sequence of analyses and testing for verifying end-to-end flight performance. 4. Quantify the fidelity of each verification step.	1. Perform unit-level phasing tests. 2. Test flight S/W for table upload functionality. 3. Perform end to-end phasing test for all sensor-to-actuator combinations. 4. Develop & test contingency flight ops procedures for fixing phasing problems.	N/A	N/A
Verification:	1. Verify all elements of the operating observatory and ground system at MCR.	1. Verify at MDR.	1. Verify at SDR or SRR, PDR.	1. Verify at CDR.	1. Verify at PSR and LRR.	N/A	N/A

Revision Status:	Owner:	Reference:
Pending	Mission Engineering and Systems Analysis (590)	GEVS 2.8

1.10 Logistics and Spares

Systems Engineering; Electrical

Principle: All projects shall define a plan for required spare units (including spare EEE parts) that is compatible with available resources and acceptable risk.

Rationale: An inadequate spare parts program leads to part shortages during the development phase and has a direct impact on potential workarounds or retrofit plans.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Address spare parts program and acquisition strategy for critical long lead items in concept study. 2. Define preliminary parts plan. 3. Identify parts list and ETUs required for life testing. 4. Identify critical parts that require spares.	1. Identify parts acquisition plan for long lead parts. 2. Update preliminary parts plan. 3. Develop acquisition strategy for parts and ETUs for life testing and critical parts that require spares.	1. Finalize parts plan. 2. Implement acquisition strategy for parts and ETUs for life testing and critical parts that require spares. 3. Begin life testing where relevant.	1. Track critical spare parts and prepare specific risk mitigation plans(s) for lower quantity spares.	N/A	N/A
Verification:	N/A	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	Verify at MRR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Mission Engineering and Systems Analysis Division (590)	

1.11 Qualification of Heritage Flight Hardware

Systems Engineering

Principle: All use of heritage flight hardware shall be fully qualified and verified for use in its new application. This qualification shall take into consideration necessary design modifications, changes to expected environments, and differences in operational use.

Rationale: All hardware, whether heritage or not, needs to be qualified for its expected environment and operational uses.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Identify/list heritage hardware to be used and make a cursory assessment of 'use as is' or delta-qual.	1. Update hardware list and identify the qualification requirements. 2. Assess through the peer review process the ultimate applicability of previously flown/ heritage hardware designs.	1. Refine/finalize heritage hardware list and the required qualification requirements.	1. Qualify heritage hardware as part of overall qualification of mission hardware.	1. Develop, test, and integrate the flight articles.	N/A	N/A
Verification:	1. Review summary documentation at MCR.	1. Review summary documentation at MDR.	1. Review summary documentation at PDR.	1. Review summary documentation at CDR.	1. Review summary documentation at PER and PSR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Mission Engineering and Systems Analysis Division (590)	

1.12 Units of Measurement

Systems Engineering

Principle: All design elements shall be specified and designed to ensure the consistent and compatible use of physical units of measure.

Rationale: Critical functions can be misprepresented by errors in unit conversions.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Determine unit standards.	1. Implement unit standards.	1. Implement unit standards and document as part of requirements management process. 2. All drawings, figures, presentations, and user interfaces shall clearly include units.	1. Implement unit standards and document as part of requirements management process. 2. All drawings, figures, presentations, and user interfaces shall clearly include units.	N/A	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	N/A	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mission Engineering and Systems Analysis Division (590)	JPL D-17868 rev. 2: 4.11.1.3

1.13 Performance Demonstration During Qualification Testing

Systems Engineering

Principle: During qualification testing, hardware shall demonstrate expected (i.e.: within-tolerance) performance over a range of conditions that envelops the worst-case operating parameters anticipated to occur during the planned operational mission. Testing at all levels (system, sub-system, and component) shall have clearly defined pass/fail criteria.

Rationale: Mission success requires demonstration of performance over a range of worst-case operating conditions.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Identify worst-case operating parameters for performance testing. 2. Develop plans for qualification testing that demonstrates performance under worst-case operating parameters.	1. Update plans for qualification testing that demonstrates performance under worst-case operating parameters. 2. Document plans and put under configuration control.	1. Perform qualification testing that demonstrates performance under worst-case operating parameters.	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PER.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Mission Engineering and Systems Analysis Division (590)	

1.14 Mission Critical Telemetry and Command Capability

Systems Engineering

Principle: Continuous telemetry coverage shall be maintained during all mission-critical events. Mission-critical events shall be defined to include separation from the launch vehicle; power-up of major components or subsystems; deployment of mechanisms and/or mission-critical appendages; and all planned propulsive maneuvers required to establish mission orbit and/or achieve safe attitude. After separation from the launch vehicle, continuous command coverage shall be maintained during all following mission-critical events.

Rationale: With continuous telemetry and command capability, operators can prevent anomalous events from propagating to mission loss. Also, flight data will be available for anomaly investigations.

Phase:	A	A	B	C	D	E	F
Activities:	1. Identify and document potential mission-critical events in concept of operations. 2. Identify and document in concept of operations all potential needs for communications coverage, such as TDRSS or backup ground stations.	1. Update concept of operations. 2. Identify requirements for critical event coverage in ground system design.	1. Address and document coverage of mission critical events in draft of Mission Operations Concept. 2. Address critical event coverage in requirements for ground system design.	1. In Operation Plan, identify telemetry and command coverage for all mission-critical events.	1. Update Operations Plan. 2. Address telemetry and command coverage of critical events in Operations Procedures.	1. Perform critical events with telemetry and command capability.	N/A
Verification:	1. Verify through project team concurrence, peer review, and at MCR.	1. Verify at MRR and MDR.	1. Verify at PDR.	1. Verify through peer review and at CDR.	1. Verify through peer review and at PER , MOR, FOR and PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Guidance, Navigation and Control Systems Engineering (591)	

1.15 GSE Use at Launch Site

Systems Engineering

Principle: All testing of operations of flight systems at the launch site or in the field shall only use GSE and test configurations that have been previously used with the flight hardware.

Rationale: New testing configurations introduce unknown variables that could possibly cause damage to flight or ground test hardware as well as delays in schedule.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	N/A	1. Identify tests and associated GSE required in the field or at the launch site. 2. Ensure that the GSE required for these tests is used in I&T and is available for use in the field or at the launch site.	1. Draft test plans for launch site verifications and specify all test configurations required. 2. Ensure that these configurations are verified with the flight article and in use before shipping.	N/A	N/A
Verification:	N/A	N/A	N/A	1. Verify at CDR.	1. Verify at PER and PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mission Engineering and Systems Analysis Division (590)	

1.16 Ground Systems Configuration

Systems Engineering

Principle: Mission-critical software and hardware under configuration control shall be used when I&T and mission operations are performed.

Rationale: Software configuration ensures that ground systems will repeatedly perform as expected, which is critical for spacecraft maneuvers, mission planning, spacecraft monitoring, and science data processing.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Define all configuration items (CIs) needed for ground operations throughout the mission lifecycle, including hardware, software, and documentation.	1. Define configuration control processes, CCB members, and due dates for CIs.	1. Provide CIs to CCB for approval. 2. Populate CI database. 3. Freeze mission-critical software by FOR.	1. Ensure that only approved CIs are used for critical spacecraft operations. 2. Maintain CCB processes for including new CIs.	1. Ensure that only approved CIs are used for disposal. 2. Maintain CCB processes for including new CIs.
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify at FOR and ORR.	1. Mission Director and Flight Operations Team verify during operations.	1. Verify at DR.

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Flight Dynamics Analysis Branch (595)	

1.17 Safe Hold Mode

Observatory Subsystems; GN&C

Principle: All spacecraft shall have a power-positive control mode (Safe Hold) to be entered in spacecraft emergencies. Safe Hold Mode shall have the following characteristics: (1) its safety shall not be compromised by the same credible fault that led to Safe Hold activation; (2) it shall be as simple as practical, employing the minimum hardware set required to maintain a safe attitude; and (3) it shall require minimal ground intervention for safe operation.

Rationale: Safe Hold Mode should behave very predictably while minimizing its demands on the rest of the spacecraft. This facilitates the survival, diagnosis, and recovery of the larger system. Complexity typically reduces the robustness of Safe Hold, since it increases the risk of failure due to existing spacecraft faults or unpredictable controller behavior.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Ensure that requirements document and operations concept include Safe Hold Mode.	1. Ensure that requirements document and operations concept include Safe Hold Mode.	1. Identify hardware & software configuration for Safe Hold Mode. 2. In preliminary FMEA, demonstrate that no single credible fault can both trigger Safe Hold entry and cause Safe Hold failure. 3. Analyze performance of preliminary Safe Hold algorithms.	1. Establish detailed Safe Hold design including entry/exit criteria and FDAC requirements for flight software. 2. In final FMEA, demonstrate that no single credible fault can both trigger Safe Hold entry and cause Safe Hold failure. 3. Analyze performance of Safe Hold algorithms. 4. Via a rigorous risk assessment, decide whether or not to test Safe Hold on-orbit.	1. Implement Safe Hold Mode. 2. Verify proper mode transitions, redundancy, and phasing in ground testing. 3. Execute recovery procedures during mission simulations. 4. Perform on-orbit testing if applicable.	N/A	N/A
Verification:	1. Verify through peer review and at MCR.	1. Verify through peer review and at MDR.	1. Verify through peer review and at PDR.	1. Verify through peer review and at CDR.	1. Verify at PER and FOR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	GN&C Systems Engineering Branch (591)	Code 590 Policy

1.19 Initial Thruster Firing Limitations

Observatory Subsystems; GN&C

Principle: All initial thruster firings shall occur with real-time telemetry and command capability. If alternate actuators (e.g. reaction wheels) are present, the momentum induced by initial firings shall be within the alternate actuators' capability to execute safe recovery of the spacecraft.

Rationale: Polarity issues and thruster underperformance typically occur early in the mission. Both conditions can result in a spacecraft emergency due to excessive spacecraft spin rates.

Phase:							
Activities:	1. The Attitude Control System (ACS) Concept shall ensure that thrusters will not be required during launch vehicle separation for a 3-sigma distribution of cases. The concept for operations shall ensure that, except in case of emergency, all thrusters can be test-fired on-orbit prior to the first delta-v maneuver.	1. The Attitude Control System shall design the thruster electronics, size and place the thrusters, and size other actuators (e.g. reaction wheels) such that a failed thruster can be shut down and the momentum absorbed before power or thermal contstraints are violated. The activities specified in Pre-Phase A shall be maintained.	1. Hardware (processors, power interfaces, data interfaces, etc.) and software shall ensure that anomalous thruster firings will be shut down quickly enough to allow recovery of the spacecraft to a power-safe and thermal-safe condition. 2. Develop design and operations concept consistent with the activities established in Pre-Phase-A.	1. Estabish detailed recovery procedures. Finalize design and operations concept consistent with the activities established in Pre-Phase-A.	1. Test failed thruster conditions with the greatest possible fidelity. Verify transitions and polarity. 2. Ensure that recovery procedures have been simulated with the flight operations team. 3. During on-orbit testing, thrusters shall be test fired to verify polarity and performance prior to being used in a closed loop control.	1. Ground contact shall be maintained during thruster firings.	1. Maintain activity per Phase E. 2. Document any lessons learned.
Verification:	1. GN&C and system engineering organizations shall verify at MCR.	1. GN&C and system engineering organizations shall verify at MDR.	1. GN&C and system engineering organizations shall verify at PDR.	1. GN&C and system engineering organizations shall verify at CDR.	1. GN&C and system engineering organizations shall verify at SAR. 2. Follow-up at Operational Readiness Review (ORR).	1. Document lessons learned.	1. GN&C and system engineering organizations shall verify at DR. 2. GN&C and system engineering organizations document lessons learned.

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Flight Dynamics Analysis Branch (595)	

1.20 Manifold Joints of Hazardous Propellants

GN&C; Propulsion

Principle: All joints in the propellant manifold between the propellant supply tank and the first isolation valve shall be NDE-verified welds.

Rationale: Failure of manifold joint poses critical or catastrophic threat to personnel and/or facility.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Confirm system requirements for welded manifold joints.	1.Present weld & technician certification plans and NDE plans.	1. Certify integrity of welds by NDE.	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Propulsion Branch (597)	

1.21 Overpressurization Protection in Liquid Propulsion Systems

GN&C; Propulsion

Principle: The propulsion system design and operations shall preclude damage due to pressure surges ("water hammer"). (Note: See also rule 1.28 "Unintended Propellant Vapor Ignition.")

Rationale: Pressure surges could result in damage to components or manifolds, leading to failure of the propulsion system, damage to facilities, and/or safety risk to personnel.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Perform pressure surge analysis, based on worst-case operating conditions, to determine maximum surge pressure. 2. If maximum surge pressure is greater than system proof pressure, incorporate design features to reduce surge pressure below proof pressure.	1. Demonstrate by test that maximum surge pressure is less than system proof pressure. 2. Demonstrate by test that surge-supression features (if applicable) do not lead to violation of flowrate/pressure drop requirements. 3. Demonstrate by analysis that flight SW and/or on-orbit procedures will prevent operation of propulsion system beyond conditions assumed in pressure surge analyses and tests.	N/A	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	N/A	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Propulsion Branch (597)	

1.22 Purging of Residual Test Fluids

GN&C; Propulsion

Principle: Propulsion system design and the assembly & test plans shall preclude entrapment of test fluids that are reactive with wetted material or propellant.

Rationale: Residual test fluids can be reactive with the propellant or corrosive to materials in the system leading to critical or catastrophic failure.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. If test fluids are used in the assembled system, present plans for purging & drying of system.	1. Demonstrate that the method for drying the wetted system has been validated by test on an equivalent or similar system.	1. Verify dryness of wetted system by test.	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PSR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Propulsion Branch (597)	

1.24 Propulsion System Safety Electrical Disconnect

GN&C; Propulsion

Principle: An electrical disconnect "plug" or set of restrictive commands shall be provided to preclude inadvertant operation of components.

Rationale: Unplanned operation of propulsion system components (e.g. 'dry' cycling of valve; heating of catalyst bed in air; firing of thrusters after loading propellant) can result in injury to personnel or damage to components.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Present design and/or operational plan that preclude unplanned operation of propulsion system components.	1. Present detailed design of electrical disconnect and/or set of restrictive commands to preclude unplanned operation of propulsion system components.	1. Demonstrate the effectiveness of the disconnect and/or set of restrictive commands by test.	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Propulsion Branch (597)	

1.26 Safety Inhibits & Fault Tolerance

Systems Engineering; System Safety

Principle: If a system failure may lead to a **catastrophic hazard**, the system **shall** have three independant, verifiable inhibits (dual fault tolerant).
If a system failure may lead to a **critical hazard**, the system **shall** have two independant, verifiable inhibits (single fault tolerant).
Hazards which cannot be controlled by failure tolerance (e.g., structures, pressure vessels, etc.) are called "Design for Minimum Risk" (DFMR) areas of design, and have separate, detailed safety requirements that they must meet. Hazard controls related to these areas are extremely critical and warrant careful attention to the details of verification of compliance on the part of the developer.

Rationale: Adequate control of safety hazards is necessary in order to develop safe hardware and operations. Verification of independence of inhibits is necessary to preclude propagation of failure in safety inhibits that can result in critical or catastrophic threats to personnel, facility, and hardware.

Phase:	A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Identify proposed design inhibits that preclude hazardous condition and document in preliminary hazard analysis.	1. Demonstrate by analysis or component test that a) failure in selected inhibit will not cause failure of the other inhibits, or b) that no single event or software command can open multiple inhibits.	1. Demonstrate by analysis or component test that a) failure in selected inhibit will not cause failure of the other inhibits, or b) that no single event or software command can open multiple inhibits.	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR and in Preliminary MSPSP/Safety Data Package.	1. Verify at CDR and in Intermediate MSPSP/Safety Data Package.	1. Verify in Final MSPSP/Safety Data Package.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	System Reliability and Safety Office (302)	

1.27 Propulsion System Overtemp Fuse

GN&C; Propulsion

Principle: Flight fuses for wetted propulsion system components shall be selected such that overheating of propellant will not occur at the maximum current limit rating of the flight fuse. (Note: See also rule 2.06 "System Fusing Architecture.")

Rationale: Propulsion components such as pressure transducers normally draw very low current, and therefore their fuses are usually oversized. In such cases it may be possible for a malfunctioning component to overheat significantly without exceeding the rating of the fuse. Exceeding temperature limits of propellant can result in mission failure or critical/catastrophic hazard to personnel and facility.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Present fusing plan for wetted propulsion system components.	1. Demonstrate by analysis that wetted components will not exceed maximum allowable temperature of propellant at the maximum current limit rating for the flight fuse.	1. Verify by inspection of QA records that the correct flight fuse has been installed.	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PER or PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Propulsion Branch (597)	

1.28 Unintended Propellant Vapor Ignition

GN&C; Propulsion

Principle: Propulsion system design and operations shall preclude ignition of propellants in the feed system.

Rationale: Ignition of propellant vapor can occur due to a variety of conditions including (1) mixing of fuel and oxidizer in pressurant manifolds via diffusion and condensation; (2) pyrotechnic valve initiator products entering propellant manifolds; (3) adiabatic compression of gas due to pressure surges, i.e. "water hammer" effects. These conditions can cause hardware damage and/or mission failure.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Present design analysis, including pyrovalve firing sequence and/or propellant line initial pressurization, supporting mitigation of conditons for ignition of propellant vapors. 2. For bipropellant systems, demonstrate by analysis that the design provides adequate margin against diffusion and condensation of propellant vapors in common manifolds.	1. Demonstrate by analysis or test that pyrovalve firing sequence and/or propellant line initial pressurization plan will not promote conditions for ignition of propellant vapor. 2. For bipropellant systems, demonstrate by test that selected pressurant system components exhibit vapor diffusion resistance per the Phase B analysis.	N/A	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.		N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Propulsion Branch (597)	

1.29 Leakage of Hazardous Propellant

Safety, Propulsion

Principle: Propulsion systems shall be dual fault tolerant (3 independant inhibits) to external leakage of hazardous propellant, which is a catastrophic hazard. Components where fault tolerance is not credible or practical (e.g., tanks, lines, etc.) shall use design for minimum risk instead (see Gold Rule titled "**Safety Inhibits & Fault Tolerance**").

Rationale: Adequate control of propulsion safety hazards is necessary in order to develop safe hardware and operations. The internal volume between redundant inhibits (seals) shall be limited to the minimal practical volume and designed to limit the external leakage in the event of failures.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	Present compliance with range safety requirements, including required fault tolerance to hazardous events. Document in subsystem design and initial MSPSP.	Provide details of implementation of fault tolerance requirements of propulsion system. Document in subsystem design and Intermediate MSPSP.	Provide details of hazard control verifications addressing fault tolerance of propulsion system. Document in subsystem design and Final MSPSP.	N/A	N/A
Verification:	N/A	N/A	Verify at PDR.	Verify at CDR.	Verify at PSR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Propulsion Branch (597)	

1.30 Controller Stability Margins

Observatory Subsystems; GN&C

Principle: The Attitude Control System (ACS) shall have stability margins of at least 6db for rigid body stability with 30 degrees phase margin, and 12db of gain margin for flexible modes.

Rationale: Proper gain and phase margins are required to maintain stability for reasonable unforeseen changes and uncertainty in spacecraft configuration.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Identify in the Attitude Control System (ACS) Concept if the gain and phase margin requirements will be difficult to meet due to the spacecraft configuration.	1. Update the ACS concept and identify if the gain and phase margin requirements will be difficult to meet due to the spacecraft configuration.	1. Design all control modes so that the rigid body stability margins are at least 6 dB of gain margin and 30 degrees of phase margin. 2. Ensure that flexible modes have at least 12 dB of gain margin.	1. Stability analyses should include all flexible mode effects, sample data and delay effects (and other nonlinear effects such as fuel slosh) incorporated with adequate evaluation of mode shape, damping and frequency uncertainties.	1. Perform verification test and present data.	N/A	N/A
Verification:	1. GN&C and system engineering organizations verify at MCR.	1. GN&C and system engineering organizations verify at MDR.	1. GN&C and system engineering organizations verify at PDR.	1. GN&C and system engineering organizations verify at CDR.	1. Verify at PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Flight Dynamics Analysis Branch (595)	ACS Handbook

1.31 Actuator Sizing Margins

Observatory Subsystems; GN&C

Principle: The Attitude Control System (ACS) actuator sizing shall reflect specified allowances for mass properties growth.

Rationale: Knowledge of spacecraft mass and inertia can be very uncertain at early design stages, so actuator sizing should be done with the appropriate amount of margin to ensure a viable design.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. ACS actuators (including propulsion) shall be sized for the current best estimate of spacecraft mass properties with 100% design margin.	1. ACS actuators (including propulsion) shall be sized for the current best estimate of spacecraft mass properties with 50% design margin.	1. ACS actuators (including propulsion) shall be sized for the current best estimate of spacecraft mass properties with 25% design margin.	N/A	N/A	N/A
Verification:	N/A	1. At MDR, GN&C and system engineering organizations shall verify.	1. At PDR, GN&C and system engineering organizations shall verify.	1. At CDR, GN&C and system engineering organizations shall verify.	N/A	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Flight Dynamics Analysis Branch (595)	

1.32 Thruster and Venting Impingement

Systems Engineering

Principle: Thruster or external venting plume impingment shall be analyzed and demonstrated to meet mission requirements.

Rationale: Impingement is likely to contaminate critical surfaces and degrade material properties. It can also create adverse and unpredictable S/C torques and unacceptable localized heating.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Develop analytical mass transport model. 2. Update as design evolves.	1. Refine analysis based on updated designs.	1. Refine analysis based on updated designs. 2. Measure venting rates during T/V tests and verify analysis.	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mechanical Engineering and Systems Analysis Division (590)	JPL D-17868 rev. 2: 2.4.2.2.6

1.33 Polarity Checks of Critical Components

Observatory Subsystems

Principle: All hardware shall verified by test or inspection of the proper polarity, orientation, and position of all components (sensors, switches, and mechanisms) for which these parameters affects performance.

Rationale: Each spacecraft and instrument contains many components that can be reversed easily during installation. Unless close inspections are performed, and proper installations are verified by test, on-orbit failures can occur when these components are activated.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Identify all polarity-dependent components in the spacecraft design concept. 2. Ensure that design concept provides capability for testing functionality of polarity-dependent components at end-to-end mission system level, in addition to subsystem level.	1. Identify all polarity-dependent components in the spacecraft prelminary design. 2. Ensure that preliminary design provides capability for testing functionality of polarity-dependent components at end-to-end mission system level, in addition to subsystem level. 3. Develop test plan for polarity-dependent components.	1. Identify all polarity-dependent components in the spacecraft detailed design. 2. Ensure that detailed design provides capability for testing functionality of polarity-dependent components at end-to-end mission system level, in addition to subsystem level. 3. Develop test procedures for polarity-dependent components.	1. Execute polarity tests at subsystem and end-to-end mission system levels.	N/A	N/A
Verification:	N/A	1. Verify through peer review and at MDR.	1. Verify through peer review and at PDR.	1. Verify through peer review and at CDR.	1. Verify through peer review, at PER, and at PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	GN&C Systems Engineering Branch (591)	

1.34 Closeout Photo Documentation of Key Assemblies

Systems Engineering

Principle: Projects shall produce closeout photographic documentation of key assemblies during the manufacturing process and of the final integrated configuration "as flown."

Rationale: Closeout photographic documentation provides an essential record in the event of mishaps or anomalies.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Identify plan to capture closeout photographic documentation of key assemblies.	1. Update plan to capture closeout photographic documentation of key assemblies.	1. Implement plan to capture closeout photographic documentation of key assemblies.	1. Provide closeout photographic documentation of key assemblies.	N/A	N/A
Verification:	N/A	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PSR	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Office of Mission Success	

1.35 Maturity of New Technologies

Systems Engineering; Instruments

Principle: All technologies shall achieve a TRL 6 by PDR. Not applicable to technology demonstration opportunities.

Rationale: The use of new and unproven technologies requires a thorough qualification program in order to reduce risk to an acceptable level.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Identify relevant technologies, readiness levels, develop overall risk mitigation plan (including fall back to existing technologies), and conduct peer review(s).	1. Develop qualification plan for specific technologies, including risk mitigation. Peer review plan.	1. Implement qualification plan and demonstrate that TRL 6 has been achieved. Peer review qualification results.	N/A	N/A	N/A	N/A
Verification:	1. Review summary documentation at MCR.	1. Review summary documentation at MDR.	1. Review summary documentation at PDR.	N/A	N/A	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Applied Engineering and Technology Directorate (500)	

1.36 Block-Redundant Component Failure

Systems Engineering

Principle: Failure in block-redundant components shall not damage the redundant block nor prevent successful switching to the redundant block (where the primary block has failed).

Rationale: Cascading of failures can result in system being zero-fault tolerant and may lead to loss of mission.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Conduct preliminary failure modes and effects analysis (FMEA) to demonstrate that failure of primary components will not prevent successful switching to, and operation of, redundant components.	1. Conduct final failure modes and effects analysis (FMEA) to demonstrate that failure of primary components will not prevent successful switching to, and operation of, redundant components.	N/A	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	N/A	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Guidance, Navigation and Control Systems Engineering (591)	

1.37 Stowage Configuration

GN&C

Principle: When a spacecraft is in its stowed (launch) configuration, it shall not obscure visibility of any attitude sensors required for acquisition, and it shall not block any antennas required for command and telemetry.

Rationale: Establishment of spacecraft communications and acquisition of safe attitude are the two highest-priority post-separation activities, and should not be dependent on completion of deployments.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Demonstrate by inspection that mechanical subsystem concept allows for full visibility of sensors and telemetry & command antennas.	1. Demonstrate by field-of-view analysis that mechanical subsystem preliminary design allows for full visibility of sensors and telemetry & command antennas.	1.Demonstrate by field-of-view analysis that mechanical subsystem detailed design allows for full visibility of sensors and telemetry & command antennas.	1. Ensure during I&T that mechanical subsystem detailed design allows for full visibility of sensors and telemetry & command antennas.	N/A	N/A
Verification:	N/A	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Guidance, Navigation and Control Systems Engineering (591)	

1.38 Configuration Command Confirmation

Systems Engineering; CNDH

Principle: Every configuration command shall have a direct telemetry confirmation and a secondary indirect confirmation.

Rationale: Undetected failure to properly configure spacecraft could lead to premature or unsafe operations, resulting in mission failure.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Establish telemetry parameters to ensure that at least two methods can be used to verify success of each configuration command.	1. Establish go/no-go criteria to proceed with any post-configuration operations and include these in procedures for ground testing and on-orbit tests.	1. During all test operations, exercise all available methods to verify success of configuration commands.	1. During all flight operations, exercise all available methods to verify success of configuration commands.	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify at FOR and PSR	1. Verify during mission operations.	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Guidance, Navigation and Control Systems Engineering (591)	

2.01 Flight Electronic Hardware Operating Time

Electrical

Principle: One thousand (1000) hours of operating/power-on time shall be accumulated on all flight electronic hardware (including all redundant hardware) prior to launch, of which at least 200 hours shall be in vacuum. The last 350 hours of operating/power-on time shall be failure-free.

Rationale: Accumulated power-on time that demonstrates trouble-free parts performance helps reduce the risk of failures after launch.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Draft test plan	1. Approve test plan.	1. Update test plan.	1. Conduct 1000 hours of testing of all flight hardware and spares. The last 350 hours shall be trouble-free. At least 200 shall be in vacuum.	N/A	N/A
Verification:	N/A	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PSR that testing has been conducted. 2. Verify at PER that the test plan is sufficient for completion of required hours.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Office of Systems Safety and Mission Assurance (300)	GEVS 2.3.4

2.02 EEE Parts Program for Flight Missions

Electrical

Principle: A EEE parts program shall be plannned for and implemented for all flight missions for the purpose of part selection, de-rating, screening, and overall qualifications.

Rationale: Lack of comprehensive parts program may lead to parts shortages or design impacts due to unexpected long lead times or qualification status of the parts.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Address parts program and acquisition strategy for critical long lead parts in concept study.	1. Define preliminary parts plan.	1. Identify parts acquisition plan for long lead parts.	1. Prepare a detailed list of critical part(s) (including spares) and qualification plan(s).	1. Track critical parts and prepare specific risk mitigation plan(s).	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	1. Verify at MRR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electrical Engineering Division (560)	

2.03 Radiation Hardness Assurance Program

Electrical

Principle: A Radiation Hardness Assurance (RHA) Program shall be planned for and implemented for all flight missions to verify component- and system-level radiation hardness by CDR.

Rationale: Projects that ignore or underfund this discipline often discover too late that instruments/spacecraft are susceptible to radiation effects.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Include a preliminary RHA assessment in the concept study.	1. Update RHA assessment, and include resources for RHA program support in proposal.	1. Complete radiation environment analysis and assess radiation sensitivity of parts through test databases or by testing.	1. Implement radiation hardness requirements for part selection. 2. Identify mitigation plans for non-compliance. 3. Complete parts acceptability categorization. 4. Complete parts RHA qualification.	1. Implement mitigation plans. 2. Complete radiation test reports.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	1. Verify through peer review prior to start of manufacturing and at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electrical Engineering Division (560)	

2.04 Dedicated Hardware ETU and EGSE

Electrical; Systems Engineering

Principle: All new developments with components at TRL 5 or lower at Pre-Phase A shall have a dedicated hardware ETU & EGSE.

Rationale: A hardware ETU & EGSE helps reduce risk to mission performance and project execution by reducing scheduling conflicts and identifying potential problems early in a mission's lifecycle.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Identify items at TRL levels 5 or lower and define plans for ETU and EGSE.	1. Address needed resources for dedicated ETU and EGSE.	1. Begin implementation of ETU and EGSE. 2. Develop preliminary development schedule.	1. Prepare detailed development schedule utilizing dedicated ETU. 2. Build and test ETU and EGSE.	N/A	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MRR.	1. Verify at PDR.	1. Verify at CDR.	N/A	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electrical Engineering Division (560)	

2.05 System Grounding Architecture

Electrical

Principle: A system grounding concept shall be developed for all missions.

Rationale: Poor system grounding design will lead to grounding incompatibility between different systems during the integration phase, with potential degradation of end-to-end functional performance, especially for magnetic sensitive missions.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Identify a preliminary grounding concept.	1. Complete a preliminary grounding design and communicate it to all hardware developers.	1. State grounding requirements in all Electrical ICDs for the users.	1. Prepare a detailed System Grounding Document. 2. Implement the design.	1. Oversee implementation of the design. 2. Demonstrate safety, compatibility, and system performance.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify through peer review and at PDR.	1. Verify through peer review and at CDR.	1. Verify through peer review prior to TRR and at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electrical Engineering Division (560)	

2.06 System Fusing Architecture

Electrical

Principle: A system fusing architecture shall be developed for all missions, including the payloads. (See also 1.27 "Propulsion System Overtemp Fuse.")

Rationale: Lack of a system fusing design may lead to fuse incompatabilities between the power source and the payloads, which could lead to the power source fuse being blown prior to the payloads. The system fusing design should maximize the reliability of the system.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Indentify a preliminary system fusing architecture for the mission and communicate with all hardware developers.	1. Develop system fusing requirements for the mission and and state requirements in all Electrical ICDs for the users, including transient requirements.	1. Prepare a detailed System Fusing Document.	1. Oversee correct implementation of design by all users.	N/A	N/A
Verification:	N/A	1. Verify through peer review and at MDR.	1. Verify all system fusing requirments (including the payloads) through peer review and at PDR.	1. Verify user implementation at electrical systems peer peview and at CDR.	1. Verify that design verification includes fusing design prior to TRR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electrical Engineering Division (560)	

2.07 End-to-End Test of Release Mechanism for Flight Deployables

Electrical

Principle: A release mechanism test for the flight deployable components shall be performed as an end-to-end system-level test under worst-case conditions and a realistic timeline.

Rationale: Often when EGSE is used for mechanism release during I&T, potential system design problems with the release mechanisms are not detected until after the completion of the environmental program. Redesigning late in the program has many technical implications and significant cost/schedule impact.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Develop preliminary environmental test plan (with reference to end-to-end aspect of the test program).	1. Develop final environmental test plan including the end-to-end system level test and present at Peer Review.	1. Develop test procedures for the end-to-end system level test and present at Peer Review.	1. Present detailed test configuration at PER.	N/A	N/A
Verification:	N/A	1. Verify at MDR.	1. Verify through peer review and at SDR and PDR.	1. Verify at CDR.	1. Verify at PER that spacecraft circuits will be used during tests.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Office of Systems Safety and Mission Assurance (300)	GEVS 2.6.2.4.b

2.09 Spectrum Allocation Considerations

Electrical

Principle: National spectrum paperwork shall be developed for all new GSFC missions, as well as analysis of mission compliance with national and international spectrum regulations and recommendations. This will include the determination of what specific carrier frequencies should be recommended for these missions to minimize potential interference.

Rationale: NASA requires that all operating missions be in accordance with national allocations, service requirements, and authorizations, and that its satellite systems be protected against unacceptable interference from other satellite systems.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Begin work with mission to determine spectrum requirements and inform mission as to what frequency bands are available and what regulations must be met (e.g., PFD limits, OOB emissions limits).	1. Continue consultations with project, including evaluating mission design changes based on requirement to comply with national and international spectrum regulations.	1. Confirm compliance with applicable national and international regulations. 2. Determine optimal frequency within desired band, based on search of GMF and ITU databases and interference analysis. 3. If there is non-compliance, inform project and recommend changes to bring mission into compliance. If an acceptable frequency cannot be found, recommend appropriate systems modifications.	1. Validate compliance with applicable national and international regulations by performing end-to-end compatibility test.	1. If mission experiences interference while in orbit, investigate cause and recommend appropriate technical and/or regulatory remedies.	1. If mission will be operational past originally authorized date, file appropriate paperwork to ensure extension is granted.
Verification:	N/A	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PER and PSR.		

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Applied Engineering and Technology Directorate (500)	

2.10 Electronic Design for Flight Missions

Electrical

Principle: All flight mission electronics design and development shall comply with the GSFC Electronics Design and Development Guidelines 500-PG-8700.2.2.

Rationale: Applying a structured approach to the planning, execution and validation phases of a flight electronics product mitigates the risk of budget and schedule overruns, and incorporates the use of good engineering practices.

Phase:							
Activities:	1. Identify mission requirements and formulate a preliminary electrical conceptual design.	1. Collect all applicable design inputs into a requirements document. 2. Generate design planning documentation. 3. Finalize conceptual design.	1. Perform detailed design. 2. Demonstrate high risk areas through the use of breadboards, analysis and/or simulations. 3. Conduct design trade studies.	1. Build design verification platform such as an ETU, testbed, etc. 2. Demonstrate the design meets mission requirements.	1. Fabricate and assemble flight hardware. 2. Validate performance via the environmental test program. 3. Document all results properly. 4. Certify all requirements have been met.	N/A	N/A
Verification:	1.Verify at MCR.	1. Verify at SRR and MCR.	1. Verify through peer review and at PDR.	1. Verify through peer review and at CDR.	1. Verify through peer review and at PER and PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electrical Engineering Division (560)	500-PG-8700.2.2

2.11 EMI/EMC Design for Flight Missions

Electrical

Principle: All flight mission systems/subsystems shall comply with EMI/EMC requirements in GEVS Section 2.5.

Rationale: Applying a structured EMI approach to the planning, execution and validation phases of a flight electronics product mitigates the risk of budget and schedule overruns, and incorporates the use of good engineering practices.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Assess potential for EMI/EMC concerns.	1. Identify system/ subsystem components and their interfaces relative to EMI/EMC concerns. 2. Categorize system components according to known or expected noise magnitude and frequencies.	1. Using detailed electrical design, identify potential noise sources and victims as well as coupling mechanisms. 2. Perform analysis and simulations as required to assess and optimize system configuration. 3. Generate design guidelines for system and subsystems, including grounding and shielding philosophy. 4. Customize EMC test levels and configuration and publish as the EMC Test Plan.	1. Using subsystem ETU's and Test Beds, Confirm by measurement the high risk source-victim noise coupling levels. 2. Implement corrective measures as needed. 3. Verify effectiveness of corrective measures. 4. Identify mitigation strategies applicable to the flight hardware.	1. EMI Test Facility generates the EMI Test Procedure. 2. Using flight hardware, conduct environmental EMI tests to validate performance against the EMC Test Plan requirements. 3. Evaluate EMI Test Results Report for EMI compliance.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at SRR and MCR.	1. Verify through peer reviews and at PDR.	1. Verify through peer reviews and at CDR.	1. Verify through peer reviews and at PER and PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electrical Engineering Division (560)	GEVS 2.5

2.12 Printed Circuit Board Coupon Analysis

Electrical

Principle: All flight printed circuit boards (PCBs) shall be verified by coupon testing.

Rationale: Verifying the integrity of printed circuit boards reduces the risk of an on-orbit board failure, and saves the added cost of replacing flight-qualified components and reassembly if board failure occurs during qualification testing.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Provide within the conceptual study the electronic requirements that will drive mission cost, schedule, and design.	1. Update electronic requirements. 2. Include coupon verification of flight boards in mission cost and schedule estimates.	1. Update coupon evaluation requirements.	1. Finalize required PCBs.	1. Submit coupons for analysis.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	1. Verify results of all coupon testing at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electrical Engineering Division (560)	300-PG-7120.2.2B

2.13 Electrical Connector Mating

Electrical

Principle: Mating of all flight connectors which cannot be verified via ground tests, shall be clearly labeled and keyed uniquely, and mating of them shall be verified visually to prevent incorrect mating.

Rationale: Error in mating of interchangeable connectors can result in mission degradation or failure.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Identify operations that cannot be tested on the ground.	1. Present plans to prevent error in mating of electrical connectors.	1. Verify by inspection & photo documentation that electrical connectors are mated correctly.	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electrical Engineering Division (560)	

2.14 Capping of Test Points and Plugs

Flight System I&T (EED)

Principle: All test points and plugs must be capped or protected from discharge for flight.

Rationale: Capping open connectors provides protection from electrostatic discharge resulting from space charging.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Develop electrical systems requirements. 2. Identify the need for capping all open connectors and grounding the caps to chassis.	1. Develop electrical ICD stating requirement for capping open connectors. 2. Develop harness drawings.	1. Verify by inspection of build records (WOAs, traveler, etc.) that provisions for capping open connectors have been completed. 2. Verify final blanket closeout procedure includes check to verify connectors are capped.	N/A	N/A
Verification:	N/A	N/A	1. Verify through peer review and at PDR. 2. Ensure parts and materials list include connector caps.	1. Verify harness drawings include connector caps for any open connectors and their grounding provisions.	1. Inspect during pre-fairing, post fairing installation and final blanket closeouts.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Flight Systems Integration and Test Branch (568)	

2.15 Flight and Ground Electrical Hardware

Flight System I&T (EED)

Principle: The use of pure tin, cadmium, and zinc plating in flight and ground electrical hardware shall be prohibited.

Rationale: High purity tin, zinc and cadmium finishes are prone to formation of metallic whiskers which may produce an electrical shorting or contamination hazard. The current worldwide initiative to reduce the use of potentially hazardous materials such as lead (Pb) is driving the electronics industry to consider alternatives to the widely used tin-lead alloys used for plating. Pure tin, cadmium and zinc finishes renew the concern over the threat of system failures due to metallic whiskers.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Define procurement specs for EEE parts and mechanical hardware to preclude the use of pure tin, zinc and cadmium finishes (to include both external and internal finishes as well as the use of these finishes an under plates).	1. Evaluate Application Specific Risks to assess the risk of whisker induced failures. These factors include circuit geometries that are sufficiently large to preclude the risk of a tin whisker short, mission criticality, mission duration, collateral risk of rework, schedule and cost. 2. Manufacturers should provide material and chemical information on packages, solder and lead finishes of the parts manufactured for their project to document/ certify zinc, cadmium tin alloy.	1. Parts Lists should be generated for tracking potential parts application issues, and to ensure monitoring of GIDEP/Manufacturer process change notices to be aware of lead free changes at specified manufacturers. 2. Parts lists should be kept current, uploaded into the parts database, and reviewed for risk assessment. 3. Conduct EEE parts materials evaluation of each of parts list to verify that the chemical composition of the packages, lead frames, connectors and/or solder does not contain prohibited materials.	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify using the Parts List Evaluation Report prior to Launch (PER, PSR).	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Parts, Packaging and Assembly Technologies (562); Materials Engineering (541)	

2.16 Solar Arrays

Flight System I&T (EED)

Principle: Solar Arrays shall be designed in accordance with 563-PG-8700.2.2, and tested to withstand the environment to which they will be exposed. The q-panel and array shall be tested under illumination at the highest predicted operating temperature, and in accordance with AIAA S-111-2005 and AIAA S-112 -2005.

Rationale: At the time this is written, solar arrays are the least reliable component on spacecraft.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Design the array.	1. Revise the design of the array.	1. Revise the design of the array.	1. Revise the design and develop test plans for the array. 2. Write an ICD.	1. Fabricate the solar cells and solar array. 2. Test the q-panel and array under illumination at highest predicted operating temperature to AIAA S-111-2005 & AIAA S-112-2005. 3. Test the solar cells, q-panel and solar array to AIAA S -111-2005 & AIAA S -112-2005.	1. Monitor array output on an hourly basis for 48 hours subsequent to launch and on a weekly basis thereafter. 2. Check output versus predictions and reconcile.	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR. 2. Peer review the array design, applicable ICDs and test program.	1. Verify at PER, PSR.	1. Verify hourly in the 48 hours subsequent to launch, and weekly thereafter.	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Flight Systems Integration and Test (568)	

2.17 I&T Development Input

Electrical Engineering

Principle: Integration & Test discipline expertise shall be used throughout the product lifecycle.

Rationale: Projects proposed, defined or designed without adequate focus on the integration and testing process have had significant cost and schedule overruns.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Analyze system level requirements for test planning.	1. Review system level and subsystem requirements for I&T planning.	1. Review system verification and testing plans and subsystem test concepts and flow-down. 2. Formulate I&T Plan and begin facilities planning.	1. Review test plans and procedures.	1. Establish final staffing personnel. 2. Review subsystem testing and results. 3. Finalize environmental test plans. 4. Finalize test scripts and C&T database. 5. Conduct I&T per I&T Plan.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify at SDR, PDR.	1. Verify at CDR.	1. Verify at PER, PSR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Flight Systems Integration and Test (568)	

3.01 Verification and Validation Program for Mission Software Systems

Software

Principle: A thorough verification and validation process shall be applied to all mission software systems. This process shall trace customer/mission operations concepts and science requirements to implementation requirements and system design, and shall include requirements based testing of all mission elements, and end-to-end system operations scenario testing.

Rationale: Mission software, especially flight software, must be tested thoroughly to ensure a successful mission/project.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Develop first version of Operations Concept with customer. 2. Document SW functionality at high level. 3. Document SW verification and validation approach. 4. Document cost estimate for overall SW design.	1. Update Ops Concept. 2. Identify test tools to be used for software testing (fidelity, quantity). 3. Update verification and validation approach and associated cost and schedule based on updated requirements.	1. Draft Software Test Plan. 2. Draft SW traceability matrix showing SW requirements traced to parent requirements and to software components.	1. Complete SW test plan. 2. Identify verification and validation program risks. 3. Update SW traceability matrix.	1. Develop detailed test scenarios/cases. 2. Complete traceability of requirements to SW design and SW test program. 3. Execute SW test plan.	N/A	N/A
Verification:	1. Verify by inspection through peer review and at MCR.	1. Review by analysis the verification and validation approach for the mission through peer review and at MDR.	1. Verify software development and test program by analysis through peer review. 2. Verify that budget and schedule accommodate regression and end-to-end mission testing at SDR and PDR.	1. Verify by analysis at software PDR.	1. Verify by analysis at software CDR and Test Readiness Review.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Systems Integration and Engineering Branch (581)	GPR 8700.5

3.03 High Fidelity Interface Simulation Capabilities

Software

Principle: A software simulation capability shall be provided for each external interface to FSW. Both nominal and anomalous data inputs to FSW shall be configurable in real-time using the procedure language of the FSW test workstation.

Rationale: When adequate simulation capabilities aren't planned, there is severe impact to FSW development/maintenance productivity and funds.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Describe functional and performance capabilities for each flight processor external interface in technical proposal. 2. Include cost estimate.	1. Update description of required simulation capabilities to reflect any changes in requirements since previous phase. 2. Document acquisition strategy for acquiring simulation capabilities, including responsible organizations.	1. Update requirements to reflect any changes since previous phase. 2. Deliver flight software external interface test tools to FSW team.	1. Maintain FSW external interface test tools.	N/A	N/A
Verification:	N/A	1. Verify by observation at MDR.	1. Verify by observ. at SW SRR. 2. Verify flight sim. capabil. defined to accommod. test of all FSW data I/O, FSW modes, nominal & anomalous conditions & load/stress tests for each flight CPU. 3. Verify sim. develop. & FSW schedules consistent	1. Verify by observation at software CDR.	1. Verify by observation at MOR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Flight Software Branch (582)	

3.04 T&C System Selection Trade Study for Operations Ground System

Mission Operations

Principle: An engineering trade analysis shall be performed on the selection of the flight operations telemetry and command (T&C) system. This analysis shall define the benefits, costs, and risks associated with each candidate system. The trade shall explicitly address potential reuse of the I&T T&C system, as well as the use of government-provided versus commercial systems.

Rationale: The selection of the flight operations T&C system is one of the most important decisions made by the ground system implementation team. There are several systems available that generally could meet the ground system requirements, but each will provide its own benefits and drawbacks. A thorough engineering trade analysis will help ensure the best system is selected for the mission.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Begin early stages of the trade study to evaluate the candidate systems. The study should identify the factors and characteristics of the mission that will have the greatest influence on the trade.	1. Update trade study. At minimum, trade shall address potential reuse of I&T products in ops, approach for developing & validating ops products (e.g., procedures & data-bases), configuration and maintenance costs, history of candidate systems providing ops support, & potential to use ops system for I&T. 2. For in-house missions, trade study shall also assess impacts to FSW develop./test & I&T if ops T&C sys. different than default FSW & I&T system.	1. Complete the trade study. 2. Make a decision on operations T&C system. This is needed to provide a reference architecture within which ground system requirements are defined and cost estimates are solidified.	N/A	N/A	N/A	N/A
Verification:	1. Verify at MCR that trade is adequate.	1.Verify at MDR that trade addresses above and other appropriate items.	1. Verify at PDR that the trade study is completed and demonstrates a thorough analysis that justifies the decision .	N/A	N/A	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Systems Integration and Engineering Branch (581)	

3.05 Flight / Ground System Test Capabilities

Ground System; Mission Operations

Principle: Flight system interface and functional capabilities shall be provided to support ground system development and test, and flight operations development, test and training. These capabilities shall be provided via a combination of one or more spacecraft simulators and the actual spacecraft. The spacecraft capabilities, access time, and schedule required to support ground system/operations development and test shall be defined by and negotiated with the ground system and operations teams.

Rationale: The ground system must be compatible with the S/C it is being designed to support, and this must be proven prior to launch via tests. Similarly, the ops team must be able to develop and validate a variety of operations products, such as procedures, databases, display pages, and launch scripts. The ops team must also have opportunities to learn about operating the S/C and prove this knowledge has been acquired prior to launch.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Develop plans for providing the flight system interfaces for use by the ground sytsem and flight operations teams.	1. Develop preliminary simulation concepts.	1. Generate preliminary simulator requirements and identify long lead procurement items. 2. Incorporate the agreements on simulator and spacecraft access time into the I&T schedule.	1. Complete simulator requirements, design, and delivery plan/schedules. 2. Ensure simulator and spacecraft access times are integrated into the detailed I&T schedule.	1. Provide simulator and S/C hardware access for both ground system verification and validation, and for ops teams to prepare for launch. 2. Ensure S/C and instrument design changes are accommodated by simulator updates as appropriate. 3. Ensure plan & budget are in place to maintain simulators post-launch.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	1. Verify at MOR that plan for simulator use is described. 2. Verify at FOR that plan and schedule for simulator maintenance is in place.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Systems Integration and Engineering Branch (581)	

3.06 Dedicated ETU for Flight Software (FSW) Testing

Software

Principle: An ETU flight data system testbed shall be dedicated to FSW teams specifically for FSW development and test. Such ETUs are supplemented by external interface simulators as specified in Rule 3.03. Hardware and I&T teams shall not plan to use the FSW ETUs for their critical path schedule. The number of flight data system testbed units shall be sufficient to support the FSW development schedule and the overall mission schedule.

Rationale: Early investment in dedicated FSW testbed hardware fidelity saves costs and avoids significant schedule risks to FSW and I&T teams. Anything less than a dedicated ETU will add to mission risk and threaten cost/schedule.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Define high-level ETU requirements for FSW with clear and detailed rationale.	1. Update ETU requirements from Phase A. 2. FSW team ensure that ETU development and delivery schedule is consistent with FSW development team need dates. 3. FSW team develop ETU acceptance criteria for ETU deliveries.	1. Review ETU design. 2. Review ETU delivery schedule.	1. FSW team verify availability of ETUs to meet FSW development and test schedules. 2. FSW team lead accept ETU deliveries and verify functionality.	1. FSW team review and provide inputs on ETU maintenance plan.	N/A
Verification:	N/A	1. Verify by observation at MDR that ETU quality FSW test beds are clearly represented in the technical proposal, and that costs for dedicated FSW testbed ETUs are included in the electronics cost proposal.	1. Verify by observ. at SDR & SW SRR that a) FSW ETU testbed (s) represent maturing flight architecture; b) min. 1 test bed w/ full ETU fidelity costed & deliv. sched. consis. w/ FSW needs; c) I&T plans minimize shar-ing ETU, or dedicated ETU provided.	1. Verify by observation at SW PDR that a) deliv. plans for ETU-quality FSW testbed(s) consistent w/ FSW develop. needs; b) I&T plans require minimal use of a shared ETU, or I&T have own dedicated ETU.	1. Verify by observ. at SW CDR that a) ETU-quality FSW testbed(s) have been delivered to FSW team; b) ETU FSW testbed confirmed adequate by FSW staff for on-orbit maintenance and ops support.	1. Verify by observ. at FOR that a) FSW ETU testbeds have been moved to their long-term environ. for FSW maint. & ops support; b) Sys. Admins, facility and hardware support are in place.	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Flight Software Branch (582)	

3.07 Flight Software Margin Warnings

Software

Principle: Flight software development teams shall adhere to the resource margins specified in Table 3.07-1.

Rationale: Early and repeated attention by flight software teams to resource utilization will improve resource margins for future phases of the mission.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Establish clear rationale for FSW resource estimates using the proposed hardware.	1. Update software margins based on updated requirements. 2. Coordinate with S/C and instrument procurement and hardware development teams to ensure margins can be maintained.	1. Design FSW within defined design margins. 2. Continue coordination with S/C and instrument hardware development teams.	1. Track development to design margins. 2. Report systems not able to maintain margins. 3. Provide mitigation plans or work-arounds for margins that are not being maintained.	N/A	N/A
Verification:	N/A	1. Verify by observation at MDR.	1. Verify by observation at SDR and FSW SRR.	1. Verify by observation at Mission CDR and FSW PDR.	1. Verify by observation at FSW CDR and PER.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Flight Software Branch (582)	

Table 3.07-1 Resource Margins for Flight Software Development

The numbers in the table below are margins for different mission phases and maturity levels. These do not represent hard limits, but levels where the software development team should start to get concerned. Project waivers are not required unless the resource starvation means the system can't meet one of its requirements.

Margin is calculated using the formula: (available resource – estimated usage of resource) / available resource.

Mission Phase	FSW SRR	FSW PDR	FSW CDR	Ship/Flight
Method	Estimate	Analysis	Analysis/ Measured	Measured
Average CPU	50%	50%	40%	30%
CPU Deadlines	50%	50%	40%	30%
PROM	50%	30%	20%	0%
EEPROM	50%	50%	40%	30%
RAM	50%	50%	40%	30%
PCI Bus	75%	70%	60%	50%
1553 Bus	30%	25%	20%	10%
Spacewire (1355)	TBD	TBD	TBD	TBD
UART/Serial I/F	50%	50%	40%	30%

3.07-1 Flight Software Margin Table

Selecting which column to use at a particular time is not always obvious. Generally, one should pay more attention to the "Method" row than the "Mission Phase" row. For example, if there is a lot of re-use and you have actual measured code sizes for most modules, your PROM could be 80% full at PDR without causing concern. Different resource elements can be at different maturity levels at any given point in a project. The right-most column should only be used when the code is fully integrated <u>and tested</u>. Those are the margins we want to save for in-flight maintenance.

Average CPU Utilization: This should be estimated/measured over about a five second interval under the worst-case normal operating conditions. The numbers represent the percentage of time the CPU is doing non-background processing work. Background processing may include tasks such as memory scrubbing or table check summing if those tasks have very loose timing requirements.

Deadlines: This is the fine-scale companion to the row above. This row usually represents the interrupt timing requirements of the system. For example: How quickly does the processor need to re-fill that FIFO after the HW interrupt is asserted? If you have a 50ms deadline for an ISR and you estimate the processor can meet it in 20ms, your usage (margin) is 40%(150%). If that same ISR occurs twice per second, it would only add 4% to the CPU usage calculation. All deadlines in the system should be considered, and compared individually to the recommended margin. Also, consider which deadlines can occur simultaneously to calculate the worst-case timing.

PROM is non-volatile memory that cannot be modified in flight.

EEPROM is non-volatile memory that can be modified in flight.

RAM is volatile memory where the executing code and data are stored. This memory is always on the processor's local bus.
Note: Bulk memory used for storage of housekeeping and science data has been removed from this table. The amount of bulk memory is driven more by mission parameters (data rates, number of ground contacts, etc) than software design. So, systems engineers should track the bulk memory margin. However, some systems have the "bulk" memory on the processor card, indistinguishable from regular RAM. In this case, the software team should track margins on this combined RAM/bulk memory space.

1553 Bus: Usage calculations should include 1 retry for each transaction, unless mission requirements specify otherwise. If the scheduling of bus traffic is segmented into slots or channels, the usage should be calculated based on the number of slots used (rather than actual bus time).

Spacewire: Under development.

Other Data Busses: For busses and interfaces not listed, try to select the one that is closest in behavior among the listed busses. If none is even close, work with your systems engineer to define acceptable margins for that unique bus. Then, we can add that new bus to the table.

3.09 Software Development Approach

Software

Principle: Acquisition and development of software shall be performed in accordance with the requirements of NPR 7150.2. GSFC in-house developments shall use practices documented in GSFC GPR-8700.5 and reflected at the software.gsfc.nasa.gov website. Out of house development efforts shall be assessed against these same criteria during an independent software peer review which shall include peers fully familiar with the requirements of GSFC GPR-8700.5 and the software.gsfc.nasa.gov website.

Rationale: External organizations will often apply pressure to software teams to abandon good engineering practices to reduce costs and/or improve schedule. However, the consistent application of sound and proven discipline engineering practices throughout the life cycle greatly facilitates meeting cost, schedule and quality expectations while managing risk. Sound discipline practices provide the best assurance of developing the right products on schedule and within costs.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Review NPR 7150.2 and GPR referenced above. 2. Scope software plans.	1. Develop and execute software acquisition strategy. 2. Classify software products based on mission criticality. 3. Develop software contents of RFPs and proposals. 4. Draft software cost estimates.	1. Develop Software Management Plan, CM Plan, Test Plan and Software Requirements as described in NPR 7150.2 and at above website. 2. Complete compliance matrix for NPR 7150.2.	1. Document software development and test plans and adhere to the documented plans and practices. 2. Set up software test environment.	1. Software development, test and deliveries adhere to the documented Plans and practices. 2. Software Maintenance Plan is developed to be consistent with the above website.	1. Software maintenance and test adhere to the documented plan and practices.	N/A
Verification:	1. Verify by observation at MCR that new business plans reflect the intent to follow the above standard.	1. Verify by observation at MDR that a) SW plans are consistent with formulation and applicable requirements in NPR 7150.2. 2. Perform "Quick Look Review" of the proposed software plan.	1. Verify by observation at SW SRR that a) SW Plans and requirements documentation are consistent with GPR and NPR; b) any waiver requests have been thoroughly evaluated.	1. Verify by observation at Mission CDR and Software PDR.	1. Verify by observation at Software CDR and Mission FOR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Flight Software Branch (582)	http://software.gsfc.nasa.gov

3.10 Flight Operations Preparations and Team Development

Mission Operations; Software; Systems

Principle: Mission preparation tests shall require a minimum of 2 successful end-to-end tests (to include launch and early orbit simulations), and 2 day-in-the-life simulations, and a minimum of 200 hours with the flight ops team running the flight system. Flight operators shall participate as test conductors during integration and test (I&T) at a minimum as specified in the tests above.

Rationale: Using flight operators as test conductors gives them a great deal of real, hands-on experience with the observatory prior to launch without requiring as much time dedicated to FOT training and simulations during operations. Involving the FOT early in the mission helps ensure that the mission design will be considerate of operational requirements and practicalities, and will allow the FOT to become intimately familiar with the mission design, including design rationale.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Assess the flight operations team's role throughout the mission lifecycle. Flight operations experts review the operations concept.	1. Flight operations and software experts support the development of operations concepts and flight/ground architecture. 2. Update mission design estimates.	1. Identify candidate FOT members. 2. Review and update operations concepts and identify details on approach to operations team support. 3. Conduct peer review flight/ground architecture for soundness.	1. Involve FOT in test plan development. Support the completion of the operations concept.	1. Ensure all FOT members are assigned as test conductors during I&T. 2. Ensure all FOT members gain knowledge & experience on ground system during I&T. 3. Prior to launch, require a min of 2 successful end-to-end tests (to include launch & early orbit sims) and 2 day-in-the-life sims, and a min of 200 hrs w/ flight ops team running flight sys 4. Complete flight ops plan.	N/A	N/A
Verification:	1. Verify at MCR: a) Ensure flight development experts were consulted during mission formulation. b) Ensure that operations concept covers flight ops team's role during entire mission lifecycle.	1. Verify at MDR: a) Flight operations concepts are sound. b) Inquire about project coordination with the flight software organization.	1. Verify at PDR: a) Flight operations personnel are identified. b) Flight and ground system interfaces are well defined.	1. Verify at CDR: a) Flight ops experts have been consulted on the overall system design. b) FOT will provide test conductors during I&T. c) The project has completed full mission life cycle design.	1. Verify at MOR and FOR: a) Members of FOT are serving as test conductors during I&T. b) Test items above were completed at MRR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Systems Integration and Engineering Branch (581)	

3.11 Long Duration And Failure Free System Level Test of Flight Software

Software

Principle: Ground test of the fully integrated FSW system shall include demonstration of error free operations-like scenarios over an extended time period. The minimum duration uninterrupted FSW system-level test (on the highest fidelity FSW testbed) is 72 hours for Class A and B, 48 hours for Class C, and 36 hours for Class D missions, respectively.

Rationale: Frequent restart of FSW during ground tests may mask problems which will only occur following extended execution of the FSW.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	N/A	1. Develop FSW Test Plan.	1. Complete and execute FSW Test Plan, to include long duration FSW testing.	N/A	N/A
Verification:	N/A	N/A	N/A	1. Verify at PDR that FSW Test Plan is baselined and that it includes long duration testing.	1.Verify at MOR: a) The longest duration, uninterrupted FSW system-level test (on the highest fidelity FSW testbed) has been completed. b) Verify that long duration tests were minimally between 36 and 72 hrs. c) Verify that realistic post-launch science operations and safe - hold operations were represented by the long duration test(s).	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Flight Software Branch (582)	

3.12 Visibility of Spacecraft State

Software

Principle: Onboard telemetry and downlink priorities shall be defined to unambiguously report the state of the spacecraft and instruments to underground operators early in each ground tracking pass - specifically identifying any faults experienced.

Rationale: Immediate ground attention to anomalous spacecraft status at the start of a ground contact provides the greatest opportunity for ground reaction, if necessary, during this same ground pass.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Develop requirements and operations concept. 2. Complete preliminary design.	1. Update requirements and operations concept. 2. Update design.	1. Define on-board events and telemetry. 2. Establish priorities for downlink of onboard data. 3. Test and verify implementation.	N/A	N/A
Verification:	N/A	N/A	1. At PDR: a) Verify overall s/c & instrument states of health; characteristics of critical onboard anomalies are the first downlink of each ground contact during all mission phases and anomalous conditions. b) Verify same during minimum telemetry bandwidth conditions.	1. At CDR: a) Verify overall s/c & instrument states of health; characteristics of critical onboard anomalies are the first downlink of each ground contact during all mission phases and anomalous conditions. b) Verify same during minimum telemetry bandwidth conditions.	1. Verify above items at FOR. 2. Verify at MOR: a) Overall s/c & instrument states of health ; characteristics of critical onboard anomalies are the first downlink of each ground contact during all mission phases and anomalous conditions. b) Verify same during minimum telemetry bandwidth conditions.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Owner: Flight Software Branch (582)	

3.13 Operational Software Redundant Element

Software

Principle: The updating of code/software should be limited to a single target memory device under user ground control and monitoring. Under no circumstances shall prime and redundant memories be modified concurrently, or before the operational performance of the change is properly assured in a single unit.

Rationale: Prevents inadvertent updates of the backup element from the primary element. Ensures that the ground system can update each element without dependence on any of the other elements.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	N/A	1. Ensure system level design does not allow modification of software between one CPU and its redundant elements.	N/A	N/A	N/A
Verification:	N/A	N/A	N/A	1. Verify at CDR.	N/A	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Real-Time Software Engineering Branch (584)	

3.14 Command Procedure Changes

Software

Principle: Command procedures and mission databases (on-board and ground) shall be controlled (treated with the same rigor as changes to flight critical software). This includes formal configuration management, peer review by knowledgeable technical personnel, and full verification with up-to-date simulations wherever possible. (Routine loads to perform nominal operations may require less test rigor.)

Rationale: Changes in command procedures and critical database areas that are not tracked, controlled, and fully tested can cause loss of science and/or the mission.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Ensure draft CM Plans address items defined in this rule.	1. Ensure that the final CM and Test Plans address the items defined in this rule. 2. Ensure that the Ops Plan and Sustaining Eng Plan address the items defined in this rule.	1. Perform routine maintenance.	N/A	N/A
Verification:	N/A	N/A	1. Verify at CDR.	1. Verify at CDR.	N/A	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Real-Time Software Engineering Branch (584)	

3.15 Test and GSE Software Interfaces

Flight Systems I&T, Software

Principle: Test and GSE (Ground Support Equipment) software that interfaces with or evaluates flight software and hardware shall be acceptance tested before testing with FSW and flight hardware.

Rationale: Test and GSE software are used to test critical flight software and hardware and, in doing so, may cause damage to flight hardware if not developed and tested in a rigorous manner.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Identify test and GSE software functions needed for GSE and flight software testing. 2. Ensure software development costs/ schedule include critical testing of test and GSE software.	1. Ensure that the final CM and Test Plans address the items defined in this rule. 2. Ensure that the Ops Plan and Sustaining Eng Plan address the items defined in this rule.	1. Perform routine maintenance.	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify at FSW CDR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Flight Systems Integration and Test (568); Real-Time Software Engineering (584)	

4.01 Contamination Control, Planning, and Execution

Mechanical

Principle: Specific contamination control requirements and processes (such as analytical modeling, laboratory investigations, and contamination protection and avoidance plans) that support mission objectives shall be identified.

Rationale: Contamination sensitive components are often critical elements that directly affect system performance. It is essential that critical component performance be preserved and not allowed to degrade due to contamination exposure & accumulations.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Provide within the conceptual study the preliminary contamination control requirements that will drive mission cost, schedule, and design.	1. Update requirements and develop control methodologies. 2. Write draft Contamination Control Plan (CCP) to document cost, schedule, and design requirements.	1. Update CCP as mission and design details evolve.	1. Finalize CCP. 2. Implement appropriate elements of CCP in fabrication.	1. Implement all elements of the CCP.	1. Monitor system performance for evidence of contamination related degradation and prepare mitigation plans if necessary.	N/A
Verification:	1. Verify above at MCR.	1. Verify through peer review, proposal team, and at MRR.	1. Verify through peer review and at MDR.	1. Verify that CCP is under formal configuration control. 2. Verify through peer review and at PDR and CDR.	1. Verify through peer review.	1. Verify mitigation plan at ORR.	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mechanical Systems Division (540)	GEVS 2.7

4.03 Structural Analysis and Design Factors of Safety

Mechanical

Principle: Structural analysis and design factors of safety shall apply to all systems in accordance with GEVS Section 2.2.5.

Rationale: This will provide confidence that the hardware will not experience failure or detrimental permanent deformation under test, ground handling, launch, or operational conditions.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Employ design factors of safety in accordance with GEVS 2.2.5.	1. Employ design factors of safety in accordance with GEVS 2.2.5.	1. Employ design factors of safety in accordance with GEVS 2.2.5.	1. Employ design factors of safety in accordance with GEVS 2.2.5.	N/A	N/A
Verification:	N/A	1. Verify that factors of safety are defined at MDR.	1. Verify that factors of safety are defined at SDR and PDR.	1. Verify that factors of safety are defined at CDR.	1. Verify that factors of safety are being met at PER and PSR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Mechanical Systems Division (540)	GEVS 2.2.5

4.06 Validation of Thermal Coatings Properties

Mechanical

Principle: All thermal analysis shall employ thermal coatings properties validated to be accurate for materials and mission flight parameters over the lifecycle of the mission.

Rationale: Thermal coatings properties directly affect mission success through S/C or instrument thermal design.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Determine appropriate BOL and EOL coatings properties to be used in the thermal analysis.	1. Update thermal coatings properties as coatings selection matures.	1. Update thermal coatings properties as coatings selection matures. 2. Measure coatings properties when appropriate.	N/A	N/A
Verification:	N/A	N/A	1. Verify through peer review and at PDR.	1. Verify at CDR.	1. Verify at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Thermal Engineering Branch (545)	Coatings Handbook (future)

4.07 Solder Joint Intermetallics Mitigation

Mechanical

Principle: All materials at a solder joint shall be selected to avoid the formation of potentially destructive intermetallic compounds.

Rationale: Solder joints can be significantly weakened by excessive intermetallic formations. Particularly destructive is the formation of gold-tin intermetallics which are brittle and change the conductivity of the joints. Substrates to be joined using a soldering process should be selected to mitigate the formation of these compounds.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Substrates and processes shall be selected to avoid the formation of excessive intermetallics. Use of gold coated substrates shall be carefully monitored to keep gold concetration in joint below 5% by weight.	1. Test representative samples of joint materials to assure compatibility.	1. Practices to mitigate the intermetallic formations in solder joints shall be considered if incompatible substrates can't be avoided.	1. Monitor system performance for evidence of potential solder joint-related failures. Use these data to refine solder joint substrate requirements for future missions.	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PER.	1. Document lessons learned.	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Materials Engineering Branch (541)	

4.08 Space Environment Effects on Material Selection

Mechanical

Principle: Thorough evaluation of the environmental effects of the trajectory paths/orbits shall be assessed for the impact on materials selection and design.

Rationale: Understanding the trajectory and orbital environmental effects (e.g., ESD, radiation, Atomic Oxygen, etc.) on the spacecraft will eliminate costly redesign and fixes, as well as minimize the on-orbit failures due to environmental interaction with spacecraft materials.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Orbit and life requirement information shall be used by MAE to assure compatibility of material selections.	1. Refine materials compatibility analysis.	1. Review preliminary M&P list for environmental compatibility. Effects to be considered should include but not be limited to ESD, thermal effects, radiation, atomic oxygen, and orbital debris. As appropriate, environmental simulation tests shall be conducted to characterize material compatibility.	1. Review updated M&P list for environmental compatibility. Continue material testing as appropriate.	1. Review updated M&P list for environmental compatibility. Continue material testing as appropriate.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Materials Engineering Branch (541)	

4.09 Mechanical Test Factors and Duration

Mechanical

Principle: The project shall employ the mechanical test factors and durations in accordance with Section 2.2.4 of GEVS.

Rationale: Using minimum recommended test durations and factors developed over years of development experience will increase confidence in test adequacy and verification status.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	N/A	1. Formulate test plans for all structural elements incorporating the requirements described in the principle.	1. Write test plans and execute tests.	N/A	N/A
Verification:	N/A	N/A	N/A	1. Verify at CDR.	1. Verify at engineering peer reviews, PER, and PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mechanical Systems Analysis and Simulation Branch (542)	GEVS SE 2.2.4

4.10 Minimum Workmanship

Mechanical

Principle: All electrical, electronic, and electro-mechanical components shall be subjected to minimum workmanship test levels as specified in GEVS Section 2.4.2.5.

Rationale: The workmanship levels defined in GEVS Section 2.4.2.5 have been found to be the minimum input level necessary to adequately screen aerospace electronic hardware for workmanship flaws.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Envelop minimum workmanship levels when deriving component random vibration test levels.	1. Envelop minimum workmanship levels when deriving component random vibration test levels.	1. Envelop minimum workmanship levels when deriving component random vibration test levels.	N/A	N/A
Verification:	N/A	N/A	1. Verify that component test levels envelop minimum workmanship.	1. Verify that component test levels envelop minimum workmanship.	1. Verify that components have been adequately screened for workmanship.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mechanical Systems Analysis and Simulation Branch (542)	GEVS Section 2.4.2.5

4.11 Testing in Flight Configuration

Mechanical

Principle: Mechanical environmental testing (sine, random & acoustic) of flight hardware shall be performed with the test article in appropriate (e.g. launch, landing, etc.) configuration. Hardware that is to be powered on for launch shall be powered on for testing.

Rationale: Testing in-flight configuration ensures that hardware that is difficult to analyze (i.e. blankets, harnesses, mechanisms) will be adequately screened by environmental testing for design or workmanship flaws.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	N/A	1. Develop plans necessary to allow testing of hardware in flight configuration.	1. Perform testing in flight configuration.	N/A	N/A
Verification:	N/A	N/A	N/A	1. Verify that appropriate planning has been performed to conduct test in flight configuration.	1. Verify that testing has been performed with the test article in flight configuration.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mechanical Systems Analysis and Simulation Branch (542)	GEVS Sections 2.4.2, 2.4.3, 2.4.4

4.12 Structural Proof Testing

Mechanical

Principle: Primary and secondary structures fabricated from nonmetallic composites, beryllium, or containing bonded joints or bonded inserts shall be proof tested in accordance with GEVS Section 2.4.1.4.1.

Rationale: The mechanical strength of the above items is dependent on workmanship and processing and can only be verified by proof testing.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Identify structure requiring proof testing.	1. Develop test methods and plans for performing proof testing.	1. Perform proof testing to verify mechanical strength.	N/A	N/A
Verification:	N/A	N/A	1. Verify that all structural elements requiring proof testing have been identified.	1. Verify that approach for proof testing appropriate structural elements has been defined.	1. Verify that proof testing has been performed.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mechanical Systems Analysis and Simulation Branch (542)	GEVS 2.4.1.4.1

4.13 Modal Survey Characterization

Mechanical

Principle: A modal survey shall be performed for flight hardware that has modes in the frequency range as specified in GEVS Section 2.4.1.2.

Rationale: Modal surveys are invaluable tools in the process of validating computer model analysis of structures. They are essential elements of any verification process.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Include modal survey in the verification plan and verification matrix for all appropriate structural elements.	1. Formulate test plans describing appropriate modal survey techniques for structural elements.	1. Write test procedures and conduct modal surveys.	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PER and PSR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Mechanical Systems Analysis and Simulation Branch (542)	GEVS 2.4.1.2.

4.14 Structural Qualification

Mechanical

Principle: Structural tests that demonstrate that flight hardware is compatible with expected mission environments shall be conducted in compliance with GEVS 2.4.

Rationale: Demonstration of structural requirements is a key risk reduction activity during mission development.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Develop outline of structural qualification methodology.	1. Update structural qualification methodology and develop preliminary strength qualification plan.	1. Develop draft structural qualification methodology and plan.	1. Finalize structural qualification plan. 2. Implement plan.	1. Demonstrate that flight hardware supports expected mission environments and complies with specified verification requirements.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify that plan is under configuration control. 2. Verify through peer review and at PDR.	1. Verify through CDR peer review and at CDR.	1. Verify at PER and PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mechanical Engineering Branch (543)	GEVS Sections 2.4.2, 2.4.3, 2.4.4

4.15 Torque Margin

Mechanical

Principle: The Torque Margin (TM) requirement defined in GEVS section 2.4.5.3 shall apply to all mechanical functions, those driven by motors as well as springs, etc. at beginning of life (BOL). End of Life (EOL) mechanism performance shall be determined by life testing, and/or by analysis; however, all torque increases due to life test results and/or analysis shall be included in the final TM calculation and verification. Margins shall include all flight drive electronics effects and limitations.

Rationale: This torque margin requirement relates to the verification phase of the hardware in question. Conservative decisions should be made during the design phase to ensure adequate margins are realized. However, it is recognized that under some unique circumstances these specified Factors of Safety (FOS) might be detrimental (excessive) to the design of a system. For specific cases that require approval of a waiver, appropriate FOS shall be determined based on design complexity, engineering test data, confidence level, and other pertinent information.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Identify and create a plan for determination and implementation for Torque Margin verification.	1. The Torque Margin (TM) shall be calculated per the guidelines in GEVS Section 2.4.5.3 using PDR Factors of Safety. Identify basis for input to analysis.	1. The Torque Margin (TM) shall be calculated per the guidelines in GEVS Section 2.4.5.3 using CDR Factors of Safety. Identify basis for input to analysis. 2. Present all available engineering test data used for these analyses.	1. The Torque Margin (TM) shall be Calculated per the guidelines in GEVS Section 2.4.5.3 using Post Acceptance / Qualification Factors of Safety.	1. Monitor system performance for evidence of mechanism degradation. Use this data to improve future design approaches. 2. Prepare mitigation plan to extend the life of the mission if degradation becomes evident.	N/A
Verification:	N/A	1. The Torque Margin Plan shall be presented at MDR as part of the analysis and verification process.	1. Present TM analysis at PDR.	1. Present TM analysis at CDR.	1. Present final test verified TM analysis at PSR. Identify basis for input to analysis. Present all available hardware verification test data used for these analyses.		N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Mechanical Engineering Branch (543)	GEVS (Rev B Draft) 2.4.5.3

4.18 Deployment and Articulation Verification

Mechanical

Principle: All flight deployables, movable appendages, and mechanisms shall demonstrate full range of motion and articulation under worst-case conditions prior to flight.

Rationale: Environmental factors such as temperature, gravity, acceleration fields, wire bundle stiffness, and others can adversely effect successful deployment. Verification of these systems under worst-case conditions will improve on-orbit success.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Include articulation in the verification plan and verification matrix.	1. Analyze design and use environment to determine worst case deployment conditions. 2. Demonstrate that all deployable system test plans include provisions to verify deployment under worst case conditions.	1. Update worst case analysis and test plans. 2. Write test procedure(s). 3. Conduct tests.	N/A	N/A
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify worst case condition analysis and test plans/ procedures through engineering peer review and at CDR.	1. Verify test procedures and test results through engineering peer reviews, and at PER and PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Mechanical Engineering Branch (543)	

4.20 Fastener Locking

Mechanical

Principle: All threaded fasteners shall employ a locking feature.

Rationale: If not locked in the torqued, preloaded position, threaded fasteners subjected to vibration and thermal cycling loads will tend to relieve their preload and potentially jeopardize the mission.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	N/A	1. Review all design drawings and specifications to assure all fastners employ an appropriate locking feature.	1. Inspect all threaded fastener-related assemblies to verify that the specified locking feature has been properly applied.	N/A	N/A
Verification:	N/A	N/A	N/A	1. Verify at CDR.	1. Verify at PER and PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electromechanical Systems Branch (544)	

4.22 Precision Component Assembly

Mechanical

Principle: When precise location of a component is required, the design shall use a stable, positive location system (not relying on friction) as the primary means of attachment.

Rationale: When in the domain of arc-sec to sub-arc-sec location requirements, the use of pinning or similar non-friction reliant method will help ensure alignment is maintained through all expected stresses.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Begin to identify potential high precision interfaces.	1. Refine identification of high precision interfaces.	1. Identify methodology for precise location attachment.	1. Design and document attachment methods.	1. Inspect assemblies to assure specified attachment techniques are properly applied.	N/A	N/A
Verification:	N/A	N/A	1. Verify through peer review and at PDR.	1. Verify through peer review and at CDR.	1. Verify through peer review and at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electromechanical Systems Branch (544)	

4.23 Life Test

Mechanical

Principle: A life test shall be conducted, within representative operational environments, to at least 2x expected life for all repetitive motion devices with a goal of completing 1x expected life by CDR.

Rationale: Reliability of electro-mechanical systems can have serious mission success implications. Documented life testing must be performed which demonstrate performance requirements for mission life. Life tests must consider the flight drive electronics effects and limitations.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	1. Develop a life test outline for all repetitive motion devices.	1. Develop draft life test plan.	1. Finalize plan and implement.	1. Present life test conclusions and compare to mission performance requirements.	N/A	N/A
Verification:	N/A	1. Verify at MDR.	1. Verify that plan has been drafted at PDR.	1. Verify plan and any existing life test data.	1. Verify life test results at PER and PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electromechanical Systems Branch (544)	GEVS 2.4.5.1

4.24 Mechanical Clearance Verification

Mechanical

Principle: Verification of mechanical clearances and margins (e.g. potential reduced clearances after blanket expansion) shall be performed on the final as-built hardware.

Rationale: Proper mechanical clearances are often critical to successful on-orbit performance (e.g. free-movement area, thruster impingment, FOV, etc.). Verification through analysis and drawing checking alone is not sufficient to properly demonstrate adequate clearance.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	N/A	1. Demonstrate that mechanical integration plans include provisions for verifying mechanical clearences at appropriate integration milestones. 2. Conduct inspections and measurements.	1. Demonstrate that mechanical integration plans include provisions for verifying mechanical clearences at appropriate integration milestones. 2. Conduct inspections and measurements.	N/A	N/A
Verification:	N/A	N/A	N/A	1. Verify at CDR.	1. Verify at PER and PSR.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Electromechanical Systems Branch (544)	

4.25 Thermal Design Margins

Mechanical

Principle: Thermal design shall provide adequate margin between stacked worst-case flight predictions and component allowable flight temperature limits. Note: This applies to normal operations and planned contingency modes. This does not apply to cryogenic systems.

Rationale: Positive temperature margins are required to account for uncertainties in power dissipations, environments, and thermal system parameters.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Thermal design concept produces minimum 5C margins, except for heater controlled elements which have a maximum 70% heater duty cycle, and two-phase flow systems which have a minimum 30% heat transport margin. For Pre-A, larger margins advisable.	1. Thermal design concept produces minimum 5C margins, except for heater controlled elements which have a maximum 70% heater duty cycle, and two-phase flow systems which have a minimum 30% heat transport margin. For Phase A, larger margins advisable.	1. Thermal design concept produces minimum 5C margins, except for heater controlled elements which have a maximum 70% heater duty cycle, and two-phase flow systems which have a minimum 30% heat transport margin.	1. Thermal design concept produces minimum 5C margins, except for heater controlled elements which have a maximum 70% heater duty cycle, and two-phase flow systems which have a minimum 30% heat transport margin.	1. System thermal balance test produces test-correlated model. Test and worst-case flight thermal analysis with test-correlated model demonstrate minimum 5C margins, except for heater controlled elements which demonstrate a maximum 70% heater duty cycle, and two-phase flow systems which demonstrate a minimum 30% heat transport margin.	1. Thermal analysis with flight-correlated model shows minimum 5C margins for mission trade studies, except for heater controlled elements which have a maximum 70% heater duty cycle, and two-phase flow systems which have a minimum 30% heat transport margin.	1. Thermal analysis with flight-correlated model shows minimum 5C margins for mission disposal options, except for heater controlled elements which have a maximum 70% heater duty cycle, and two-phase flow systems which have a minimum 30% heat transport margin.
Verification:	1. Verify at MCR.	1. Verify worst-case thermal analysis of concept through peer review and at SRR and MDR.	1. Verify worst-case thermal analysis of design through peer review and at PDR.	1. Verify worst-case thermal analysis of detailed design through peer review and at CDR.	1. Verify through peer review and at PER and PSR.	1. Verify thermal analysis of flight system using flight-correlated thermal model through peer review.	1. Verify thermal analysis of flight system using flight-correlated thermal model through peer review.

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Thermal Engineering Branch (545)	GEVS 2.63; 545-PG-8700.2.1

4.26 Thermal Design Margins - Unplanned Conditions

Mechanical

Principle: For credible abnormal conditions, the thermal design shall maintain temperatures with allowable flight temperature (AFT) limits extended by +/- 5C (Flight Acceptance (FA) temperature range).

Rationale: The Acceptance Temperature margin of +/-5C can be used to absorb temperature impacts resulting from credible abnormal conditions such as anomaly-induced power dissipation, off-nominal sun attitude conditions, and/or thermal control element (active or passive) anomalous behavior.

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Systems Engineering defines credible abnormal conditions for inclusion in system definition for thermal analysis.	1. Systems Engineering refines and updates credible conditions for evaluation in system definition for thermal analysis.	1. Thermal Balance Testing shall include, where appropriate, a simulation of the abnormal credible condition for empirical evaluation.	1. Thermal analysis with flight-correlated model shows temperatures at or less than FA Limits for System Engineering defined credible abnormal conditions.	1. Thermal analysis with flight-correlated model shows temperatures at or less than FA Limits for System Engineering defined credible abnormal conditions.
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify through peer review and at PSR.	1. Verify through thermal analysis of flight system using flight-correlated thermal model.	1. Verify through thermal analysis of flight system using flight-correlated thermal model.

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Thermal Engineering Branch (545)	JPL D-17868 rev. 2: 4.8.2.4

4.27 Test Temperature Margins

Mechanical

Principle: Components and systems shall be tested beyond allowable flight temperature limits. The margin required for proto-flight thermal vacuum testing is 10C beyond allowable flight temperature limits. Acceptance test margin may be reduced to 5C. For actively controlled systems with selectable/variable setpoints, the margin may be reduced to 5C. For active control systems with a fixed setpoint, margin shall be demonstrated by increasing or decreasing (as appropriate) the heat load (internal or external) by at least 30% and still maintain the control temperature.

Rationale: (Note: This rule does not apply to cryogenic systems.)

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Component proto-flight thermal vacuum test temperatures shall be specified with the required margin as stated in principle above.	1. Component, subsystem, and system proto-flight thermal vacuum test temperatures shall be specified with the required margin as stated in principle above.	1. Components and systems shall undergo proto-flight thermal vacuum testing with the required margin as stated in principle above. Yellow and Red limits for flight temperature telemetry database shall be consistent with actual proto-flight system thermal vacuum test temperatures.	1. Yellow and Red limits for flight temperature telemetry database shall be consistent with actual proto-flight system thermal vacuum test temperatures.	1. Yellow and Red limits for flight temperature telemetry database shall be consistent with actual proto-flight system thermal vacuum test temperatures.
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify results of component and subsystem thermal vacuum tests at PER. 2. Verify results of system thermal vacuum test at PSR. 3. Verify flight data base limits at MRR and/or FRR.		

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Thermal Engineering Branch (545)	GEVS 2.6

4.28 Thermal Design Margin Verification

Mechanical

Principle: All subsystems/systems having a thermal design with identifiable thermal design margins shall be subject to a Thermal Balance Test at the appropriate assembly level per GEVS Section 2.6.

Rationale: This test shall provide an empirical verification of the subsystem/system's thermal design margin. In addition, steady state temperature data from this test shall be used to validate subsystem/system thermal math models (TMMs).

Phase:	<A	A	B	C	D	E	F
Activities:	1. Identify thermal balance test concepts.	1. Include thermal balance test in environmental test plan.	1. Identify preliminary thermal balance test architecture and scope.	1. Identify specific thermal balance test architecture and cases.	1. Implement test.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify at SDR and PDR.	1. Verify at CDR.	1. Verify at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Thermal Engineering Branch (545)	GEVS 2.6

4.29 Thermal-Vacuum Cycling

Mechanical

Principle: All systems flying in unpressurized areas shall have been subjected to a minimum of eight (8) thermal-vacuum test cycles prior to installation on a spacecraft. Four (4) of these cycles may include cycles at the subsystem or instrument level of assembly.

Rationale: This provides workmanship and performance verifications at lower levels of assembly where required environments can be achieved and reduces the risk to cost during spacecraft Integration and Test (I&T).

Phase:	<A	A	B	C	D	E	F
Activities:	1. Identify environmental test concept.	1. Develop preliminary environmental test plan.	1. Update environmental test plan and put under configuration control.	1. Update plan.	1. Implement test cycles.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at MDR.	1. Verify at SDR and PDR.	1. Verify at CDR.	1. Verify that all components have seen required testing prior to spacecraft I&T at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Office of Systems Safety and Mission Assurance (300)	GEVS 2.6.2.4.b

5.04 Instrument Testing for Multipaction

Instruments; Electrical

Principle: Active RF components, such as radars, shall be designed and tested for immunity to multipaction.

Rationale: Multipaction on RF components that carry large amounts of RF power can degrade overall performance and cause damage. Unless significant design margin is demonstrated, small unit-to-unit variations make it impossible to predict whether an RF component is susceptible to multipaction.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Determine the likely maximum power levels that components are going to see and determine if multipaction could be an issue.	1. Further refine power requirements and for components that are likely to have multipaction issues. 2. Begin vendor research to determine the extent of the issues.	1. Down select vendor and finalize component performance and power requirements. 2. Develop multipaction immunity verification plan.	1. Build engineering models of all components that could experience multipaciton and perform testing on these components before and after environmental testing.	1. Build flight models and perform multipaction testing on all flight components before and after environmental testing.	1. Monitor instrument performance to determine if component damage or degradation is occurring due to multipaction.	N/A
Verification:		1. Gather data from multiple vendors to have several points of comparison.	1. Verify design and verification plan at PDR.	1. Verify results of EM testing at CDR.	1. Verify results of testing at PSR.	1. Track long-term performance of instrument for trends in overall performance and compare to expectations.	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Microwave Instrument Technology Branch (555)	

5.05 Fluid Systems GSE

Instruments

Principle: Fluid systems GSE used to pressurize flight systems shall be single-fault tolerant against over-pressurizing the flight system.

Rationale: Fluid systems GSE is usually at a pressure significantly above the flight systems final pressure and therefore poses a risk of over-pressurizing the flight system.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Recognize the need for this specialized GSE.	1. Determine if candidate GSE exist and availability (versus a new build).	1. Secure agreement for existing GSE. 2. Design new GSE and procure components.	1. Recertify existing GSE before use. 2. Assemble and certify GSE.	1. Use GSE to test flight system (and components if necessary).	N/A	N/A
Verification:	1. Verify inclusion in proposal write-up and cost estimate.	1. Present GSE asessment at MDR.	1. Verify through peer review and at PDR.	1. Present certification at CDR.	1. Verify that procedures for GSE are approved by PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Cryogenics and Fluids Branch (552)	

5.06 Flight Instrument Characterization Standard

Instruments

Principle: Flight instruments and their components shall be characterized for performance over their expected operating temperature range.

Rationale: Detector performance falls of rapidly as a function of temperature for both increasing and decreasing temperature. Additionally, structural-thermal, and optical performance models need to be correlated against tests.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Test mission-enabling parts and components at room temperature (extrapolate performance at other than room temperature).	1. Test critical parts and components over the flight operation temperature range, plus margin (no extrapolations) beyond intended operating range.	1. Test flight-like subsystem and components over the flight operation temperature range, plus margin beyond intended operating range.	1. Test flight-like systems and components operating temperature range, plus margin beyond intended operating range.	1. Test flight system over operating temperature range, plus margin beyond intended operating range.	N/A	N/A
Verification:	1. Test result reviewed by principal investigator.	1. Test result reviewed by principal investigator and science working group.	1. Review summary of results at PDR.	1. Review summary of results at CDR.	1. Verify through peer review and at PER.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Revision C, October 30, 2006	Detector Systems Branch (553)	

5.08 Laser Development Contamination Control

Instruments

Principle: All flight laser development shall include an approved laser-specific Contamination Control Plan (CCP).

Rationale: Component and/or system contamination has been identified as the contributing cause in most laser failures to-date. There are unique requirements of a laser CCP that differ significantly from those of a general CCP (as required by 4.01).

Phase:	<A	A	B	C	D	E	F
Activities:	N/A	N/A	1. Review 'Laser Contamination Control Plan Outline' and prepare a program specific CCP.	1. Implement CCP at the component level.	1. Continue implementation of the CCP through launch.	1. Continue any post-launch aspects of the CCP.	N/A
Verification:	N/A	N/A	1. Review documentation at PDR.	1. Verify at CDR.	1. Verify at PER and PSR.	1. Verify post-launch summary of activities.	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Laser and Electronic Optics Branch (554)	

5.09 Cryogenic Pressure Relief

Instruments

Principle: Stored cryogen systems (and related GSE) shall be single fault tolerant against over-pressurization due to blockage or failure of a relief path.

Rationale: Credible, albeit unintended, conditions can lead to potential system over-pressurization.

Phase:	<A	A	B	C	D	E	F
Activities:	1. Identify personnel or organization to conduct the appropriate analyses during subsequent phases.	1. Identify underlying assumptions and conduct preliminary emergency venting analysis.	1. Refine analysis and identify candidate relief devices.	1. Finalize analysis and include relief devices in design. Procure devices and test them at the component level.	1. Include the devices in the hardware build-up and test function during build-up as appropriate. 2. Review flight hardware and GSE configurations prior to testing to ensure that relief paths are not circumvented.	N/A	N/A
Verification:	1. Grass-root cost estimate to include cryogenic engineering.	1. Ensure venting analysis included in larger cryogenic system analysis report/ summary that is reviewed by the system engineer and/or review team.	1. Review at PDR.	1. Review at CDR.	1. Review at PER.	N/A	N/A

Revision Status:	Owner:	Reference:
Revision C, October 30, 2006	Cryogenics and Fluids Branch (552)	

GLOSSARY AND ACRONYM GUIDE

Anomaly	An unanticipated or unpredicted behavior that occurs as a discrete episode
ASIC	Application Specific Integrated Circuit
Assembly	A functional subdivision of a component consisting of parts or subassemblies that perform functions necessary for the operation of a component as a whole (Ref: GEVS 1-6)
ACS	Attitude Control System
BOL	Beginning of Life
Breadboard	A model used to test hardware at TRL 4 or 5 (See TRL levels.)
Catastrophic Hazard	A condition that may cause death or permanently disabling injury, major system or facility destruction on the ground, or vehicle during the mission.
CCB	Configuration Control Board
CCP	Contamination Control Plan
CDR	Critical Design Review
CI	Configuration Item
CM	Configuration Management. A management discipline applied over the product's life cycle to provide visibility and to control performance and functional and physical characteristics (Ref: NPR 7120.5b)

Component	A functional subdivision of a subsystem and generally a self-contained combination of items performing a function necessary for the subsystem's operation (Ref: GEVS 1-6)
Credible	Capable of being believed (A plausible likelihood of failure)
Critical Hazard	A condition that may cause severe injury or occupational illness, or major property damage to facilities, systems, or flight hardware.
DR	Decommissioning Review
EEE	Electrical Engineering
EGSE	Electrical Ground Support Equipment
Element	A portion of a hardware or software unit that is logically discrete
EMC	Electromagnetic Compatibility
End-to-end test	A test performed on the integrated ground and flight system, including all elements of the payload, its control, stimulation, communications, and data processing (Ref: GEVS 1-5)
ETU	Engineering Test Unit
EOL	End of Life
FDAC	Failure Detection and Correction
FOR	Flight Operations Review
FOS	Factors of Safety

FOV	Field of Vision
FPGA	Field Programmable Gate Arrays
FSW	Flight Software
GEVS	General Environmental Verification Specification
GMF	Geomagnetic Field
GN&C	Guidance, Navigation, and Control
GPR	Goddard Policy Requirement
GSE	Ground Support Equipment
Heritage hardware	Hardware from a previous project, program, or mission
High fidelity	Addresses form, fit, and function. Equipment that can simulate and validate all system specifications within a laboratory setting (Ref: Defense Acquisition University)
High-level objectives	High level objectives – science or technology validation objectives that define the purpose of the mission. Also Level 0 requirements
HW	Hardware
ICD	Interface Control Document
ICR	Initial Confirmation Review

ITU	Integrated Test Unit
I&T	Integration and Testing
LRR	Launch Readiness Review
Level 1 Requirements	A Project's fundamental and basic set of requirements levied by the Program or Headquarters on the Project. (Ref: GPG 7120.5) Level 1 Requirements are sufficient to define the scope of scientific or technology validation objectives and describe the measurements required to achieve these objectives. Level 1 Requirements should also define success criteria for an expected mission and a minimum mission
Level 2 Requirements	Requirements allocated to mission segments (instruments, spacecraft bus, ground system, and launch vehicle). Level 2 Requirements also envelop Mission Assurance Requirements and technical resource allocations
Level 3 Requirements	Subsystem requirements. Level 3 Requirements include instrument specifications and interface definitions
Level 4 Requirements	Component requirements. Level 4 Requirements cover all hardware and software components to be designed or procured, such as optics, filter wheels, and CCDs
Margin	The amount by which hardware capability exceeds requirements (Ref: GEVS 1-7)
MAR	Mission Assurance Requirement
MAE	Materials Assurance Engineer
MDR	Mission Definition Review
MCR	Mission Concept Review

Mission-critical	Item or function that must retain its operational capability to assure no mission failure (See Mission success) (Ref: MSFC SMA Directorate)
Mission success	Those activities performed in line and under the control of the program or project that are necessary to provide assurance that the program or project will achieve its objectives. The mission success activities will typically include risk assessments, system safety engineering, reliability analysis, quality assurance, electronic and mechanical parts control, software validation, failure reporting/resolution, and other activities that are normally part of a program or project work structure (Ref: NPR 7120.5b)
MOR	Mission Operations Review
M&P	Materials and Processes
OOB	Out-of-band
ORR	Operational Readiness Review
OTS	Off-the-shelf
Payload	An integrated assemblage of modules, subsystems, etc., designed to perform a specified mission in space (Ref: GEVS 1-7)
PDR	Preliminary Design Review
PER	Pre-Environmental Review
Performance Verification	Determination by test, analysis, or a combination of the two that the payload element can operate as intended in a particular mission (Ref: GEVS 1-7)
PLD	Programmable Logic Device

Project execution	The performance with respect to schedule, cost, and other key managerial metrics and considerations.
Prototype hardware	Hardware of a new design. It is subject to a design qualification test program; it is not intended for flight (Ref: GEVS 1-6)
PSR	Pre-Ship Review
RF	Radio Frequency
RHA	Radiation Hardness Assurance
Safe Hold Mode	A control mode designed to provide a spacecraft with a mode to preserve its health and safety while recovery efforts are undertaken
Safety	Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment (Ref: NPR 7120.5b)
SAR	System Acceptance Review
S/C	Spacecraft
SDR	System Design Review
SEMP	Systems Engineering Management Plan
Simulation	A synthetic representation of the characteristics of real world system or situation, typically by interfacing controls and displays (operational or simulated) and positions of the system with a computer (Ref: MIL-HDBK-220B)
SMO	Systems Management Office

SORR	Science Operations Readiness Review
Spare part	A replacement part (reparable or expendable supplies) purchased for use in the maintenance of systems such as aircraft, launch vehicles, spacecraft, satellites, ground communication systems, ground support equipment, and associated test equipment. It can include line-replaceable units, orbit-replaceable units, shop-replaceable units, or piece parts used to repair subassemblies (Ref: NPR 5900.1)
SPP	Spare Parts Program
SRR	System Readiness Review
Subsystem	A functional subdivision of a payload consisting of two or more components (Ref: GEVS 1-6)
System	The combination of elements that function together to produce the capability required to meet a need. The elements include all hardware, software, equipment, facilities, personnel, processes, and procedures needed for this purpose (Ref: NPR 7120.5, NASA Program and Project Management Processes and Requirements)
System Integrity	The ability of a system to maintain its form and function (See System)
SW	Software
T&C	Telemetry and Command
T&M	Time and Materials
TM	Torque Margin

TRL	Technology Readiness Level - A systematic metric/measurement system that supports assessments of the maturity of a particular technology and the consistent comparison of maturity between different types of technology. NASA recognizes nine technological readiness levels: TRL 9 Actual system “flight proven” through successful mission operations TRL 8 Actual system completed and “flight qualified” through test and demonstration (ground or flight) TRL 7 System prototype demonstration in a space environment TRL 6 System/subsystem model or prototype demonstration in a relevant environment (ground or space) TRL 5 Component and/or breadboard validation in relevant environment TRL 4 Component and/or breadboard validation in laboratory environment TRL 3 Analytical and experimental critical function and/or characteristic proof-of-concept TRL 2 Technology concept and/or application formulated TRL 1 Basic principles observed and reported (Ref: Space Science Enterprise Management Handbook, Appendix E 11)
Traceability Matrix	A matrix demonstrating the flow-down of requirements to successively lower levels
TSR	Technical Status Review

Validation	Proof that Operations Concept, Requirements, and Architecture and Design will meet Mission Objectives, that they are consistent, and that the "right system" has been designed. May be determined by a combination of test or analysis. Generally accomplished through trade studies and performance analysis by Phase B and through tests in Phase D (Ref: GPG 7120.5)
Verification	Proof of compliance with requirements and that the system has been "designed and built right." May be determined by a combination of test, analysis, and inspection (Ref: GPG 7120.5)

Revision	Effective Date	Description
Baseline Release	**10-Dec-04**	
A	**30-May-05**	[P. 10] User's Guide: removed text examples, replaced with bullets explaining what general information goes into each rule section.
		Addition of Change History page (against 12/10 baseline rulebook).
		[P. 7] Revised Front Matter Graphics (architectural diagram - Figure 2).
		[Rule 1.17, Glossary] 1. Added "credible" to Principle, Phase B, and Phase C; 2. Added "credible" definition to Glossary.
		[Rule 1.22] Phase C revision - Replaced existing language with: "Demonstrate that the method for drying the wetted system has been validated by test on an equivalent or similar system."
		[Rule 1.14] Revision to the Principle and Rationale. <u>Revised Principle</u>: Telemetry coverage shall be acquired during all mission-critical events. *Continuous telemetry and command capability shall be maintained during launch and until the spacecraft has been established on-orbit in a stable, power-positive mode."*
		[Rule 1.06] Added table 1.06-1 to website rule set.
		[Rule 3.07] Added table 3.07-1 to website rule set.
		[Rules: 2.01, 2.07, 2.11, 4.01, 4.03, 4.09, 4.10, 4.11, 4.12, 4.13, 4.14, 4.15, 4.23, 4.25, 4.27, 4.28, 4.29] 1. Corrected GSFC-STD-7000 (GEVS) references in GSFC-STD-1000. 2. Created reference PDFs. 3. Added reference links.
		[Rule 3.09] Added web links to source material (NPR 7150.2, GPG 8700.5).
Revision	**Effective Date**	**Description**
B	**30-June-06**	[P. 6] Updated Introduction.
		[P. 9] Revised Figure 3 Lifecycle Chart - Removed “from SMO”
		[P. 10] Updated User’s Guide.
		New Systems Engineering Rule: 1.04 – System Modes.
		New Systems Engineering Rule: 1.08 – End to End Testing.
		[Rule 1.14] Revised Principle, Rationale, Activities (Phase E), and Verification (Phases pre-A, A, C → E). <u>Revised Principle:</u> *Continuous telemetry and command coverage shall be maintained during all mission-critical events. Mission-critical events shall be defined to include separation from the launch vehicle; power-up of major components or subsystems; deployment of mechanisms and/or mission-critical appendages; and all planned propulsive maneuvers required to establish mission orbit and/or achieve safe attitude.*

B	**30-June-06**	Revised Rationale: *With continuous telemetry and command capability, operators can prevent anomalous events from propagating to mission loss. Also, flight data will be available for anomaly investigations.*
		[Rule 1.30] Revised Principle, Rationale, and Activities and Verification (Phases pre-A → D). Revised Principle: *The Attitude Control System (ACS) shall have stability margins of at least 6db for rigid body stability with 30 degrees phase margin, and 12db of gain margin for flexible modes.*
		New Systems Engineering Rule: 1.36 – Block-Redundant Component Failure.
		New Systems Engineering Rule: 1.37 – Stowage Configuration.
		New Systems Engineering Rule: 1.38 – Configuration Command Confirmation.
		[Rule 2.01] Revised Activities and Verification for Phases A, B, C, and D.
		New Electrical Rule: 2.14 – Capping of Test Points and Plugs
		New Electrical Rule: 2.15 – Flight and Ground Electrical Hardware.
		New Electrical Rule: 2.16 – Solar Arrays.
		New Electrical Rule: 2.17 – I&T Development Input.
		New Software Rule: 3.11 – Long Duration and Failure Free System Level Test of Flight Software.
		New Software rule: 3.12 – Visibility of Spacecraft State.
		New Software Rule: 3.13 – Operational Software Redundant Element.
		New Software Rule: 3.14 – Command Procedure Changes.
		New Software Rule: 3.15 – Test and GSE Software Interfaces.
		Elimination of Rule 4.17 – Limits of Certain Alloy Types.
		[Rule 5.01] Relocation and re-numbering of rule 5.01, from Instruments section to Systems Engineering section. New rule number is 1.35.
		Elimination of Rule 5.07 – Laser Design.
B.1	**29-Sept-06**	Formatting changes to Rules 1.17, 2.02, 2.17, 3.03, 3.06, 3.07, 3.09, 3.10, 3.14, 3.15, 4.07, 4.15, 4.20, 4.28, Page 2, Table 307-1 and Glossary "Space Part"
		Typographical errors corrected on Rule 1.28, 3.10, 4.08, 4.18, 4.23, 4.26
		Replaced Page 2 and 3 of Table 3.07-1
C	**30-Oct-06**	Rule 1.14 – Revised Language in "Principle" Statement
		Rule 1.26 – Major Revision
		New Systems Engineering Rule: 1.29 Leakage of Hazardous Propellant
		Glossary – Added definitions for critical and catastrophic hazards
		Table of Contents – Updated to Reflect Changes for Rules 1.26, 1.29