GODDARD TECHNICAL STANDARD	GSFC-STD-1000E
Goddard Space Flight Center Greenbelt, MD 20771	Approved: 08-03-2009 - With Administrative Changes Expiration Date: 08-03-2014 Superseding GSFC-STD-1000D

Goddard Space Flight Center

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

Requests for information, corrections, or additions to this standard should be submitted via "Feedback" in the GSFC Technical Standards System at http://standards.gsfc.nasa.gov.

Goddard Space Flight Center

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

GSFC-STD-1000
Revision E

Approved

Original Signed by:
Goddard Technical
Standards Coordinator

Original Signed by:
Chief Engineer
Goddard Space Flight Center

Original Signed by:
Director of Applied
Engineering and Technology

Original Signed by:
Director of Flight
Programs and Projects

Original Signed by:
Director of Safety and
Mission Assurance

Requests for information, corrections, or additions to this standard should be submitted via "Feedback" in the GSFC Technical Standards System at http://standards.gsfc.nasa.gov.

Table of Contents

INTRODUCTION

Purpose:
The Goddard Open Learning Design (GOLD) Rules specify sound engineering principles and practices, which have evolved in the Goddard community over its long and successful flight history. They are intended to describe foundational principles that "work," without being overly prescriptive of an implementation "philosophy." Along with principles, the GOLD Rules also include a select list of more quantitative requirements, which warrant special attention due either to their historical significance, or their new and rapidly evolving nature.

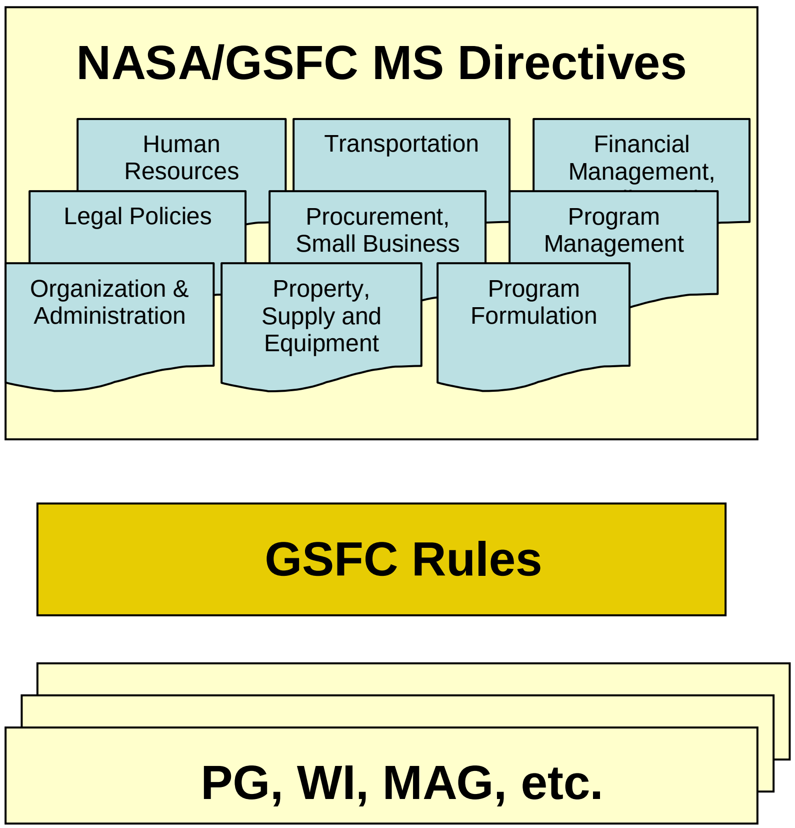
The formalization of key requirements helps establish the methodology necessary to consistently and efficiently achieve safety and mission success for all space flight products. The GOLD Rules share valuable experiences, and communicate expectations to developers. Where appropriate, the rules identify typical activities across lifecycle phases with corresponding evaluation criteria. The GOLD Rules also provide a framework for the many responsible Goddard institutions to assess and communicate progress in the project's execution. The GOLD Rules ensure that GSFC Senior Management will not be surprised by late notification of noncompliance to sound and proven engineering principles that have made GSFC missions consistently successful. Each GOLD Rule, whether stated as a general principle or in a more quantitative form, specifies requirements in the form of a Rule Statement, along with supporting rationale, and guidance in the form of typical lifecycle phase activities and verifications.

Scope:
The GOLD Rules focus on fundamental principles and requirements, and therefore are intended to apply to all space flight products, regardless of implementation approach or mission classification. Whenever necessary, rules clarify requirements and expectations consistent with different mission classifications. Although not expected to be required, an a priori Mission Exceptions List (MEL) may be proposed at the start of a Program and/or Project, to highlight rules which may not apply. If a MEL is submitted and approved, the waivers will not be required for exceptions covered by the MEL. Other exceptions that arise during execution of the mission still require waivers, as appropriate. A MEL approved at the program level for multi project programs will be reviewed at key points in the program lifecycle (e.g. At the release of a new Announcement of Opportunity) to validate its applicability for new Projects.

The GOLD Rules is a living document, periodically assessed and updated to improve its clarity of purpose and effectiveness. While its engineering principles and practices are stable, its select set of requirements may evolve based on whether they continue to warrant the increased visibility they are afforded by inclusion. The intent is to improve the GOLD Rules over time, not to grow it in size, complexity, and coverage so that it becomes more cumbersome and less helpful over time. Requirements temporarily included because of their new and rapidly evolving nature, must be accompanied by transition plan out of GOLD rules and into an appropriate lower level document.

GSFC Rules are governed by GPR 8070.4, 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 and waivers.

NASA/GSFC Processes and Rules Hierarchy



NPDs, NPRs, GPDs, GPRs
Provide policy direction and High-level requirements
Owner: Center Director via Management System Council

Rules for the Design, Development, Verification and Operation of Flight Systems applicable to all GSFC Projects
Owner for Content: AETD
Owner for Configuration Management: SMA-D
Owner for Implementation: FPD

Procedures and Guidelines, applicable to specific line Organizations and engineering disciplines
Owner: Directorates

Figure 1

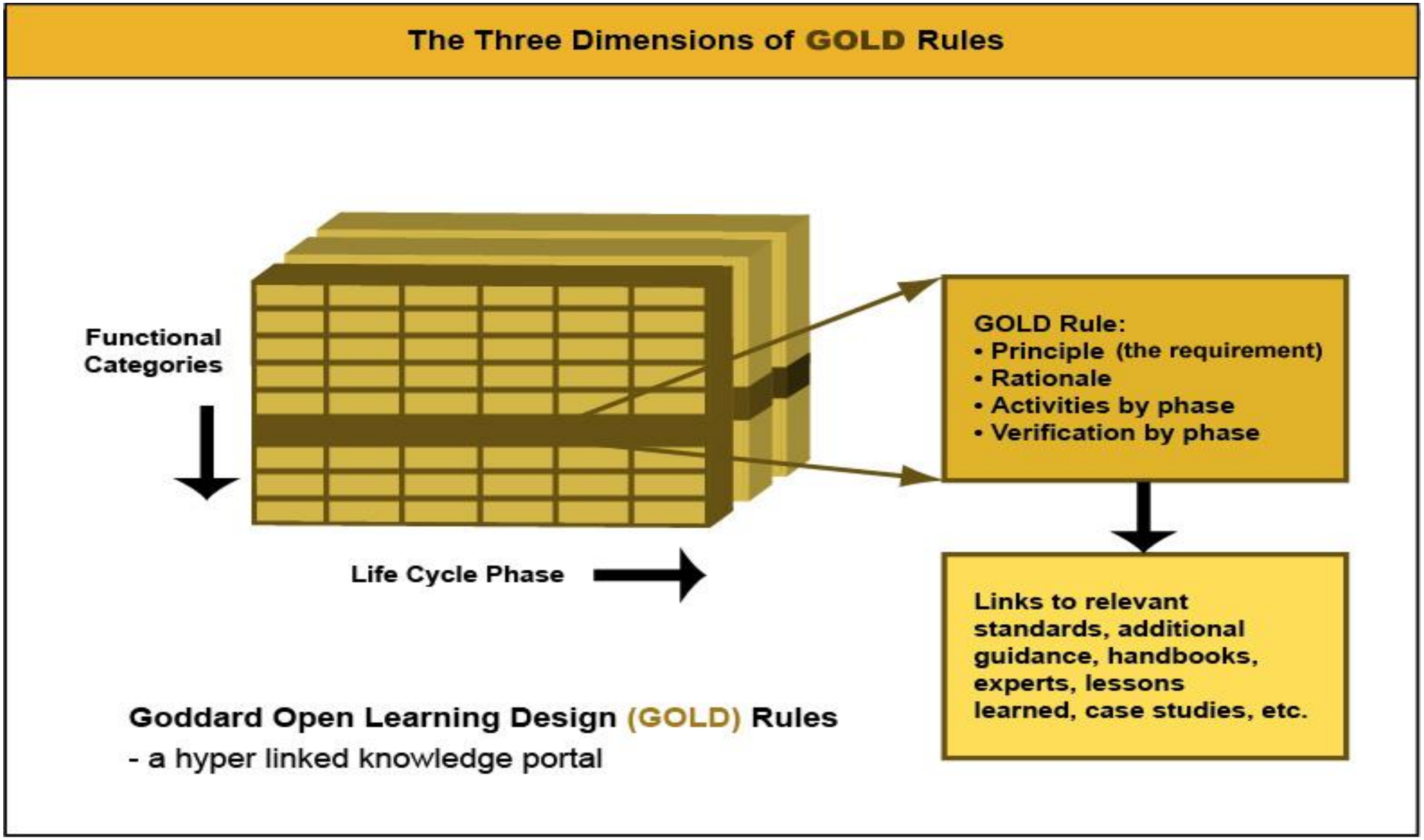

The Three Dimensions of GOLD Rules
Functional Categories
Life Cycle Phase
GOLD Rule:
• Principle (the requirement)
• Rationale
• Activities by phase
• Verification by phase
Links to relevant standards, additional guidance, handbooks, experts, lessons learned, case studies, etc.
Goddard Open Learning Design (GOLD) Rules
- a hyper linked knowledge portal

Figure 2

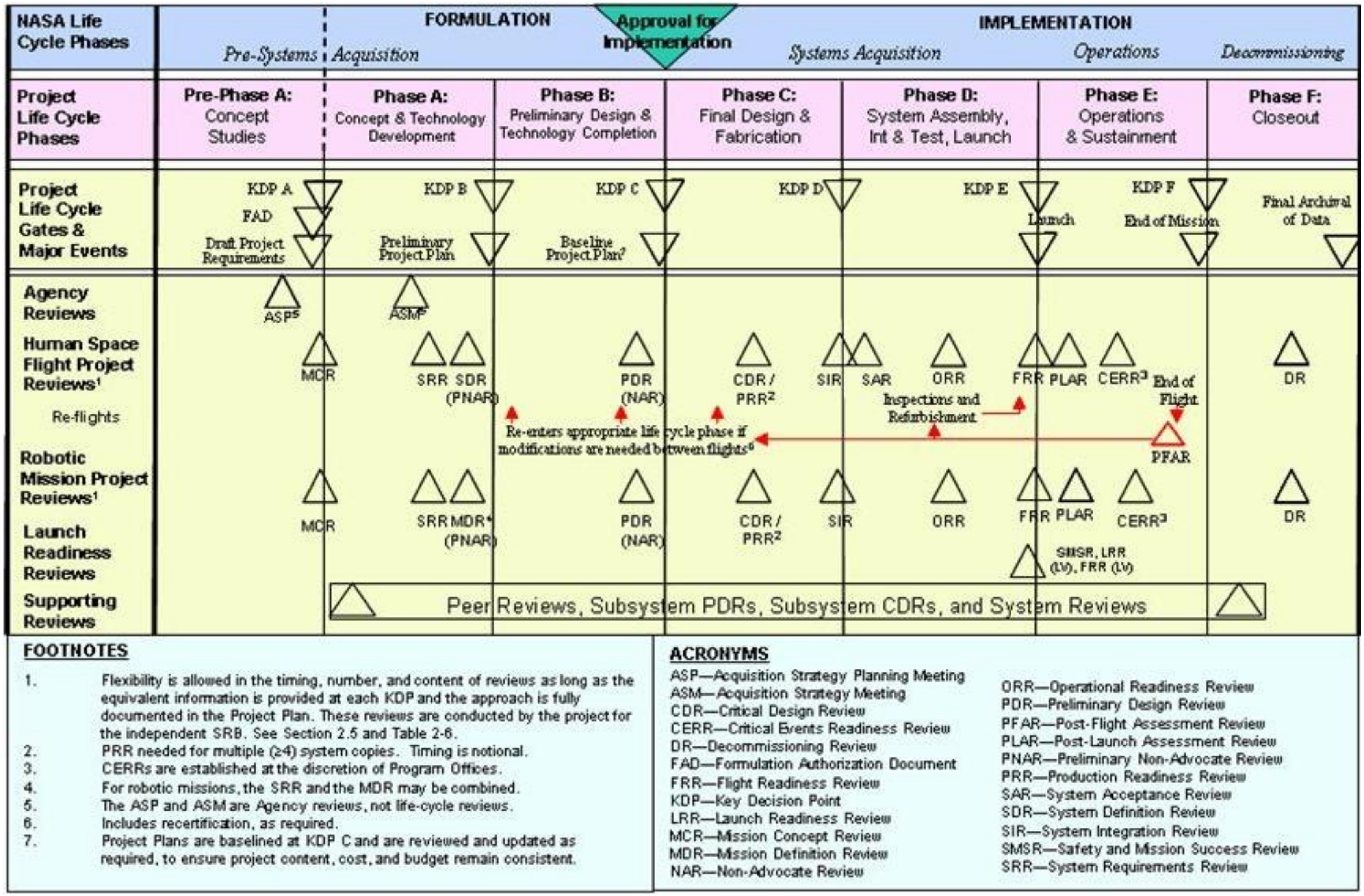


Figure 3 (Reference: NPR 7120.5D, The NASA Project Lifecycle)

User's Guide

Rule #	Title				Discipline		
Rule Type: P = general Principle R = quantitative Requirement	Rule Statement – The requirement, either stated as a general principle or in a more quantitative form.						
Rationale:	Statement(s) providing justification, clarification and/or context.						
Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:	Rule-associated best practices, within each phase, to ensure compliance (guidance only)						
Verification:	Rule-associated best practices, within each phase, to ensure compliance (guidance only)						
Revision Status: When implemented/modified		**Owner:** Subject Matter Expert / Technical Authority				**Reference:** Supporting Materials	

Figure 4

1.05	Single Point Failures				Systems Engineering		
Rule: **R**	Single point failures that prevent the ability to fully meet 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 or present management exceptions at MCR.	1. Verify or present management exceptions at MDR.	1. Verify or present management exceptions at PDR.	1. Verify or present management exceptions at CDR.	1. Verify or present management exceptions at PER and PSR.	N/A	N/A
Revision Status: Rev. E		**Owner:** Mission Engineering and Systems Analysis Division (590)				**Reference:** New Fault Management PG (Future Reference)	

1.06	Resource Margins				Systems Engineering		
Principle: **R**	System resource margins shall be evaluated in accordance with Table 1.06-1, with system margin and contingency/reserve defined in the table, and illustrated in Figures 1.06-1 and 1.06-2. Table 1.06-2 is a schedule of recommended mass contingency/reserve by subsystem.						
Rationale:	Judicious application of these margins improves performance on cost and schedule as well as overall mission performance. NOTE: Flight software margins are covered in Rule 3.07.						
Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:	1. Identify system resource margins 2. Identify subsystem development maturity 3. Identify appropriate resource contingency/reserve for each subsystem.	1. Update system resource margins 2. Update subsystem development maturity 3. Update appropriate resource contingency/reserve for each subsystem	1. Update system resource margins 2. Update subsystem development maturity 3. Update appropriate resource contingency/reserve for each subsystem	1. Update system resource margins 2. Update subsystem development maturity 3. Update appropriate resource contingency/reserve for each subsystem	1. Update system resource margins 2. Update subsystem development maturity 3. Update appropriate resource contingency/reserve for each subsystem	N/A	N/A
Verification:	1. At MCR, If noncompliant, provide a return-to-compliance plan or request a waiver..	1. At ICR and MDR, If noncompliant, provide a return-to-compliance plan or request a waiver..	1. At PDR and confirmation review, if noncompliant, provide a return-to-compliance plan or request a waiver.	1. At CDR, if noncompliant, provide a return-to-compliance plan or request a waiver.	1. At PER and PSR, if noncompliant, provide a return-to-compliance plan or request a waiver.	N/A	N/A
Revision Status: Rev. E		**Owner:** Mission Engineering and Systems Analysis Division (590)				**Reference:** Guidelines for Margins (Future Reference)	

Table 1.06-1 Required Minimum Acceptable Technical Resource System Margin

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
MEV for Dry Mass	30%	25%	20%	15%	0	
MEV for Power (at EOL)	30%	25%	15%	15%	10%[1]	
Propellant (Δv)[2]	3σ				3σ	
Telemetry and Command hardware channels[3]	25%	20%	15%	10%	0	
RF Link	3 db	3 db	3 db	3 db		

Maximum Possible Value = The physical limit or agreed-to limit.
Maximum Expected Value (MEV) = Current Best Estimate (CBE) + Contingency/Reserve
System Margin=Maximum Possible Value-Maximum Expected Value
% System Margin=100% x System Margin/Maximum Expected Value

1. At launch there shall be 10% predicted power system margin for mission critical, cruise, and safing modes as well as to accommodate in-flight operational uncertainties.
2. The 3σ variation is due to: 1). Worst-case spacecraft mass properties; 2). 3σ low launch vehicle performance; 3). 3σ low propulsion subsystem performance (due to thruster performance alignment, propellant residuals); 4). 3σ flight dynamics errors and constraints; 5). Thruster failure on single fault tolerant systems.
3. Telemetry and command hardware channels read data from hardware such as thermostats, heaters, switches, motors, and so on.
4. See Table 1.06-2 for recommended mass contingency.

Table 1.06-2 Recommended Mass Contingency/Reserve by Subsystem[1]

All values are assumed to be at the end of the phase

Sub-system Design Maturity[2]	TRL Range[2]	Contingency/Reserve (in percent)[3]											
		Electrical/Electronic											
		0-5 kg	*5-15 kg*	*>15 kg*	*Structure*	*Brackets, Clips, Hardware*	*Battery*	*Solar Array*	*Thermal Control*	*Mechanisms*	*Propulsion*[4]	*Wire Harness*	*Science Instrument*
Basic principles reported thru technology concept and/or application formulated.	0 to 2	30	25	20	25	30	25	30	25	25	25	55	55
Analytical/experimental proof of concept thru breadboard validation in relevant environment	3 to 5	25	20	15	15	20	15	20	20	15	15	30	30
Sub-system/component prototype demo in an operational environment	6	20	15	10	10	15	10	10	15	10	10	25	25
Sub-system engineering unit test in an operational environment	7	10	5	5	5	6	5	5	5	5	5	10	10
Actual sub-system completed and flight qualified	8	3	3	3	3	3	3	3	3	3	3	5	5
Actual sub-system flight proven through successful mission operations	9	0	0	0	0	0	0	0	0	0	0	0	0

1. Adapted from Table 1, "Space Systems - Mass Properties Control for Space Systems",S-120-2006e, AIAA.
2. See the latest version of NPR 7120.8 Appendix J for NASA TRL definitions and classification schema.
3. Contingency % =100% x Contingency(kgs)/(Maximum Expected Value(kgs) - Contingency(kgs))
4. Propulsion sub-system dry mass only.
5. For system margins, see Table 1.06-1.
6. Subsystems not identified as new technology developments can be evaluated as if they are at TRL 6.
7. Subsystems which are fully qualified at the system level for the current mission, and have been weighed, can be evaluated as if they are at TRL 9

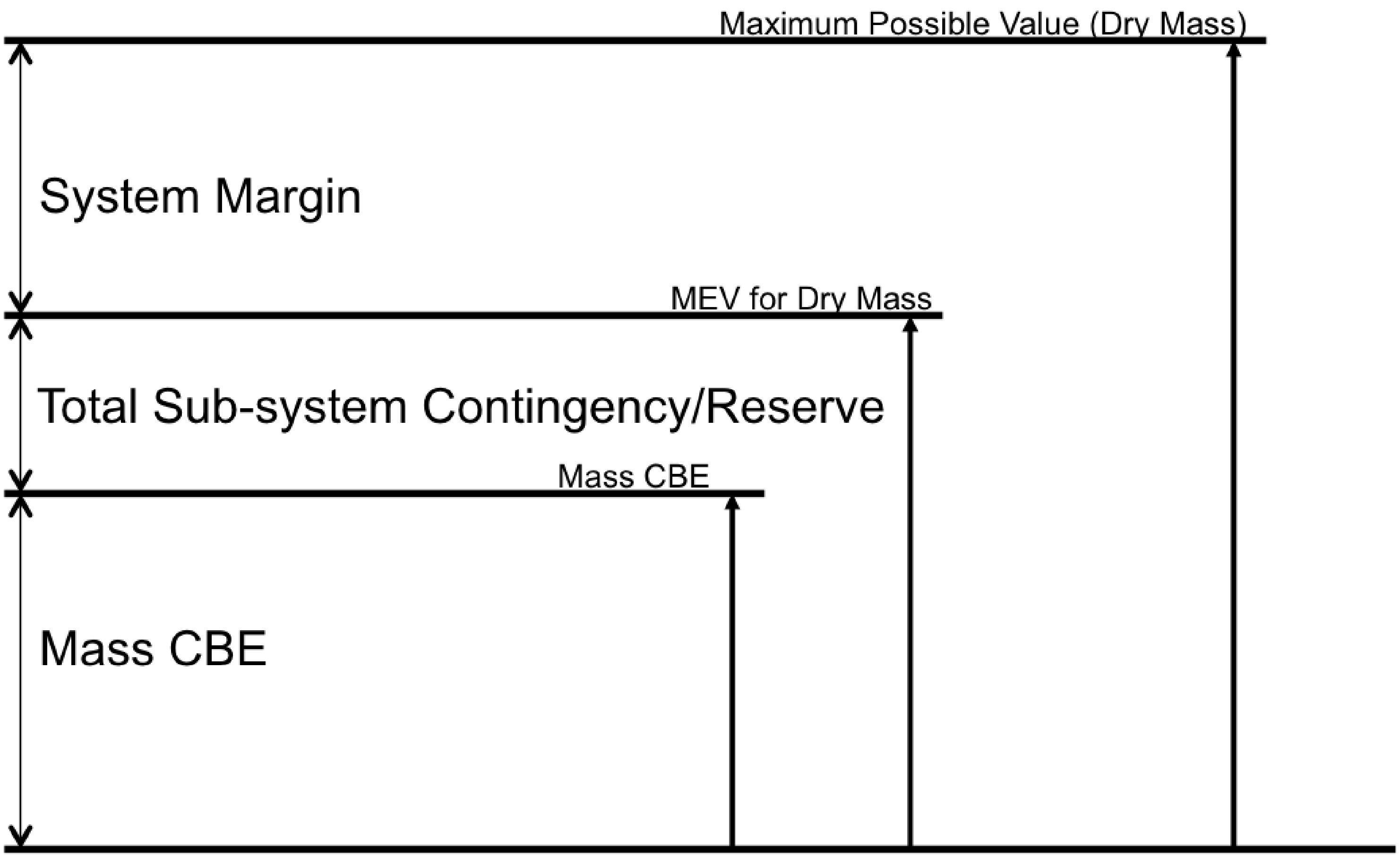


Figure 1.06-1: Mass Property Definitions

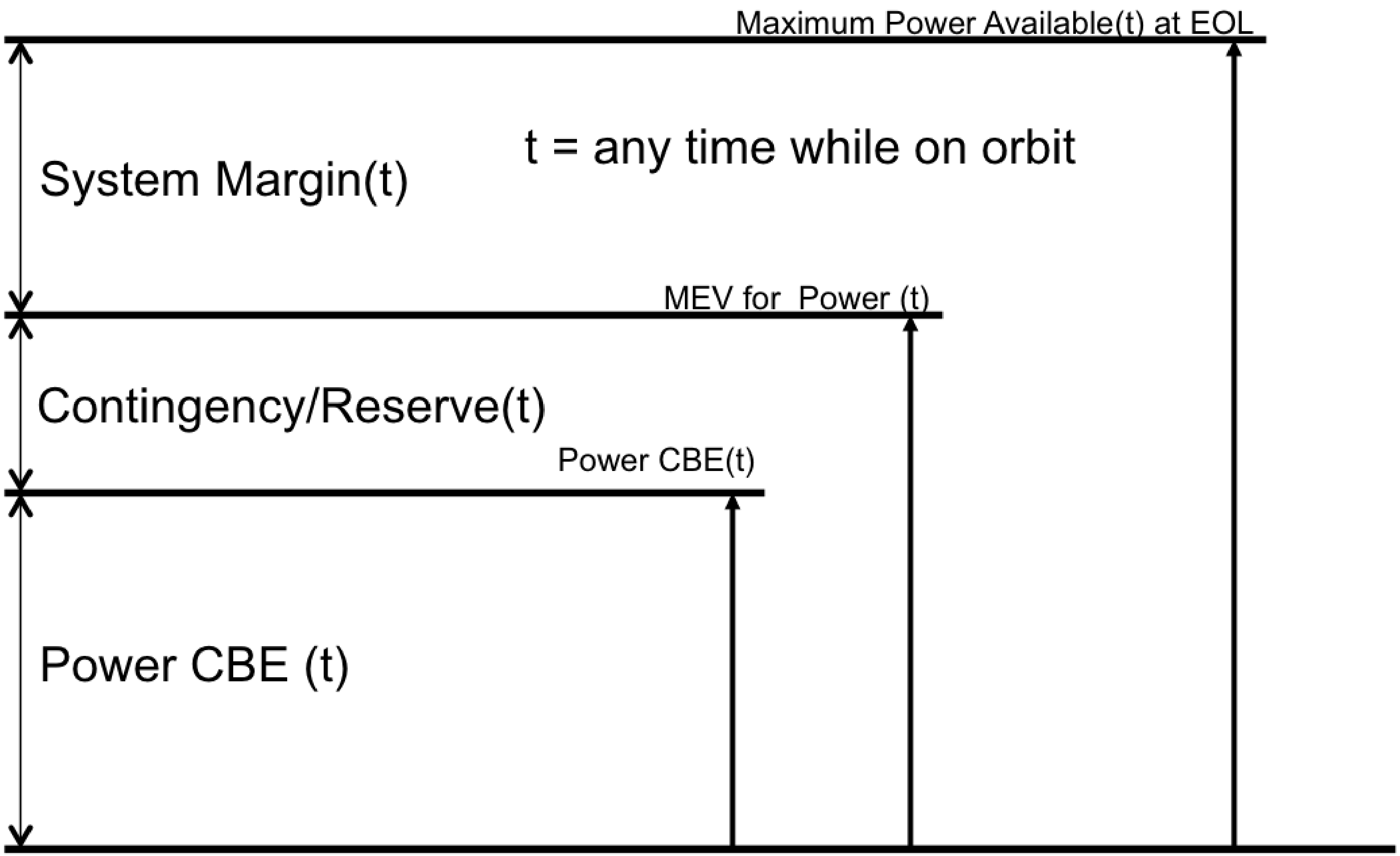


Figure 1.06-2: Power Property Definitions

1.07	End-to-End GN&C Phasing				Systems Engineering		
Rule: **R**	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: Rev. E		**Owner:** Guidance, Navigation, and Control Systems Engineering Branch (591)				**Reference:** ACS Handbook sec. 7.3.3.1	

1.08	**End-to-End Testing**				**Systems Engineering**		
Rule: **P**	System end-to-end testing shall be performed using actual flight hardware and software, wherever practicable, 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: Rev. E		**Owner:** Mission Engineering and Systems Analysis Division (590)				**Reference:** GEVS 2.8	

1.09	Test as You Fly					Systems Engineering
Rule: P	All GSFC missions shall follow a, "Test as You Fly (TYF) - Fly as You Test" approach, throughout all applicable lifecycles.					
Rationale:	Testing of all critical mission-operation elements as they will be flown greatly reduces the risk of encountering negative impacts upon Mission success, from partial to full loss of mission capability.					

Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:		1. Develop the preliminary test plan employing a TLYF philosophy.	1. Develop final test plan, employing a TLYF philosophy.	1. Develop test procedures employing a TLYF philosophy.	1. Perform testing per plan / procedures.	N/A	N/A
Verification:		1. Verify at MDR.	1. Verify at PDR.	1. Verify at CDR.	1. Verify at PER.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Rev. E	Applied Engineering and Technology Directorate (500)	

1.11	Qualification of Heritage Flight Hardware				Systems Engineering		
Rule: **P**	All 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: Rev. E		**Owner:** Mission Engineering and Systems Analysis Division (590)				**Reference:**	

1.14	**Mission Critical Telemetry and Command Capability**				**Systems Engineering**		
Rule: **P**	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 or present exceptions at MCR.	1. Verify or present exceptions at MDR.	1. Verify or present exceptions at PDR.	1. Verify or present exceptions at CDR.	1. Verify or present exceptions at ORR.	1. Verify telemetry capability for events not excepted in Phase D during mission operations.	N/A
Revision Status: Rev. E		**Owner:** Mission Systems Engineering (599)				**Reference:**	

1.17	Safe Hold Mode				Systems Engineering	
Rule: P	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: Rev. E		**Owner:** GN&C Systems Engineering Branch (591)			**Reference:**	

1.19	**Initial Thruster Firing Limitations**				**Systems Engineering**		
Rule: **R**	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:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
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 constraints 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. Establish 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: Rev. E		**Owner:** Guidance, Navigation, and Control Systems Engineering Branch (591)				**Reference:** ACS handbook (Future Reference)	

1.20	Manifold Joints of Hazardous Propellants				Systems Engineering	
Rule: **R**	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:**
Rev. E	Propulsion Branch (597)	Propulsion Handbook (Future Reference)

1.21	Overpressurization Protection in Liquid Propulsion Systems				Systems Engineering		
Rule: **R**	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-suppression 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: Rev. E		**Owner:** Propulsion Branch (597)				**Reference:** Propulsion Handbook (Future Reference)	

1.22	**Purging of Residual Test Fluids**				**Systems Engineering**		
Rule: **R**	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: Rev. E		**Owner:** Propulsion Branch (597)				**Reference:** Propulsion Handbook (Future Reference)	

1.23	Spacecraft 'OFF' Command				Systems Engineering		
Rule: **R**	In a redundant Spacecraft with no hardware failures, no single command shall result in Spacecraft "OFF." In a single string Spacecraft, or a redundant Spacecraft with a failure, no single command shall result in Spacecraft "OFF."						
Rationale:	While redundancy can greatly enhance system reliability and confidence, it also incorporates added complexity to the overall design. Design considerations must take into account the complexity that is added by redundant components, in order to mitigate potential negative effects upon the overall system reliability.						
Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:	1. Complete applicability assessment.	1. Reassess and update applicability. 2. Complete initial compliance assessment, based upon applicability.	1. Reassess compliance. 2. Ensure flow-down traceability to appropriate sub-system in draft technical requirements and Design-To specifications. 3. Define verification approach.	1. Reassess compliance. 2. Ensure flow-down traceability to appropriate sub-system in technical requirements and Design-To specification baselines. 3. Update verification approach.	1. Reassess compliance. 2. Perform verification activity.	N/A	N/A
Verification:	Verify at MCR.	Verify at SRR, MDR, and PNAR.	Verify at PDR and NAR.	Verify at CDR and SIR.	Verify at ORR, SMSR, and FRR.	N/A	N/A
Revision Status: Rev. E		**Owner:** Mission Engineering and Systems Analysis Division (590)				**Reference:** Fault Management PG (Future Reference)	

1.24	Propulsion System Safety Electrical Disconnect				Systems Engineering		
Rule: **R**	An electrical disconnect "plug" and/or set of restrictive commands shall be provided to preclude inadvertent operation of propulsion system 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	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:**
Rev. E	Propulsion Branch (597)	Propulsion Handbook (Future Reference)

1.25	**Redundant Systems**				**Systems Engineering**		
Rule: **P**	When redundant systems or functions are implemented for risk mitigation, the redundant components, or functional command paths, shall be independent, such that the failure of one component or command path does not affect the other component or command path. Critical single point failures due to electrical, thermal, mechanical and functional dependencies should be documented.						
Rationale:	While redundancy can greatly enhance system reliability and confidence, it also incorporates added complexity to the overall design. Design considerations must take into account the complexity that is added by redundant components, in order to mitigate potential negative effects upon the overall system reliability.						
Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:	1. Complete applicability assessment.	1. Reassess and update applicability. 2. Complete initial compliance assessment, based upon applicability.	1. Reassess compliance. 2. Ensure flow-down traceability to appropriate sub-system in draft technical requirements and Design-To specifications. 3. Define verification approach.	1. Reassess compliance. 2. Ensure flow-down traceability to appropriate sub-system in technical requirements and Design-To specification baselines. 3. Update verification approach.	1. Reassess compliance. 2. Perform verification activity.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at SRR, MDR, and PNAR.	1. Verify at PDR and NAR.	1. Verify at CDR and SIR.	1. Verify at ORR, SMSR, and FRR.	N/A	N/A
Revision Status: Rev. E			**Owner:** Mission Engineering and Systems Analysis Division (590)			**Reference:** Fault Management PG (Future Reference)	

1.26	**Safety Inhibits & Fault Tolerance**					**Systems Engineering**	
Rule: **P**	If a system failure may lead to a **Catastrophic Hazard**, the system **shall** have three independent, verifiable inhibits (dual fault tolerant). If a system failure may lead to a **Critical Hazard**, the system **shall** have two independent, verifiable, inhibits (single fault tolerant). Hazards, which cannot be controlled by failure tolerance (e.g., structures, pressure vessels, lines, etc.), must be "Designed for Minimum Risk" (DFMR), and have separate, detailed safety requirements. 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. The external leakage of hazardous propellant is a Catastrophic Hazard. Dynamic seals (e.g. solenoid valves) shall be independently verified as close to propellant loading as possible. Static seals (i.e. crush gaskets, o-rings, etc) are recognized as non-verifiable at the system level. The integrity of these seals shall be controlled by process or procedures consistent with industry standards. Components where fault tolerance is not credible or practical (e.g., tanks, lines, etc.) shall use design for minimum risk instead.						
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. 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	1. Identify proposed design inhibits that preclude hazardous condition and document in preliminary hazard analysis. 2. Present compliance with range safety requirements, including fault tolerance to hazardous events. Document in subsystem design and initial MSPSP.	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. 2. Provide implementation details of the fault tolerance requirements of propulsion system. Document in subsystem design and Intermediate MSPSP.	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. 2. Provide hazard control verification details addressing fault tolerance of propulsion system. Document in subsystem design and Final MSPSP.	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: Rev. E		**Owner:** System Safety Branch (321) & Propulsion Branch (597)				**Reference:** Fault Management PG (Future Reference)	

1.27	**Propulsion System Overtemp Fuse**				**Systems Engineering**		
Rule: **R**	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: Rev. E		**Owner:** Propulsion Branch (597)				**Reference:** Propulsion Handbook (Future Reference) EEE-INST-002 (Update Pending)	

1.28	Unintended Propellant Vapor Ignition					Systems Engineering	
Rule: **R**	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 conditions 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: Rev. E		**Owner:** Propulsion Branch (597)				**Reference:** Propulsion Handbook (Future Reference)	

1.30	Controller Stability Margins				Systems Engineering		
Rule: **R**	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. Verify that the stability analyses presented at CDR encompass the “as built” mass properties and flexible body models. 2. Update CDR analyses if necessary to verify that stability margin requirements are met	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. GN&C and system engineering organizations verify at PSR.	N/A	N/A
Revision Status: Rev. E		**Owner:** Guidance, Navigation, and Control Systems Engineering Branch (591)				**Reference:** ACS Handbook (Update Pending)	

1.31	Actuator Sizing Margins					Systems Engineering
Rule: **R**	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: Rev. E		**Owner:** Guidance, Navigation, and Control Systems Engineering Branch (591)				**Reference:** ACS handbook (Update Pending)	

1.32	Thruster and Venting Impingement				Systems Engineering	
Rule: **P**	Thruster or external venting plume impingement 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: Rev. E		**Owner:** Mechanical Engineering and Systems Analysis Division (590)				**Reference:** JPL D-17868 rev. 2: 2.4.2.2.6	

1.33	Polarity Checks of Critical Components				Systems Engineering		
Rule: **P**	All hardware shall be verified by test or inspection for 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 preliminary 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: Rev. E		**Owner:** Mission Systems Engineering Branch (599)				**Reference:**	

1.34	Closeout Photo Documentation of Key Assemblies				Systems Engineering		
Rule: **P**	Projects shall produce closeout photographic documentation of all 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: Rev. E		**Owner:** Applied Engineering and Technology Directorate (500)				**Reference:**	

1.35	**Maturity of New Technologies**				**Systems Engineering**		
Rule: **R**	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: Rev. E		**Owner:** Applied Engineering and Technology Directorate (500)				**Reference:**	

1.37	Stowage Configuration				Systems Engineering		
Rule: **P**	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:**
Rev. E	Mission Systems Engineering Branch (599)	

2.01	Flight Electronic Hardware Operating Time			Electrical			
Rule: **R**	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: Rev. E		**Owner:** Applied Engineering and Technology Directorate (500)				**Reference:** GEVS 2.3.4	

2.02	EEE Parts Program for Flight Missions				Electrical		
Rule: **P**	A EEE parts program shall be planned 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: Rev. E		**Owner:** Parts, Packaging, and Assembly Technologies Office (562)				**Reference:** EEE-INST-002 (Update Pending)	

2.03	Radiation Hardness Assurance Program			Electrical			
Rule: **P**	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: Rev. E		**Owner:** Flight Data Systems and Radiation Effects Branch (561)				**Reference:**	

2.05	System Grounding Architecture				Electrical		
Rule: **P**	A system grounding design shall be developed and documented 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: Rev. E		**Owner:** Electrical Systems Branch (565)			**Reference:** Electrical System Design Guidelines (Future Reference)		

2.06	System Fusing Architecture				Electrical	
Rule: **R**	A system fusing architecture shall be developed and documented for all missions, including the payloads.					
Rationale:	Lack of a system fusing design may lead to fuse incompatibilities 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 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 requirements (including the payloads) through peer review and at PDR.	1. Verify user implementation at electrical systems peer preview and at CDR.	1. Verify that design verification includes fusing design prior to TRR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Rev. E	Parts, Packaging, and Assembly Technologies Office (562)	EEE-INST-002 (Update Pending)

2.07	End-to-End Test of Release Mechanism for Flight Deployables				Electrical		
Rule: R	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: Rev. E		**Owner:** 540 and 590				**Reference:** GEVS 2.6.2.4.b	

2.12	**Printed Circuit Board Coupon Analysis**				**Electrical**		
Rule: **R**	All flight printed circuit boards (PCBs) shall be verified by coupon testing prior to assembly of components onto the boards.						
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: Rev. E		**Owner:** Electrical Engineering Division (560)				**Reference:** 300-PG-7120.2.2B	

2.13	**Electrical Connector Mating**				**Electrical**		
Rule: **R**	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: Rev. E			**Owner:** Electrical Systems Branch (565)			**Reference:** Electrical Systems Design Guidelines (Future Reference)	

2.14	**Protection of Avionics Enclosures External Connectors Against ESD**				**Electrical**		
Rule: **R**	All avionics enclosures shall be protected from ESD. All external connectors must be fitted with shorting plus or appropriate caps during transportation between locations. Additionally, 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: Rev. E		**Owner:** Electrical Systems Branch (565)			**Reference:** Electrical Systems Design Guidelines (Future Reference)		

2.15	Flight and Ground Electrical Hardware				Electrical		
Rule: R	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 and PSR).	N/A	N/A
Revision Status: Rev. E		**Owner:** Parts, Packaging and Assembly Technologies (562); Materials Engineering (541)				**Reference:** EEE-INST-002 (Update Pending) NASA-STD-6016 (4.2.2.11, 4.2.2.6, 4.2.2.7)	

2.18	**Implementation of Redundancy**				**Electrical**		
Rule: **R**	The implementation of redundant functions shall be accomplished in such a way that any credible single point failure anywhere in the system shall not result in unacceptable degradation of the redundant side. When cross-strapping, the design shall avoid routing of redundant signals through a single connector, relay or integrated circuit.						
Rationale:	While redundancy can greatly enhance system reliability and confidence, it also incorporates added complexity to the overall design. Design considerations must take into account the complexity that is added by redundant components, in order to mitigate potential negative effects upon the overall system reliability. Analysis of cross-strapping networks, using FMECA or other techniques, is essential for these types of systems.						
Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:	1. Complete applicability assessment.	1. Reassess and update applicability. 2. Complete initial compliance assessment, based upon applicability.	1. Reassess compliance. 2. Ensure flow-down traceability to appropriate sub-system in draft technical requirements and Design-To specifications. 3. Define verification approach.	1. Reassess compliance. 2. Ensure flow-down traceability to appropriate sub-system in technical requirements and Design-To specification baselines. 3. Update verification approach.	1. Reassess compliance. 2. Perform verification activity.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at SRR, MDR, and PNAR.	1. Verify at PDR and NAR.	1. Verify at CDR and SIR.	1. Verify at ORR, SMSR, and FRR.	N/A	N/A
Revision Status: Rev. E		**Owner:** Electrical Engineering Division (560)			**Reference:** Electrical Systems Design Guidelines (Future Reference) Fault Management PG (Future Reference)		

2.22	Corona Region Testing of High Voltage Equipment				Electrical		
Rule: **R**	Assemblies containing a High Voltage supply that is not tested through the Corona region shall undergo venting / outgassing analysis to determine when it is safe to turn on and operate after launch.						
Rationale:	Each High Voltage supply is different in its design and the voltage where coronal discharge may occur will vary by the construction and materials used. It will also be dependent on how clean the supply is and how well the outgassing products are vented to space.						
Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:	1. Complete applicability assessment.	1. Reassess and update applicability. 2. Complete initial compliance assessment, based upon applicability.	1. Reassess compliance. 2. Ensure flow-down traceability to appropriate sub-system in draft technical requirements and Design-To specifications. 3. Define verification approach.	1. Reassess compliance. 2. Ensure flow-down traceability to appropriate sub-system in technical requirements and Design-To specification baselines. 3. Update verification approach.	1. Reassess compliance. 2. Perform verification activity.	N/A	N/A
Verification:	1. Verify at MCR.	1. Verify at SRR, MDR, and PNAR.	1. Verify at PDR and NAR.	1. Verify at CDR and SIR.	1. Verify at ORR, SMSR, and FRR.	N/A	N/A
Revision Status: Rev. E		**Owner:** Power Systems Branch (563)				**Reference:** NASA/TP-2006-21413	

3.01	Verification and Validation Program for Mission Software Systems				Software		
Rule: **P**	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. The activities described below provide guidance on recommended software verification and validation activities at each lifecycle phase to supplement the requirements found in NPR 7150.2.						
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 Operations Concept. 2. Identify test tools to be used for software testing (i.e., fidelity, quality, etc.). 3. Update verification and validation approach and associated cost and schedule based on updated requirements.	1. Draft Software Test Plan. 2. Draft SW bi-directional traceability matrix showing SW requirements traced to parent require-ments and to SW components and tests. 3. Plan SW test environment.	1. Complete Software Test Plan. 2. Identify verification and validation program risks. 3. Update SW bi-directional traceability matrix. 4. Set up FSW test environment. 5. Execute FSW tests.	1. Develop detailed test scenarios/cases. 2. Complete bi-directional traceability of requirements to SW design and SW test program. 3. Set up ground SW test environment. 4. Modify FSW test environment as necessary to increase fidelity. 5. Execute ground SW tests.	N/A	N/A
Verification:	1. Verify by inspection through peer reviews and at MCR.	1. Review by analysis the verification and validation approach for the mission through peer review and at MDR.	1. Verify SW development and test program by analysis and through peer review. 2. Verify that budget and schedule accommodate regressions and end-to-end mission testing at SDR and software PDR.	1. Verify by analysis at software CDR.	1. Verify by analysis through peer review and at Test Readiness Review.	N/A	N/A
Revision Status: Rev. E		**Owner:** Software Systems Engineering Branch (581)				**Reference:** NPR 7150.2	

3.02	Elimination of Unnecessary and Unreachable Software				Software		
Rule: **P**	An analysis of unnecessary and/or unreachable code, as defined per Table 3.02-1, shall be performed on the intended flight load for launch. The analysis shall identify all instances (areas) of unnecessary/unreachable flight code, the general functionality associated with the code, the reason each is intended to be left within the flight load, and the justification (e.g. mitigating action) that explains why the included code does not provide a risk to the mission. The focus is on technical risk to the long-term mission, not cost.						
Rationale:	There are significant benefits to re-using software from past missions but each mission has different requirements and re-using heritage software often carries forward software not required by the current mission. Unnecessary and unreachable software can also occur within a mission's lifecycle as system and software requirements change during the software development process. Unnecessary and unreachable software is typically not verified or validated as part of the current mission test programs, as a mission is only required to verify its mission requirements. This creates the potential for negative side-effects, costs, and risks during the current mission's on-orbit life. Table 3.02-2 provides sample types of unnecessary or unreachable code.						
Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:	N/A	1. Document that a FSW Reuse Plan and risk assessment of unnecessary and/or unreachable code will be developed.	1. Document the FSW Reuse Approach and the plan for managing unnecessary and/or unreachable code in the FSW Management/Development Plan(s). 2. Identify and document code capabilities/ requirements that are not required for the current mission but are intended to be included in the FSW product(s). 3. Provide initial risk identification, assessment & anticipated mitigation technique for each known type of unnecessary/ unreachable code. 4. Present analysis at FSW reviews.	1. Analyze the potential risk of leaving the code in the flight product rather than removing it. 2. Remove unnecessary and unreachable software that creates risk. 3. Update software verification plans if justified to reduce risk. 4. Present analysis and risk mitigations at FSW reviews. 5. Update the documentation of unnecessary and unreachable code associated with the intended flight products.	1. Update and analyze the documentation of unnecessary and unreachable code from heritage and newly developed flight products. 2. Remove unnecessary and unreachable software that creates risk. 3. Update software verification plans if justified to reduce risk. 4. Present analysis at FSW reviews.	N/A	N/A
Verification:	N/A	Verify at MDR.	1. Verify at FSW SRR and FSW PDR. 2. Verify at SDR and PDR.	1. Verify at CDR. 2. Verify at FSW CDR.	1. Verify at FSW Acceptance Test Review. 2. Verify at PSR and FRR.	N/A	N/A
Revision Status: Rev. E		**Owner:** Software Systems Engineering Branch (581) Flight Software Systems Branch (582)				**Reference:**	

Table 3.02-1 Unnecessary and Unreachable Software Definitions

Term	Definition
Source Code	Code produced by software engineers and by code generation tools (e.g. Matlab, Rational Rose).
Unnecessary Software	Source code that is not linkable to any mission software requirements. Classic examples include: 1) functions in a mathematic library not applicable for the mission; and, 2) source code that interfaces with hardware that is not present in the current mission design.
Unreachable Software	Source code that should never be executed within normal software execution. A classic example would be source code that is guarded by a control statement or statements that should never be true; hence, the software is unreachable.
Note	Well known Commercial Off-the-Shelf (COTS) and Open Source products with flight heritage and unnecessary and unreachable features are to be included in the analysis and will likely not require extensive mitigation actions.

Table 3.02-2 Sample Types of Unnecessary and Unreachable Software

Sample Types	Definition
Parameter Checking	A section of software that can never be executed because pre-conditions should never be met. For example, a properly developed function will validate all parameters to ensure the function doesn't perform any illegal actions based upon the input parameters. However, it is possible to write the software system such that it never calls the function with invalid input parameters. In such a case, the error condition checks within the function should never execute.
Unused Design Capability	Application Program Interfaces (API) are developed to promote software reuse. For example, an Operating System (OS) API will have interface calls for dealing with semaphores (e.g. *create, give, take*, etc). If a new mission does not require the use of semaphores, then these OS API functions will never be executed.
Unused Reuse Capabilities	A reused software component/library or set of reused software components/libraries will typically contain capabilities and features not required by a mission.
Debug/Test Features	Debug and test features, which are not a required part of the operational system, are often required to test the software system. For example, debug software is often used in conjunction with testing Error Detecting And Correcting (EDAC) memory. It is extremely difficult to inject correctable and uncorrectable errors into EDAC memory, whereas a test command can easily inject these erroneous conditions to verify that the application software handles and reports the EDAC errors correctly.

3.03	High Fidelity Interface Simulation Capabilities				Software	
Rule: **P**	A high fidelity software simulation capability for each external interface to FSW shall be provided in the FSW development/maintenance environments. 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 FSW 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 observation at SW SRR. 2. Verify flight simulation capability defined to accommodate test of all FSW data I/O, FSW modes, nominal and anomalous conditions, and load/stress tests for each flight CPU. 3. Verify simulator development and FSW schedules are consistent.	1. Verify by observation at software CDR.	1. Verify by observation at MOR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Rev. E	Flight Software Systems Branch (582)	

3.04	Independent Software Testing				Software		
Principile: **P**	Software functional/requirements and comprehensive performance verification/validation testing shall be performed by qualified testers that are independent of the software designers and developers. NOTE: For small projects, members of the same development team can perform independent testing as long as the assigned testers have not been involved in any part of the design and development of the software components being tested.						
Rationale:	Ideally, an independent team should develop the software test plan and verification/validation test procedures, and execute the tests. Frequently the software development team will be used to perform these functions as a means to reduce cost and schedule. Having authored the code, they already know how it should function and can quickly perform the testing activities. The independent test team approach is non-biased, with an end-user perspective, and specialized test teams frequently have greater expertise on various test tools and technologies; thus, providing a more thorough and comprehensive test program. An independent test team ensures adequate time for testing because there is a clear demarcation between development, and testing. However, if utilizing an independent test team is not feasible, at a minimum, the use of independent testers who were not involved with the software design and development process allows alternate interpretations of requirements and multiple approaches to testing.						
Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:	N/A	Project provides WBS for Test Team Lead. Test Team Lead is given signature authority on the Mission Flight Software Require-ments document. Test Team Lead reviews requirements for testability, plus compatibility with the Operations Concept. Software Test Plan is written and approved.	Software Test Plan is updated as needed. Requirements to Test Procedures Matrix, is drafted.	Software Test Team staffed. Ensure members are independent from development team. Continue to update Requirements to Test Procedures Matrix and begin drafting test procedures.	Test procedures drafted, reviewed, and executed.	Independent verification/validation testing completed.	N/A
Verification:	N/A	Verify at SRR.	Verify at PDR.	Verify at CDR.	Verify at TRR.	N/A	N/A
Revision Status: Rev. E		**Owner:** Software Engineering Division (580)				**Reference:**	

3.05	**Flight / Ground System Test Capabilities**				**Software**		
Rule: **P**	Access to flight system interface and functional capabilities, provided either by the spacecraft or by spacecraft simulators, shall be negotiated with all stakeholders, including the ground system and operations teams. Schedules and agreements should address the spacecraft and spacecraft simulators at all levels of fidelity.						
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 operations team must be able to develop and validate a variety of operations products, such as procedures, databases, display pages, and launch scripts. The operations 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 system and flight operations teams.	1. Develop preliminary simulation concepts.	1. Generate preliminary simulator requirements and identify long lead procurement items. 2. Establish preliminary agreements on simulator usage between all stakeholders. 3. Identify critical ground system and operations readiness tests along with estimated durations and equipment dependencies, and incorporate into the mission I&T schedule.	1. Complete simulator requirements, design, and delivery plan/schedules. 2. Refine previously established agreements on simulator and spacecraft access times 3. Ensure all ground system and operations readiness test details, including test durations and equipment dependencies, are incorporated into the detailed I&T plans and schedules.	1. Provide simulator and S/C hardware access for both ground system verification and validation, and for operations teams to prepare for 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.	N/A	N/A
Revision Status: Rev. E		**Owner:** Software Systems Engineering Branch (581)				**Reference:**	

3.06	**Dedicated Engineering Test Unit for Flight Software Testing**				**Software**		
Rule: **P**	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 (High Fidelity Interface Simulation Capabilities). 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 ensures that ETU development and delivery schedule is consistent with FSW development team need dates. 3. FSW team develops ETU acceptance criteria for ETU deliveries.	1. Review ETU design. 2. Review ETU delivery schedule.	1. FSW team verifies availability of ETUs to meet FSW development and test schedules. 2. FSW team lead accepts ETU deliveries and verifies functionality.	1. FSW team reviews and provides inputs on ETU maintenance plan.	N/A
Verification:	N/A	1. Verify by observation at MDR that ETU-quality FSW testbeds 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 observation at SDR and SW SRR that: a) FSW ETU testbed(s) represent maturing flight architecture; b) minimum 1 testbed with full ETU fidelity is costed and delivery schedule is consistent with FSW needs; and, c) I&T plans minimize sharing ETU, or dedicated ETU is provided.	1. Verify by observation at SW PDR that: a) delivery plans for ETU-quality FSW testbed(s) are consistent with FSW development needs; and, b) I&T plans require minimal use of a shared ETU, or I&T has their own dedicated ETU.	1. Verify by observation at SW CDR that: a) ETU-quality FSW testbed(s) have been delivered to FSW team; and, b) ETU FSW testbed is confirmed to be adequate by FSW staff for on-orbit maintenance and operations support.	1. Verify by observation at FOR that: a) FSW ETU testbeds have been moved to their long-term environment for FSW maintenance & operations support; and, b) system administration, facility, and hardware support are in place.	N/A
Revision Status: Rev. E		**Owner:** Flight Software Systems Branch (582)				**Reference:**	

3.07	**Flight Software Margins**				**Software**		
Rule: **R**	Flight software resource margins shall be maintained in accordance with Table 3.07-1 and presented at Key Decision Point (KDP) milestone reviews.						
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. 3. If margins are below guidelines at PDR, provide rationale as to how mission requirements can still be met and necessary mitigation and/or corrective actions needed.	1. Track development to design margins. If margins are below guidelines at CDR, provide rationale as to how meeting mission requirements are not at risk.	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: Rev. E		**Owner:** Software Systems Engineering Branch (581)				**Reference:** Table on next page	

Resource Margins for Flight Software Development

The numbers provided 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.

Table 3.07-1. Flight Software Margins

Mission Phase	**FSW SRR**	**FSW PDR**	**FSW CDR**	**Ship/Flight**
Method	Estimate	Analysis	Analysis/ Measured	Measured
Average CPU Usage	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%

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

Note: Selecting which column to use at a particular time is not always obvious. Generally, one should pay more attention to the "Method" row rather 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.

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 50 ms 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. (Question: Should there be different recommended numbers for 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 are 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.

<table>
<tr><td>3.10</td><td colspan="4">Flight Operations Preparations and Team Development</td><td colspan="3">Software</td></tr>
<tr><td>Rule:
P</td><td colspan="7">Experienced operations personnel shall participate as early as possible during mission development, preferably during the mission operations concept phase and the development of specifications for the spacecraft and/or instruments which impact operations. To prepare and train the FOT, they shall participate in flight operations readiness tests that are specified in Table 3.10. Note that these serve as guidelines and are not intended to be prescriptive.</td></tr>
<tr><td>Rationale:</td><td colspan="7">Involving experienced operations personnel early in the mission helps ensure that the mission design will be considerate of operational requirements and practicalities. It will allow the operations team to become intimately familiar with the mission design, including design rationale, spacecraft limitations, and operating constraints. Involving FOT members during mission operations readiness tests gives them a great deal of hands-on experience with the observatory prior to launch thereby enhancing their training; and, the FOT will be able to assume their responsibility with a reasonable degree of skill and knowledge for conducting on-orbit spacecraft operations.</td></tr>
<tr><td>Phase:</td><td><A</td><td>A</td><td>B</td><td>C</td><td>D</td><td>E</td><td>F</td></tr>
<tr><td>Activities:</td><td>1. Assess the flight operations team's role throughout the mission lifecycle. Flight operations experts develop preliminary operations concepts.</td><td>1. Flight operations and software experts support the development of more detailed operations concepts, and flight/ground architecture.
2. Update mission design estimates.</td><td>1. Identify roles and responsibilities for FOT members.
2. Review and update operations concepts and identify details on approach to operations team support.
3. Conduct peer review of flight/ground architecture.
4. Develop test plans (see Table 3.10).</td><td>1. Involve FOT in test plan development.
2. Support the completion of the operations concepts.</td><td>1. Ensure all FOT members gain knowledge and experience on ground systems during I&T.
2. Conduct tests (see Table 3.10).
3. Complete flight operations plan.</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Verification:</td><td>1. Verify at MCR:
a) Ensure flight development experts were consulted during mission formulation.
b) Ensure that operations concept covers flight operations team's role during entire mission lifecycle.</td><td>1. Verify at MDR:
a) Flight operations concepts are sound.</td><td>1. Verify at PDR:
a) Flight operations roles are defined and personnel identified.
b) Flight and ground system interfaces to all mission support elements are well defined and documented.</td><td>1. Verify at CDR:
a) Flight operations experts have been consulted on the overall ground system design.
b) The project has completed full mission lifecycle design to include extended mission and mission termination phases.</td><td>1. Verify at MOR and FOR:
a) MRT items completed by MRR.</td><td>N/A</td><td>N/A</td></tr>
<tr><td colspan="3">Revision Status:
Rev. E</td><td colspan="4">Owner:
Flight Systems Integration and Test Branch (568)
Software Systems Engineering Branch (581)
Mission Validation & Operations Branch (584)</td><td>Reference:</td></tr>
</table>

Table 3.10 Simulation Types and Minimum Number of Successful Simulations/ Test Hours versus Mission Class

Simulation Type	Class A	Class B	Class C	Class D
End-to-end	5 tests	4 tests	3 tests	3 tests
Day-in-the-life (focused on instrument)	3 tests	2 tests	1 test	1 test
Day-in-the-life (focused on spacecraft)	3 tests	2 tests	1 test	1 test
Launch & early-orbit phase	4 tests	3 tests	2 test	2 test
Critical operations	each planned critical operation included in at least 2 simulations, 1 of which is in LE&O phase	each planned critical operation included in at least 2 simulations, 1 of which is in LE&O phase	each planned critical operation included in at least 1 simulation	each planned critical operation included in at least 1 simulation
Contingency operations	each contingency/critical operation included in at least 2 simulations, one of which is in LE&O phase	each contingency/critical operation included in at least 2 simulations, one of which is in LE&O phase	each contingency/critical operation included in at least 1 simulation	each contingency/critical operation included in at least 1 simulation
Flight system operation with spacecraft	400 hours	300 hours	250 hours	200 hours

Note: Simulations and tests may be performed in parallel or in combination, if appropriate, to satisfy above goals.
End-to-end test implies spacecraft-to-Control Center interface and includes all supporting elements, i.e., Science Data Center, communications network, etc. Ground Readiness Tests (GRTs) are not included in this table.

3.11	**Long Duration And Failure Free System Level Test of Flight and Ground System Software**				**Software**		
Rule: **R**	Ground test of the fully integrated FSW and ground system shall include demonstration of error free operations-like scenarios over an extended time period. The minimum duration of uninterrupted FSW system-level test (on the highest fidelity FSW testbed) and ground system operations is 72 hours for Class A and B missions; 48 hours for Class C missions; and, 36 hours for Class D missions, respectively.						
Rationale:	Frequent restart of FSW and the ground system during ground tests may mask problems which will only occur following extended execution of these systems. Also, ground system stress testing is needed to ensure reliable operation. The number of hours specified is based on discussion with senior-level engineers, and reflect best practices accumulated over a period of 15 years.						
Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:	N/A	N/A	1. Complete Draft FSW and Ground System Test Plans.	1. Complete Final FSW and Ground System Test Plans.	1. Complete and execute test plans, to include long duration FSW and ground system testing.	N/A	N/A
Verification:	N/A	N/A	N/A	1. Verify at CDR that FSW and Ground System Test Plans are baselined and that they include long-duration testing.	1. Verify at MOR: a) The longest duration, uninterrupted FSW system-level test (on the highest fidelity FSW testbed), and ground system testing have been completed. b) Verify at FOR that realistic post-launch science operations and safehold operations were represented by the long duration test(s).	N/A	N/A
Revision Status: Rev. E		**Owner:** Software Systems Engineering Branch (581) Flight Software Systems Branch (582)				**Reference:**	

3.13	Maintenance of Mission Critical Components			Software			
Rule: **P**	The updating of mission critical components during the mission operations phase (including any combination of hardware platforms, hardware devices, and software code) shall not compromise the capability of the system to meet mission requirements. Missions shall provide sufficient quantities of flight and ground resources to allow development, test, and operations activities to be conducted without compromising mission availability requirements.						
Rationale:	Missions should provide sufficient resources to allow updates to mission critical/high availability components, such as flight software and ground system components directly supporting space-ground communications, to be developed and tested without compromising operations. Missions should also ensure against inadvertent updates or deliberate concurrent updates of mission critical/high availability components. For example, under no circumstances should prime and redundant components, such as prime and backup flight software code images, be modified/updated concurrently, before the operational performance of the change is properly verified in a single unit.						
Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:	N/A	N/A	1. Ensure preliminary flight and ground system design contains adequate strings or quantities of equipment to satisfy both maintenance and mission availability requirements during Phase E.	1. Ensure flight and ground system level design does not allow modification of software between one CPU and its redundant elements. 2. Ensure final flight and ground system design contains adequate strings or quantities of equipment to satisfy both continuing maintenance and mission availability requirements during Phase E.	1. Ensure flight and ground system maintenance plans define approach for development and test of changes to mission critical functions before committing to operations.	N/A	N/A
Verification:	N/A	N/A	Verify at PDR.	1. Verify at CDR.	Verify at MOR.	N/A	N/A

Revision Status:	**Owner:**	**Reference:**
Rev. E	Software Systems Engineering Branch (581)	

3.14	Command Procedure Changes				Software	
Rule: **P**	Command procedures and/or scripts, and mission databases (onboard 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 command loads to perform nominal operations may require less test rigor based on experience of senior engineers.)					
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 operations and sustaining engineering plans address the items defined in this rule.	1. Implement CM plans. Make changes to procedures and databases as necessary based on changing mission needs/requirements.	1. Implement CM plans. Make changes as necessary based on changing mission needs/requirements (i.e., aging S/C, etc.).	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:**
Rev. E	Software Systems Engineering Branch (581) Flight Software Systems Branch (582) Mission Validation & Operations Branch (584)	

4.03	**Factors of Safety for Structural Analysis and Design, and Mechanical Test Factors & Durations**				**Mechanical**		
Rule: **R**	Structural analysis and design factors of safety shall apply to all systems in accordance with GEVS Section 2.2.5. The project shall employ the mechanical test factors and durations in accordance with GEVS Section 2.2.4.						
Rationale:	This will provide confidence that the hardware will not experience failure or detrimental permanent deformation under test, ground handling, launch, or operational conditions. 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	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. 2. Formulate test plans for all structural elements incorporating the requirements described in the principle.	1. Employ design factors of safety in accordance with GEVS 2.2.5. 2. Write Test plans and execute tests	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 these factors of safety, test factors, and test durations at CDR.	1. Verify these factors of safety, test factors, and test durations at EPR, PER, and PSR.	N/A	N/A
Revision Status: Rev. E		**Owner:** Mechanical Systems Analysis and Simulation Branch (542) Mechanical Engineering Branch (543)				**Reference:** GEVS 2.2.4 & 2.2.5	

4.06	**Validation of Thermal Coatings Properties**				**Mechanical**		
Rule: **R**	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: Rev. E		**Owner:** Contamination & Coatings Engineering Branch (546)			**Reference:** NASA/TP-2005-212792 Spacecraft Thermal Control Coatings References; Lonny Kauder		

4.07	Solder Joint Intermetallics Mitigation						Mechanical
Rule: **R**	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 concentration 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: Rev. E		**Owner:** Materials Engineering Branch (541)				**Reference:** NASA-STD-8739.3	

4.08	Space Environment Effects on Material Selection				Mechanical		
Rule: **R**	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: Rev. E		**Owner:** Materials Engineering Branch (541)				**Reference:** NASA-STD-6016 (4.2.3.7)	

4.10	Minimum Workmanship				Mechanical		
Rule: **R**	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: Rev. E		**Owner:** Mechanical Systems Analysis and Simulation Branch (542)				**Reference:** GEVS Section 2.4.2.5	

4.11	**Testing in Flight Configuration**				**Mechanical**		
Rule: **R**	Mechanical environmental testing (sine, random, & acoustic, shock, etc.) of flight hardware shall be performed with the test article in the flight like configuration. Mechanisms are configured for flight, and the flight or flight like blankets and harness shall be present for test.						
Rationale:	Testing in-flight configuration ensures that hardware which 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: Rev. E		**Owner:** Mechanical Systems Analysis and Simulation Branch (542)				**Reference:** GEVS Sections 2.4.	

4.12	Structural Proof Testing				Mechanical		
Rule: **R**	Primary and secondary structures fabricated from nonmetallic composites, beryllium, or containing bonded joints or bonded inserts shall be proof tested in accordance with GEVS-SE 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: Rev. E		**Owner:** Mechanical Systems Analysis and Simulation Branch (542)				**Reference:** GEVS 2.4.1.4.1	

4.14	**Structural and Mechanical Test Verification**				**Mechanical**		
Rule: **R**	Structural and Mechanical Test Verification program shall comply with GEVS-Table 2.4-1, Structural and Mechanical Verification Test Requirements.						
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 Engineering Peer Review and at PDR.	1. Verify through CDR, and Engineering Peer Review and at CDR.	1. Verify at PER, Engineering Peer Review, and PSR.	N/A	N/A
Revision Status: Rev. E		**Owner:** Mechanical Engineering Branch (543), Mechanical Systems Analysis and Simulation Branch (542)				**Reference:** GEVS Sections 2.4.	

4.15	Torque Margin				Mechanical	
Rule: **R**	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: Rev. E	**Owner:** Mechanical Engineering Branch (543)	**Reference:** GEVS 2.4.5.3

4.18	**Deployment and Articulation Verification**				**Mechanical**		
Rule: **P**	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: Rev. E		**Owner:** Mechanical Engineering Branch (543)				**Reference:**	

4.20	Fastener Locking				Mechanical		
Rule: **P**	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 fasteners 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	NA
Verification:	N/A	N/A	N/A	1. Verify at CDR.	1. Verify at PER and PSR.	N/A	N/A
Revision Status: Rev. E		**Owner:** Electromechanical Systems Branch (544)				**Reference:**	

4.21	**Brush-type Motor Use Avoidance**				**Mechanical**		
Rule: **P**	Designs shall avoid brush-type motors for critical applications with very low relative humidity, or vacuum operations. Intentionally excluded from this rule are contacting sensory and signal power transfer devices such as potentiometers and electrical contact ring assemblies (slip rings, roll rings), etc.						
Rationale:	The operating life of the brush-type motors can be significantly decreased in extremely dry or vacuum conditions. Critical components relying on brush-type motors could be rendered inoperable due to excessively worn brushes or brush particulate contamination.						
Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:	N/A	1. Identify all motor applications and motor types	1. Mechanisms and Controls shall be designed to avoid the use of brush-type motors. If Brush-type motor is used, it shall be carefully scrutinized, and an alternative motor design and selection trade study shall be seriously considered.	1. Finalize motor and control design	1. Trending Motor Performance during Integration and Test activities.	N/A	NA
Verification:	N/A	1. Verify at EPR & MDR	1. Verify at EPR and PDR	1. Verify at EPR and CDR. Conducted Life Test consistent with Gold Rule 4-23, Life Test Verification	1. Verify at EPR, PER and PSR.	N/A	N/A
Revision Status: Rev. E		**Owner:** Electromechanical Systems Branch (544)				**Reference:**	

4.22	**Precision Component Assembly**			**Mechanical**			
Rule: **P**	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: Rev. E		**Owner:** Electromechanical Systems Branch (544)				**Reference:**	

4.23	Life Test				Mechanical		
Rule: **R**	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: Rev. E		**Owner:** Electromechanical Systems Branch (544)				**Reference:** GEVS 2.4.5.1	

4.24	Mechanical Clearance Verification			Mechanical			
Rule: **P**	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 impingement, 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 clearances at appropriate integration milestones. 2. Conduct inspections and measurements.	1. Demonstrate that mechanical integration plans include provisions for verifying mechanical clearances 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: Rev. E		**Owner:** Electromechanical Systems Branch (544)				**Reference:**	

4.25	Thermal Design Margins				Mechanical		
Rule: **R**	Thermal design shall provide adequate margin between stacked worst-case flight predictions and component allowable flight temperature limits per GEVS 2.6 and 545-PG-8700.2.1A. 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:**
Rev. E	Thermal Engineering Branch (545)	GEVS 2.63 545-PG-8700.2.1A

4.27	Test Temperature Margins				Mechanical		
Rule: **R**	Components and systems shall be tested beyond allowable flight temperature limits, to proto-flight or acceptance test levels as appropriate as specified in GEVS section 2.6, which specifies margins for passively and actively controlled hardware. Note that at levels of assembly above component, full specified margins may not always be achievable for all components due to test setup limitations; in these cases, the expected test levels shall be approved by the GSFC Project, and shall be presented at the earliest possible formal review, no later than PER.						
Rationale:	The test program shall ensure that the flight hardware functions properly (meets performance requirements) at temperatures more severe than expected during the mission to demonstrate robustness to meet its mission lifetime requirements. (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 the Reference (GEVS 2.6).	1. Component, subsystem, and system proto-flight thermal vacuum test temperatures shall be specified with the required margin as stated in the Reference (GEVS 2.6).	1. Components and systems shall undergo proto-flight thermal vacuum testing with the required margin as stated in the Reference (GEVS 2.6). Yellow and Red limits for flight temperature telemetry database shall be consistent with actual proto-flight system thermal vacuum (TV) test temperatures.		
Verification:	N/A	N/A	1. Verify at PDR.	1. Verify at CDR.	1. Verify results of component and subsystem thermal vacuum (TV) tests, and present plans for system TV test at PER. 2. Verify results of system thermal vacuum test at PSR. 3. Verify flight database limits at MRR and/or FRR.		
Revision Status: Rev. E		**Owner:** Thermal Engineering Branch (545)				**Reference:** GEVS 2.6	

4.28	**Thermal Design Verification**				**Mechanical**		
Rule: **R**	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: Rev. E		**Owner:** Thermal Engineering Branch (545)				**Reference:** GEVS 2.6	

4.29	**Thermal-Vacuum Cycling**				**Mechanical**		
Rule: **R**	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. For an instrument, a minimum of four (4) of these eight (8) Thermal Vacuum cycles shall be performed at the 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). For units where there is an institutional or organizational delivery to an interim level of assembly, pre-delivery testing should include a minimum of 4 cycles.						
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: Rev. E		**Owner:** Applied Engineering and Technology Directorate (500)				**Reference:** GEVS 2.6.2.4.b	

5.04	Instrument Testing for Multipaction						Instruments
Rule: **P**	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 multipaction 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:**
Rev. E	Microwave Instrument Technology Branch (555)	

5.05	**Fluid Systems GSE**				**Instruments**		
Rule: **R**	Fluid systems GSE used to pressurize flight systems shall be compliant with the fault tolerance requirements of Rule 1.26.						
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 assessment 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: Rev. E		**Owner:** Cryogenics and Fluids Branch (552)			**Reference:** Fault Management PG (Future Reference) NPR 8715.3		

5.06	Flight Instrument Characterization Standard				Instruments	
Rule: **P**	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: Rev. E		**Owner:** Detector Systems Branch (553)			**Reference:**	

5.08	Laser Development Contamination Control				Instruments		
Rule: **P**	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: Rev. E		**Owner:** Laser and Electronic Optics Branch (554)				**Reference:**	

5.09	Cryogenic Pressure Relief				Instruments		
Rule: R	Stored cryogen systems (and related GSE) shall be compliant with the fault tolerance requirements of Rule 1.26.						
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: Rev. E		**Owner:** Cryogenics and Fluids Branch (552)			**Reference:** Fault Management PG (Future Reference) NPR 8715.3		

GLOSSARY AND ACRONYM GUIDE

Anomaly	An unanticipated or unpredicted behavior that occurs as a discrete episode
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
API	Application Program Interfaces
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.
CCP	Contamination Control Plan
CDR	Critical Design Review
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)
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit

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.
Debug Features	With the best of intentions of helping to debug software and/or hardware problems, there exists a feature that is not needed by the operation software, but was accidentally or intentionally left in the code for debug purposes. (May be advertised or unadvertised; May be documented or undocumented; May be tested or untested).
DR	Decommissioning Review
EDAC	Error Detecting and Correcting
EEE	Electrical Engineering
EEPROM	Electrically Erasable Programmable Read-Only Memory
EGSE	Electrical Ground Support Equipment
Element	A portion of a hardware or software unit that is logically discrete
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
FIFO	First-In / First-Out

FOR	Flight Operations Review
FOS	Factors of Safety
FOV	Field of Vision
FRR	Flight Readiness Review
FSW	Flight Software
GEVS	General Environmental Verification Specification
GN&C	Guidance, Navigation, and Control
GPR	Goddard Policy Requirement
GRT	Ground Readiness Test
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)
HW	Hardware
ICD	Interface Control Document
I/F	Interface
I/O	Input / Output
ISR	Interrupt Service Routine

ITU	Integrated Test Unit
I&T	Integration and Testing
KDP	Key Decision Point. The event at which the Decision Authority determines the readiness of a program/project to progress to the next phase of the life cycle (or to the next KDP).
LE&O	Launch and Early Orbit
LRR	Launch Readiness Review
OS	Operating System
Margin	The amount by which hardware capability exceeds requirements (Ref: GEVS 1-7)
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

MRR	Mission Readiness Review
MRT	Mission Readiness Test
ms	milliseconds
M&P	Materials and Processes
NPR	NASA Procedural Requirements
ORR	Operational Readiness Review
Payload	An integrated assemblage of modules, subsystems, etc., designed to perform a specified mission in space (Ref: GEVS 1-7)
PCI	Peripheral Component Interconnect
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
PROM	Programmable Read-Only Memory
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

RAM	Random Access Memory
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)
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)
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)
SW	Software
TBD	To Be Determined
Test Features	With the best of intentions of helping to test and validate the software, there exists a feature that is not needed by the operational software, but is desirable to have for testing purposes. (May be advertised or unadvertised; May be documented or undocumented; May be tested or untested)
TLYF	Test Like You Fly
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
UART	Universal Asynchronous Receiver / Transmitter
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)

DOCUMENT HISTORY LOG

Revision	Effective Date	Description
-	**10-Dec-04**	Baseline
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. Revised Principle: 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). Revised Principle: *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.* 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.*
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
C.1	**12-Dec-06**	New Systems Engineering Rule: 1.09 Test Like You Fly
		New Software Rule: 3.02 Elimination of Dead Software Code
		Table of Contents – Updated to Reflect Changes/Insertion for Rules 1.09, 3.02
		Glossary – Added Definitions for Dead Software/Code & Acronym for "Test Like You Fly"
		Table of Contents – Typographical error in Rule 1.08 title corrected
		[Rule 1.14] Revised Verification for Phases pre-A → E.
C.2	**12-Dec-06**	Introduction – Corrected language for GPR 8070.4
		Table 1.06-1 – Deleted "RF Link" Margin

Revision	Effective Date	Description
D	**01-March-08**	Table of Contents – Revised to Reflect Rev D Changes
		Rule 1.03 – Revised "Principle" Statement
		Rule 1.11 – Revised "Principle" Statement
		Rule 1.16 – Revised "Principle" Statement
		Rule 3.07 – Revised "Title" and "Principle" Statement
		Rule 5.05 – Revised "Principle" Statement
		Rule 5.09 – Revised "Principle" Statement
		New Systems Engineering Rule: 1.18 Physically Co-Located Redundant Elements
		New Systems Engineering Rule: 1.23 Spacecraft "OFF" Command
		New Systems Engineering Rule: 1.25 Redundant Systems
		New Electrical Engineering Rule: 2.08 Secondary Circuit Failures
		New Electrical Engineering Rule: 2.18 Redundant Functions
		New Electrical Engineering Rule: 2.19 Multiple Circuit Power Bus Loss
		New Electrical Engineering Rule: 2.20 Single Control Line Dependency
		New Electrical Engineering Rule: 2.21 Gross Failure of Integrated Circuits
		New Electrical Engineering Rule: 2.22 Corona Region Testing of High Voltage Equipment
		Table 3.07-1 – Revised first paragraph
E	**13-July-09**	Major Revision / Rewrite
E	**03-Aug-09**	Administrative Changes Only - Rule 1.06 (pages 12 thru 16) and associated tables, modified throughout for clarity, regarding system margin.

This page intentionally left blank.