GODDARD TECHNICAL STANDARD	GSFC-STD-1000I
Goddard Space Flight Center Greenbelt, MD 20771	Approved: 8/19/2025 Expiration Date: 8/19/2030 Superseding GSFC-STD-1000H

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 I

Approved by:

Director of Engineering and Technology
Goddard Space Flight Center

Director of Safety and Mission Assurance
Goddard Space Flight Center

Director of Flight Projects
Goddard Space Flight Center

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 engineering principles and practices which have evolved in the Goddard community and are intended to describe foundational principles without being overly prescriptive of an implementation "philosophy." Each GOLD Rule specifies guidance in the form of a Rule Statement, along with supporting rationale. The GOLD Rules provide visibility to GSFC Senior Management when a project deviates from standard GSFC "best practices".

Scope and Process:

The GOLD Rules are intended to apply to all space flight projects (and where applicable, associated ground projects) regardless of implementation approach or mission classification (except where explicitly noted). Although not required, an a priori Mission Exceptions List (MEL) may be proposed at the start of a Program and/or Project, to highlight rules which **do not apply** to that mission. It is not a list of deviations from the guidelines. The GOLD rules MEL should be submitted to the Engineering Technology Directorate and Division Chief Engineers for review. If a MEL is submitted, additional assessments will not be required for exceptions covered by the MEL unless changes occur to the underlying basis for exception. For rules that include multiple elements (e.g. 1.09 "Test as You Fly"), assessments should be discussed for each deviation; acceptance of one deviation does not remove the responsibility to discuss additional deviations as they are discovered. 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 within that program.

The designated project Engineering Technical Authority (ETA) should assess compliance with the guidance and should provide rationale for deviating from GSFC Best Practices and an assessment of any additional risk and mitigations for the approach. The appropriate mission ETA shall conduct an engineering peer review assessment against the GOLD Rule guidelines with the ETD Directorate and Division Chief Engineers and report deviations from that guidance and associated risk assessments at major project milestone reviews. Additionally, subsystem engineering peer reviews should include a discussion of GOLD rules compliance. Missions that are classified as being tolerant of higher risk (e.g. class D, 7120.8, and Do No Harm missions) are still expected to conduct assessments against the GOLD Rules, but may consider a less formal review of those assessments with ETD technical leadership than an Engineering Peer Review.

Projects may choose not to apply GOLD Rules to internal constituents of Commercial-Off-The-Shelf (COTS) items and Projects should not apply GOLD Rules to standard components with established reliability. (See definition in "Glossary and Acronym Guide" at the end of this document.) In this case, any residual risk should be assessed and tracked by the project. (Note: by definition, if GSFC chooses to change COTS developer processes for an item, the item is no longer COTS.)

For other commercial procurements, the project ETA is expected to perform an assessment of the vendor's design against the GOLD rules, as noted above. Projects are not required nor expected to incorporate the rules directly into their system requirements. Instead, they should work with their vendors to determine where the vendor's standard practice meets the intent embedded in each rule.

A technical authority designated for each rule will be responsible for design assessment, related guidance and lessons learned, and participation in the evaluation of proposed changes and review of project assessment. Note: in development of the project assessment, staff will find that some rules have multiple owners listed. The project staff should work directly with the "primary owner", who will get feedback from the other owners and subject matter experts**.**

1.05	Redundant Systems and Single Point Failures	Systems Engineering
Rule:	On projects that implement redundancy (e.g. class A/B) or on subsystems that implement selective redundancy (e.g. specific subsystems on class C/D), single point failures that affect mission functionality should be identified, along with mitigations required to mitigate the risk of failure. Where redundancy is implemented, the design should be analyzed to identify any weakness in the design which removes the independence between primary and redundant functions.	
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 ensure that they are communicated to senior management. For redundancy to have the desired effect on system reliability, care should be taken to maintain independence between primary and redundant functions.	
Note:	Requirement has been updated to acknowledge that many missions do not have the resources or expectation to implement redundancy. Examples of design weaknesses that remove independence between primary/redundant functions include failure cases which prohibit the swap to the redundant side, harness faults where prime/redundant lines can short against each other or both be affected by poor connector stress relief. There are many more examples	
Revision Status: Rev I	**Owner:** Mission Engineering and Systems Analysis Division (590)	**Reference:**

1.06	Resource Margins	Systems Engineering
Rule:	Project should track technical resources and maintain growth margins commensurate with expected growth patterns. Mission-level resource margins shall be met in accordance with Table 1.06-1. Individual elements (instruments, subsystems, components) should manage their resources such that the maximum expected value (based on current estimate and maturity) will not exceed their allocation. When the maximum expected value, including maturing growth exceeds allocations, individual elements are expected to inform the project and begin work to address the issue	
Rationale:	Structured allocation and tracking of technical resource margins is needed to allow sub-elements to continue with their designs in an organized manner. Proactive mitigation of allocation exceedances is needed to enforce interface expectations across subsystems and to prevent resource exceedances from spreading to multiple elements Mission level is allocated additional margin beyond expected growth rates to cover "unknown unknowns" which come up during project. This pool is set at mission level to keep resource pool small, in lieu of offering every subsystem additional margin	
Note:	See notes that accompany attached Table	
Revision Status: Rev I	**Owner:** Mission Engineering and Systems Analysis Division (590)	**Reference:** AIAA S-120A-2015, Mass Properties Control For Space Systems

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

Resource	Pre-Phase A	Phase A	Phase B	Phase C	Phase D	Phase E
Mass *	≥15% at all times before SRR	≥15% at SRR	≥10% at PDR	≥5% at CDR and >2% at SIR	0	
Power (wrt EOL capacity)**	≥25%	≥20%	≥15%	≥10%	≥5%	
Propellant***	3σ***				3σ	
RF Link NSN DTE****/SN SR	>3dB/>0dB	>3dB/>0dB	>3dB/>0dB	>1dB/>0dB	>1dB/>0dB	

* Mass Margin

- Basic mass is the current estimated mass of dry hardware based on an assessment of the most recent design (not including mass growth allowance); in the past also referred to as current best estimate
- Mass Growth Allowance (MGA) is the predicted increase to the basic mass of an item based on an assessment of the hardware category/design maturity/fabrication status in alignment with AIAA S-120A-2015. MGA is applied bottoms-up at the MEL line level by the responsible design engineer (PDL). MGA is not to be assigned top-down.
- Predicted mass = Basic + MGA; in the past also referred to as maximum expected value.
- Allowable mass is the limit against which mass margins are calculated, typically the mass allocation or launch vehicle capacity; in the past, also referred to as Maximum Permissible Value.
- Mass margin = Allowable – Predicted.
- Mass margin (%) = (Allowable-Predicted)/Basic X 100. Note Basic mass is in the denominator in alignment with the AIAA S-120A-2015 definition.
- The terms "reserve" and "contingency" are not to be used in relation to mass margins.
- Margin and MGA apply to dry mass only. Fuel margins are handled through Delta-V margins applied against the predicted mass.
- Requirement is applicable at the mission level. Mission elements/payloads should establish mission-appropriate mass margin guidelines against their allocations.
- Mass margins apply at milestones, not strictly by phase, with ramps between milestones (in alignment with AIAA S-120A-2015).

** Power (against end-of-life) margin (in percent = (available-estimated)/available x 100). At launch there shall be 5% predicted power margin for mission critical, cruise and safing operating modes as well as to accommodate in-flight operational uncertainties.

*** The 3-sigma variation is due to the following: 1. Worst-case spacecraft mass properties 2. 3-sigma low launch vehicle performance 3. 3-sigma low propulsion subsystem performance (thruster performance/alignment, propellant residuals) 4. 3-sigma flight dynamics errors and constraints 5. Thruster failure (applies only to single-fault-tolerant systems)

**** Flight RF Comm Systems using NSN DTE ground stations should be designed for a minimum 3dB link margin for nominal modes of operation. That margin may be reduced for Phase C/D if final hardware performance (flight or ground) is less than expected. Mission users of non-NSN ground stations (commercial, partners, etc.) should use the NSN DTE link guidelines listed here; assumes EOL properties.

1.07	End-to-End Phasing/Polarity Checks	Systems Engineering
Rule:	All hardware and software used in closed-loop control systems where proper polarity is critical should be verified by test or inspection. All closed-loop algorithms should be tested on and end-to-end basis to confirm expected output for a given input. This is especially true for control systems that must work autonomously to maintain Observatory safety. Systems are recommended to allow for polarity change via a restricted command or a software parameter update, in the event that a polarity change is required to correct control performance	
Rationale:	Inadequate verification of signal phasing or polarity can result in unexpected on-orbit performance and possible loss of mission. Component-level and end-to-end phasing tests and flight software mitigations can ensure correct operation.	
Note:	Given the confusion that can accompany tracking proper polarity across different reference frames, it is also strongly recommended that polarity verification be witnessed/supported by an independent observer, to minimize the possibility of human error	
Revision Status: Rev. I	**Owner:** Mission Engineering and Systems Analysis Division (590)	**Reference:**

1.08	System End-to-End Testing		Systems Engineering
Rule:	System end-to-end testing should be performed in the final flight configuration, hardware and software. End-to-end testing should be from instrument(s) sensor input, through the spacecraft, to a command and telemetry ground system.		
Rationale:	End-to-end testing is the best verification of the system's functionality		
Revision Status: Rev I		**Owner:** Systems Engineering Branch (593)	**Reference:** GEVS 2.9

<table>
<tr><th>1.09</th><th colspan="2">Test as You Fly</th><th>Systems Engineering</th></tr>
<tr><td>Rule:</td><td colspan="3">A "test as you fly" verification philosophy should be employed through all levels of a mission's verification program. Care should be taken to verify mission functionality and performance in as flight-like a configuration as possible. This includes placing the hardware in the appropriate flight-like configuration consistent with the test environment.</td></tr>
<tr><td>Rationale:</td><td colspan="3">Testing the flight system with the hardware, software, operations and environment in the most flight situation is needed to find issues that will occur in that configuration on-orbit. Non-flight configuration testing can mask issues with the design.

Testing in a flight-like configuration ensures that the hardware will be adequately screened for design and workmanship flaws and allows for functional testing to verify adequate performance during and after environmental exposure.</td></tr>
<tr><td>Note:</td><td colspan="3">It is acknowledged that there will be some non-compliances with this design guideline, as it is impossible to fully simulate the environment of space while testing on Earth. Our expectation is that projects will work to identify those non-compliances, understand the risk associated with non-TAYF verification, and work to mitigate the risk in as responsible a manner as possible.

Since there are usually several non-compliances to this guideline, we have developed a process to hold an EPR with representatives of each Division as a way to talk through every non-compliance and risk mitigation in one sitting. This is meant to simplify the previous challenge of handling every non-compliance on a prolonged one-on-one basis.

Since non-compliances are sometimes identified in the middle of the verification program, it is noted that projects are expected to begin discussions with ETD on their approach to non-compliances in a timely manner, rather than waiting until the issue is OBE.</td></tr>
<tr><td colspan="2">Revision Status:
Rev. I</td><td>Owner:
Mission Engineering and System Analysis Division (590, Primary), Mechanical Systems Division (540), Instrument Systems and Technology Division (550), Electrical Systems Division (560), and Software Engineering Division (580)</td><td>Reference:</td></tr>
</table>

1.11	Qualification of Heritage Flight Hardware		Systems Engineering
Rule:	All heritage flight hardware should be fully qualified and verified for use in its new application. This qualification should take into consideration necessary design modifications, changes to expected environments, and differences in operational use.		
Rationale:	The guideline is written to acknowledge that the definition of flight heritage not only includes having flown on a mission, but also the specific environment (thermal, structural, radiation) and how the item was used. In other words, if a component that has flight heritage is used in a completely different environment, or used in a completely different way, the verification program needs to qualify the component for its new use, instead of simply relying on previous heritage.		
Revision Status: Rev.I	**Owner:** Systems Engineering Branch (593)		**Reference:**

1.14	Mission Critical Telemetry and Command Capability		Systems Engineering
Rule:	When possible, mission operations should be designed to provide real-time or near real-time command and telemetry capability during critical operations. In cases where near real-time telemetry is not possible, the system should be designed to store the critical telemetry at a sufficient rate to fully understand how the event proceeded and if there were any issues that must be addressed.		
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.		
Note:	Examples of critical events include, but are not limited to: separation from the launch vehicle; power-up of major components or subsystems; deployment of mechanisms and/or mission-critical appendages; initial thruster firings and all planned propulsive maneuvers required to establish mission orbit and/or achieve safe attitude "Where possible" is worded to allow for the fact that near-realtime communications are not possible for planetary missions with significant light time delay, nor for missions that are not in view of their communication relays during the critical events. It is not meant to be a clause that allows for operations to miss mission critical events when there were no significant barriers preventing that communication		
Revision Status: Rev. I	**Owner:** Systems Engineering Branch (593)		**Reference:**

1.17	Safe Hold Mode		Systems Engineering
Rule:	All spacecraft should have a power-positive, thermally safe, control mode (Safe Hold) to be entered in spacecraft emergencies. Safe Hold Mode should have the following characteristics: (1) its safety should not be compromised by the same credible fault that led to Safe Hold activation and (2) it should employ the minimum hardware set required to maintain a safe attitude.		
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.		
Revision Status: Rev. H, Updated Rev I		**Owner:** Autonomous Control and Systems Modeling Branch (591)	**Reference:**

<table>
<tr><td>1.19</td><td colspan="2">Initial Thruster Firing Limitations</td><td>Systems Engineering</td></tr>
<tr><td>Rule:</td><td colspan="3">Where operationally possible, the use of thrusters as spacecraft actuators should be protected (by FDC) against momentum thresholds which would allow for spacecraft recovery by other means.

Particular care should be given to initial use of thrusters, where polarity or performance issues would initially be found that might pose undue risk. For these cases, use of a timeout or other limitation is recommended, if possible.</td></tr>
<tr><td>Rationale:</td><td colspan="3">Issues with thruster failures or polarity discrepancies have resulted in spacecrafts being spun up multiple times. Generally, the flat spin rates that are achieved in these anomalies, if left unchecked, are well beyond the capability of the spacecraft to recover. This rule is written to recommend designers take spinup into account and specifically protect against different ways it can occur.

Time limitation at initial use is a way to checkout the thruster system before having to fully commit to its use. It is not always feasible, but recommended where possible.</td></tr>
<tr><td colspan="2">Revision Status:
Rev. I</td><td>Owner:
Autonomous Control and Systems Modeling Branch (591)</td><td>Reference:</td></tr>
</table>

1.20	Wetted Joints of Hazardous Propellants		Systems Engineering
Rule:	All joints in the propellant lines should be NDE-verified welds.		
Rationale:	Failure of wetted joint poses a catastrophic threat to personnel and/or facility, along with a threat to mission success. Additionally, a fully welded system mitigates the risk of late-discovered safety concerns from the launch range during the safety review process.		
Revision Status: Rev.I	**Owner:** Autonomous Control and Systems Modeling Branch (591)		**Reference:**

1.21	Over Pressurization Protection in Liquid Propulsion Systems		Systems Engineering
Rule:	The propulsion system design and operations should preclude damage due to pressure surges ("water hammer").		
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.		
Revision Status: Rev. E, Updated Rev I		**Owner:** Autonomous Control and Systems Modeling Branch (591)	**Reference:**

1.22	Purging of Residual Test Fluids		Systems Engineering
Rule:	Propulsion system design and the assembly & test plans should 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.		
Revision Status: Rev. E, Updated Rev I		**Owner:** Autonomous Control and Systems Modeling Branch (591)	**Reference:**

1.24	Propulsion System Safety Electrical Disconnect		Systems Engineering
Rule:	An electrical disconnect "plug" and/or set of restrictive commands should 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.		
Revision Status: Rev. E, Updated Rev. I		**Owner:** Autonomous Control and Systems Modeling Branch (591)	**Reference:**

1.27	Propulsion System Over-temp Fuse		Systems Engineering
Rule:	Flight over-current devices for wetted propulsion system components should be sized so that they provide overcurrent protection at a current that does not result in unsafe overheating of propellant.		
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. Any wetted component (i.e., in addition to fuses) that could be continuously powered should also be considered. Exceeding the auto-ignition temperature of propellant can result in mission failure or critical/catastrophic hazard to personnel and facility.		
Revision Status: Rev. I		**Owner:** Autonomous Control and Systems Modeling Branch (591)	**Reference:** EEE-INST-002

<table>
<tr><td>1.28</td><td colspan="2">Unintended Propellant Vapor Ignition</td><td>Systems Engineering</td></tr>
<tr><td>Rule:</td><td colspan="3">Propulsion system design and operations should preclude ignition of propellants in the feed system.</td></tr>
<tr><td>Rationale:</td><td colspan="3">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.</td></tr>
<tr><td colspan="2">Revision Status:
Rev. E, Updated Rev I</td><td>Owner:
Autonomous Control and Systems Modeling Branch (591)</td><td>Reference:</td></tr>
</table>

1.30	Controller Stability Margins	Systems Engineering
Rule:	Flight closed-loop controllers should have stability margins of at least 6 dB for rigid body stability and 30 degrees of phase margin. When flexible body effects are taken into account, the controller should be designed to suppress the maximum amplitude to -12 dB to avoid potential control structure interaction instabilities.	
Rationale:	Proper gain and phase margins provide margin against uncontrolled behavior if the controller is affected by unmodeled amplitude or timing changes. The additional requirement to provide flexible body suppression is based on our limited ability to model flexible body dynamics and damping..	
Note:	This design guideline does not preclude controllers that are non-compliant with the listed gain/phase margins (eg phase stabilized controllers), it only triggers the project to give more careful consideration of the need for such a controller and the efforts that have been made to understand and model timing/phase shifts which may have an impact on stability. Unless otherwise specified, stability analyses should use a sufficiently conservative modal damping value to ensure flexible interactions are properly accounted for. Refer to code 591 design documentation for recommended values and uncertainty factors.	
Revision Status: Rev. I	**Owner:** Autonomous Control and Systems Modeling Branch (591)	**Reference:** ACS Handbook

1.31	Actuator Sizing Margins		Systems Engineering
Rule:	Attitude Control System actuator sizing should take into account expected growth rates in the mass properties when components are selected and procured.		
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.		
Note:	Previous revisions recommended 100% design margin at phase A, 50% margin at phase B, and 25% margin at phase C. These recommendations are left in this note, but we acknowledge that alternate methods for estimating mass property growth may recommend different sizing margin.		
Revision Status: Rev. I		**Owner:** Autonomous Control and Systems Modeling Branch (591)	**Reference:** ACS handbook

1.32	Thruster and Venting Impingement		Systems Engineering
Rule:	Thruster or external venting plume impingement should be analyzed and demonstrated to meet contamination, thermal, and disturbance mission requirements.		
Rationale:	Impingement is likely to contaminate critical surfaces and degrade material properties and can also create adverse and unpredictable S/C torques and unacceptable localized heating.		
Revision Status: Rev. I		**Owner:** Mission Engineering and Systems Analysis Division (590)	**Reference:**

1.37	Clear Views in Launch Configuration	Systems Engineering
Rule:	When a spacecraft is in its stowed (launch) configuration, it should not obscure visibility of any attitude sensors required for acquisition, nor should it block any antenna 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.	
Note:	Some designs place Coarse Sun Sensors in locations that are covered until solar array deployment is completed. In these cases, team should review design to determine how the ACS mode performs if the Solar Array does not immediately deploy. If performance is acceptable, then design can be considered compliant. But if the associated blockage prevents acceptable performance, a different configuration should be considered.	
Revision Status: Rev. E, Updated Rev I	**Owner:** Systems Engineering Branch (593)	**Reference:**

1.39	Propellant Sampling in Liquid Propulsion Systems		Systems Engineering
Rule:	Liquid propellant quality should be verified by sampling at point of use prior to loading spacecraft propulsion system.		
Rationale:	Contaminated propellant could result in damage to components or manifolds, leading to failure of the propulsion system with a potential impact on mission success. If detected after loading propellant into the flight system, purging and cleansing the propulsion system of contaminants would incur significant cost and result in launch delay.		
Note:	If point of use sampling is precluded for some reason, project should sample at source and take steps to mitigate risk of contamination through the loading GSE.		
Revision Status: Rev. F, Updated Rev I	**Owner:** Autonomous Control and Systems Modeling Branch (591)		**Reference:**

1.40	Maintaining Command Authority of a Passive Spacecraft	Systems Engineering
Rule:	All spacecraft should be designed to prevent loss of command authority and command integrity.	
Rationale:	Mission control needs to be maintained.	
Note:	Examples of things to avoid include the ability to turn off the command receiver or place it in a configuration where it cannot receive commands. Another example would be the ability to fully power down the spacecraft. If there are areas where the spacecraft can get into a temporary configuration where command receipt is not possible, it should be able to reconfigure itself autonomously into a configuration where command and control can be restored.	

Revision Status:	**Owner:**	**Reference:**
Rev. I	Systems Engineering Branch (593)	

1.41	GSE Use At Launch Site		Systems Engineering
Rule:	Proper operation of the spacecraft in the launch configuration with either flight umbilical cable or a proxy with similar electrical and circuit characteristics. All flight GSE should be certified for its use prior to integration to the Observatory. Teams should avoid the use of new GSE at the launch site that has not been used with the spacecraft previously.		
Rationale:	Integration to the launch vehicle is too late in the development cycle to discover the spacecraft has an issue with the umbilical interface. That interface should be tested with the flight article or representative proxy before shipment to the launch site. Use of new GSE at the launch site could result in unexpected test results or potential harm to the spacecraft.		
Revision Status: Rev. I		**Owner:** Advanced Manufacturing Integration and Test (547, Primary), Systems Engineering Branch (593)	**Reference:**

1.43	Flight Software Update Demonstration		Systems Engineering
Rule:	There should be a pre-flight, end-to-end demonstration of code change, using the MOC and flight observatory, for any software or FPGA firmware which realistically might be changed in flight.		
Rationale:	Demonstration of this capability for software not hosted in the spacecraft primary computer is often overlooked prior to launch. Performing an end-to-end demonstration of the upload capability (as opposed to uploading via a test connector) verifies that function and confirms the system can be updated in flight.		
Note:	Wording has been changed from previous versions from recommending uploads on every instance of software/firmware to recommending uploads on those areas where an upload is a realistic possibility. During their assessments, projects should be prepared to explain why certain uploads that would be skipped are unrealistic.		
Revision Status: Rev. I		**Owner:** Mission Engineering and System Analysis Division (590)	**Reference:**

1.44	Early Interface Testing		Systems Engineering
Rule:	Spacecraft-to-payload electrical interfaces, including protocol and software compatibility, should be tested with breadboard or engineering unit hardware, as soon as the hardware is available, preferably before the instrument (or component) CDR.		
Rationale:	On multiple missions, it has been demonstrated that the time and effort to execute early interface tests reduces the overall mission cost and schedule by finding and correcting incompatibilities before they impact system-level I&T. While having well-written ICDs and/or the use of industry-standard interfaces, can minimize interface incompatibilities, there are often nuances that can only be uncovered via test.		
Revision Status: Rev. G, Updated Rev I		**Owner:** Mission Engineering and System Analysis Division (590, Primary) and Electrical Engineering Division (560)	**Reference:**

1.45	System Alignments		Systems Engineering
Rule:	System alignment verifications should be performed before and after exposure to system environmental testing to demonstrate alignment stability.		
Rationale:	Demonstrates stability of alignments through the environments which gives confidence that alignments will not shift due to launch vibro-acoustic environment or post-launch thermal environment.		
Revision Status: Rev. G, Updated Rev	**Owner:** Mission Engineering and System Analysis Division (590)		**Reference:**

1.46	Use of Micro-Switches		Systems Engineering
Rule:	Micro-switches should be used for information only and should not be used as the single means to initiate on-board autonomous activity or as an on-board interlock.		
Rationale:	Micro-switches have known reliability issues and have not provided deterministic results on past missions.		
Revision Status: Rev. I		**Owner:** Mission Engineering and System Analysis Division (590)	**Reference:**

1.47	Design Deployables For Test		Systems Engineering
Rule:	Whenever practical, appendages and other deployables should be capable of deployment under 1G conditions without the use of g-negation ground support equipment. When it is not practical to design for unassisted 1G deployment, the design should have provisions for interfacing to gravity off-load GSE.		
Rationale:	Numerous occasions where instrument doors, etc. are not designed for 1G deployment and don't have provisions built in for g-negation.		
Revision Status: Rev. G, Updated Rev I		**Owner:** Mission Engineering and System Analysis Division (590)	**Reference:**

1.48	Space Data Systems Standards	Systems Engineering
Rule	Data systems standards (e.g., CCSDS, OMG, commercial, international) should be utilized by missions and implemented in all space communication systems.	
Rationale:	Standardization of space data system interfaces, formats, and protocols within the Agency reduces the cost of specification and implementation of data systems. It increases reliability through the use of proven interfaces and heritage software and tested vendor products. Space data systems standards enable easier and lower-cost data interoperability between systems within a local system, across a Center or Agency, and with external partners.	
Revision Status: Rev H, Updated Rev I	**Owner:** Electrical Engineering Division (Code 560)	**Reference:** www.ccsds.org www.ccsds.org/publications www.omg.org/space/

Notes: 1) The Center CCSDS Standards Point of Contact (POC) is a recommended resource for learning the current breadth of standards to be considered and the status of CCSDS and OMG standards currently under development. 2) The Consultative Committee for Space Data Standards (CCSDS) publications span a wide range of technical areas which may be of benefit to missions, including both optical and RF communications, uplink and downlink messaging, file transfer protocols, delay-tolerant networking, navigation messages, service-oriented approaches to increase interoperability, data compression and security, and more. The Object Management Group (OMG) is an international, not-for-profit technology standards consortium. The OMG Space Domain Task Force (Space DTF) maintains standards specific to space applications, including common telemetry and command definition formats, scripting standards, and ground equipment interface definitions. Commercial or general use standards, including internet protocol or mobile device standards may also provide significant benefit to some missions and shall not be precluded.

2.01	Flight Electronic Hardware Operating Time		Electrical
Rule:	One thousand (1000) hours of operating/power-on time should be accumulated on all flight electronic hardware (including all redundant hardware) prior to launch. The last 350 hours of operating/power-on time should be failure-free, of which at least 200 hours should be in vacuum. For Class D and below, only the failure-free and vacuum requirements should apply. For hardware expected to operate for less than 100 hours in-flight, proposed pre-launch operating hours should be discussed with the rule owner.		
Rationale:	Accumulated power-on time serves functions; First, it weeds out any parts which may suffer from "infant mortality. Secondly, sufficient powered test time assures any "edge cases" have been tested. Modern avionics systems often employ parts and designs which contain thousands or millions of gates and can produce trillions of permutations. Testing all of these permutations in simulation is impractical, so the only way to ensure that they are all tested is to provide sufficient real operating time for the devices (and to provide it across the operating temperature range, hence the requirement for the 200 hours in thermal vacuum). It is advisable to review the number of hours at SIR, PER, PSR, ORR, for sufficiency of completion of recommended hours.		
Revision Status: Rev. H	**Owner:** Electrical Engineering Division (560)		**Reference:** GEVS 2.3.4

<table>
<tr><td>2.05</td><td colspan="2">System Grounding Architecture</td><td>Electrical</td></tr>
<tr><td>Rule:</td><td colspan="3">For all missions, a system grounding design should be developed and documented for flight and GSE test configurations. Except for coaxial interfaces, structure or shields should not be used for the primary circuit current return path. A dedicated conductor should be included to provide the current return path with the smallest loop area possible.</td></tr>
<tr><td>Rationale:</td><td colspan="3">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. Failure to consider GSE grounding could result in damage to flight hardware. It is advisable to have a preliminary design by PDR & final design by CDR.</td></tr>
<tr><td colspan="2">Revision Status:
Rev. F, Updated Rev. G</td><td>Owner:
Avionics and Electrical Systems Branch (565)</td><td>Reference:</td></tr>
</table>

2.06	System Fusing Architecture	Electrical
Rule:	A system fusing architecture should be developed and documented for all missions, including the payloads. All circuit breakers that can't be reset by command (i.e., fuses) should be easily accessible for replacement and/or for integrity verification at any time prior to launch vehicle integration.	
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. It is advisable to have a preliminary design by PDR & final design by CDR.	
Revision Status: Rev. H	**Owner:** Avionics and Electrical Systems Branch (565)	**Reference:** EEE-INST-002

2.13	Electrical Connector Mating		Electrical
Rule:	All flight connectors where mating cannot be verified via ground tests, should be clearly labeled and keyed uniquely, and mating of these connectors should be verified visually to prevent incorrect mating. The design should not use connectors that require a blind mating in system-level integration, test and launch operations.		
Rationale:	Error in mating of interchangeable connectors can result in mission degradation or failure.		
Revision Status: Rev. F, Updated Rev. G		**Owner:** Avionics and Electrical Systems Branch (565)	**Reference:** Electrical Systems Design Guidelines

2.14	Protection of Avionics Enclosures External Connectors Against ESD		Electrical
Rule:	All avionics enclosures should be protected from ESD. All external connectors should be fitted with shorting plugs or appropriate caps during transportation between locations. Additionally, all test points and plugs should be capped or protected from discharge for flight.		
Rationale:	Capping open connectors provides protection from electrostatic discharge resulting from space charging.		
Revision Status: Rev. F	**Owner:** Avionics and Electrical Systems Branch (565)	**Reference:** Electrical Systems Design Guidelines	

2.22	Corona Region Testing of High Voltage Equipment	Electrical
Rule:	Assemblies containing a High Voltage (>150V) supply that is not tested through the Corona region should 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.	
Revision Status: Rev. H	**Owner:** Power Systems Branch (563, Primary), Instrument Systems and Technology Division (550)	**Reference:**

<table>
<tr><td>2.23</td><td colspan="2">RF Component Testing for Multipaction and Corona</td><td>Electrical</td></tr>
<tr><td>Rule:</td><td colspan="3">Multipactor and corona margins for component of spacecraft RF communications subsystems should be maintained at the mission frequencies. All components should be vented.
If the RF transmitter is on during launch and ascent, all flight components in the transmit path should be verified as corona free at all pressures from sea level to 1E-4 Torr.
Resonant passive flight components should be verified as multipactor free by test on all units.
Non-resonant passive flight components should be verified as multipactor free by test or analysis.
The test setup should be verified with a known breakdown device.
Multipactor analysis should show a 10dB margin.
Multipactor test level for the passive components should be at least 6dB above the nominal power level in vacuum (<1E-5 Torr) during unit acceptance testing.</td></tr>
<tr><td>Rationale:</td><td colspan="3">Unless significant design margin is demonstrated, small unit-to-unit variations make it impossible to predict whether an RF component is susceptible to Multipaction or Corona. Testing/Analysis will ensure immunity to multipactor/corona at the component level.</td></tr>
<tr><td colspan="2">Revision Status:
Rev. H</td><td>Owner:
Communication Systems Branch (566)</td><td>Reference:</td></tr>
</table>

2.24	Solar Arrays	Electrical
Rule:	a. Solar arrays should incorporate solar cells that have been qualified per AIAA-S-111A-2014, “Qualification and Quality Requirements for Space Solar Cells.” If a later revision of AIAA-S-111 has been released by the time of contract award for the mission, the later revision should govern. b. Solar panels should be qualified to the mission environment via qualification panels per AIAA-S-112A-2013 (or equivalent), “Qualification and Quality Requirements for Electrical Components on Space Solar Panels.” If a later revision of AIAA-S-112 has been released by the time of contract award for the mission, the later revision should govern. c. Qualification and flight solar panels should be tested at ambient temperature and at their highest predicted operating temperature including calibrated I-V curves (where practical) before and after panel-level environmental testing. d. Flight solar arrays should be tested at wing level or array level at ambient temperature including calibrated I-V curves after all environmental testing (integrated to the spacecraft or not) is complete. Should the flight solar array be stored for a period of more than two years after the post-environmental array testing is complete, the calibrated I-V curve measurements at ambient temperature should be repeated prior to launch.	
Rationale:	Space solar arrays must survive severe environments including particulate radiation, UV, and up to tens of thousands of very rapid temperature excursions between cold and hot. Incremental changes to parts and processes can have unexpectedly large consequences. Therefore, it is essential that the solar array for each mission be rigorously qualified and tested for that mission.	
Revision Status: Rev. F, Updated Rev. H	**Owner:** Mechanical Systems Division (540) and Power Systems Branch (563, Primary)	**Reference:**

2.25	Electrical Interface Verification	Electrical
Rule:	Electrical Interface (i.e., copper-path) Verification Test (IVT) should be performed on all flight connectors following final flight mating. This may be performed via powered testing and/or physical (e.g., resistance) measurements.	
Rationale:	Final verification of flight interfaces is required to ensure proper electrical integrity and function, thereby minimizing the probability of system failure and maximizing probability of mission success.	

Revision Status:	**Owner:**	**Reference:**
Rev. F, Updated Rev. G	Electrical Engineering Division (560, Primary) and Mission Engineering and Systems Analysis Division (590)	

2.26	Power-On Reset Visibility		Electrical
Rule:	A power-on reset occurrence should be unambiguously identifiable via telemetry. Note: This does not imply real-time telemetry as the reset is occurring.		
Rationale:	An unexpected power-on reset could be an indication of a serious issue and should be able to be distinguished from resets that are indicative of less serious conditions.		
Revision Status: Rev. G		**Owner:** Electrical Engineering Division (560, Primary) and Flight and Ground Software Systems Branch (582)	**Reference:**

2.27	Spacecraft -Trending Capability		Electrical
Rule:	A minimal set of hard-line spacecraft parameters, sufficient to establish spacecraft health and safety, should be monitored and captured (stored) independent of the spacecraft telemetry system, by the EGSE whenever the spacecraft is powered. This data should be sampled at a rate sufficiently high to aid in diagnosis of abnormal power events.		
Rationale:	This capability is valuable to capture data for anomalous behavior on the spacecraft during I&T when spacecraft telemetry is not available.		
Revision Status: Rev. G		**Owner:** Advanced Manufacturing Integration and Test (547, Primary) and Systems Engineering Branch (593)	**Reference:**

3.02	Elimination of Unreachable Software	Software
Rule:	It is best practice to analyze the developed Flight Code for any instance(s) of un-called functions, or otherwise unreachable code (see Table 3.02-1). It is usually best to remove code that is not called or used.	
Rationale:	There are significant benefits to re-using software from past missions, not the least of which is cost. However, missions have different requirements and re-using heritage software often carries forward software not required by the current mission. For example, the very successful cFE/CFS framework used on many missions, will have functions within applications, which are not used in the current mission. Unreachable software can also occur within a mission's lifecycle as system and software requirements change during the software development process. 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 unreachable code.	
Note:	A well-understood exception to this practice would be the cFE/CFS code base where some code is necessarily unreachable due to its design for multi-mission reuse.	
Revision Status: Rev. E, Updated Rev. H	**Owner:** Flight and Ground Software Systems Branch (582, Primary), Software Systems Engineering and Operations (581)	**Reference:**

T

Table 3.02-1 Unreachable Software Definitions

Term	Definition
Unreachable Software	Code which cannot be properly exercised via demonstration during FSW or system level test.
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. Source code is the description of a computer program that is translated into machine code by another program such as an assembler, compiler or interpreter. If the translator creates object code modules, then the modules are combined using a linker program. The end result of the process is a program or library of functions that is executable or a processing unit. Source code includes higher level languages, including visual languages, which are first translated into lower-level languages (e.g., C or Assembler) before translation to executable code.

Table 3.02-2 Example Areas To Consider For Analysis

Examples	Definition
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:	It is best practice to provide a high-fidelity software simulation capability for each external interface to FSW and have it reside in the FSW development/maintenance environments. These simulators should allow nominal and off-nominal data inputs to FSW using a means that allows configurability in real-time, preferably using the procedural language (if that exists) of the FSW test workstation or computer.	
Rationale:	In order to adequately develop embedded FSW, a suitable test environment should exist. This environment should include the necessary GSE, ETUs, and other H/W needed to properly simulate and stimulate the Flight Code. Having this simulation capability allows the Flight Software team to develop and test the Flight Code in order to find and debug code early in the process. Not providing this simulator capability will mean that the Flight Code can only be tested in a nominally over-subscribed FLATSAT environment, or in the Flight environment. Not testing early in the process, (which is a consequence of not having a suitable, flight-like environment) will only drive up cost, since the later in the program bugs are discovered, the higher the cost to fix said bugs.	
Revision Status: Rev. H	**Owner:** Flight and Ground Software Systems Branch (582)	**Reference:**

3.04	Independent Software Testing	Software
Rule:	It is best practice to have an independent team perform Software verification and validation. **NOTE**: It's also allowable for members of the same development team to perform independent testing with the caveat that a developer is not testing his/her own developed code.	
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. This approach can lead to "blind spot" issues. Having authored the code, he/she may assume a single use case, and possibly only test to that use-case, where, the mission operations may have other use cases in mind, which may not be tested, and may present errors, which are only found later in the test program. 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.	
Revision Status: Rev. H	**Owner:** Software Engineering Division (580)	**Reference:**

3.05	Ground System/Operations Testing and Operations Team Readiness	Software
Rule:	It is best practice that access to flight system interface and functional capabilities, provided either by the spacecraft or by spacecraft simulators, be negotiated with all stakeholders, including the ground system and operations teams. Schedules and agreements should address the spacecraft/spacecraft simulators/instrument(s)/instrument simulator(s) 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.	
Revision Status: Rev. H	**Owner:** Software Systems Engineering Branch (581, Primary), Software Systems Engineering and Operations (581)	**Reference:**

3.06	Dedicated Hardware Computing Platform Testbed for Flight Software and Reconfigurable FPGA Lifecycle Development		Software/Reconfigurable FPGA
Rule:	It is best practice that a "high fidelity" data processing system testbed(s), (representative of the flight hardware), be dedicated to FSW/FPGA product development teams and used specifically for development, integration and test of the Flight Software. The quantity of data system testbed units should be sufficient to support the FSW/FPGA development schedule and the overall mission schedule. This is a proven cost driver.		
Rationale:	Early investment in dedicated flight computing system testbeds with high fidelity hardware saves costs and avoids significant schedule risks associated with FSW/FPGA development and downstream flight integration and test. Anything less than a dedicated hardware unit that is representative of the flight processing system (e.g., ETU, EDU, flight spare) will add to mission risk and threaten cost/schedule.		
Revision Status: Rev. H		**Owner:** Flight and Ground Software Systems Branch (582, Primary); Electrical Engineering Division (560)	**Reference:** **500-PG-8700.2.8B**

Notes:

1) In Rev H, this rule has been expanded to cover systems that also include reconfigurable FPGAs that will change throughout the lifecycle.
2) Projects that have a complex computing platform (multiple reconfigurable FPGAs, many-core or distributed processors, dynamic reconfiguration processing, Machine Learning applications, etc) may require multiple testbeds and/or testbeds with higher fidelity components that interface with the data processing system.
3) The testbed fidelity must include flight-like processors, supporting chips (memory, power delivery, etc.), FPGAs, and interfaces. An EDU or ETU typically meet the fidelity intent.
4) Agreement on testbed quantity must be made between FSW/FPGA leads, Systems, and Project Management.

3.07	Flight Software Margins		Software
Rule:	It is best practice that Flight software resource margins be maintained in accordance with Table 3.07-1 and presented at Key Decision Point (KDP) milestone reviews.		
Rationale:	The need to have appropriate margin at all phases cannot be overstated. Most missions outlast their stated mission lifetime goal, and inevitably will require servicing. Servicing can be related to an onboard anomaly, or capabilities may be added/or changed, leading to a need for sufficient margins to accommodate this scenario. Invariably, this is accomplished through patching/updates to the onboard Flight Software. The Margin numbers are higher during the early mission phases because the requirements are less clear, and as such there is the very real probability that as the Mission progresses, and requirements clarity increases, then more capability will be required, which will reduce margin. As we get closer to launch, requirements are more widely known, capability stabilizes, and margins can be reduced.		
Revision Status: Rev. H	**Owner:** Software Systems Engineering and Operations Branch (581, Primary), Flight and Ground Software Systems Branch (582)		**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 open a dialog with the GOLD Rule owner to assess the anticipated projection of excessing the limits and any potential risks associated with future development and sustainability that could impact science and/or flight requirements.

Table 3.07-1. Flight Software Margins

	Mission Phase (with Method)			
	FSW SRR	**FSW PDR**	**FSW CDR**	**Ship/Flight**
Resource	Estimate	Analysis	Analysis/ Measured	Measured
Average CPU Usage	50%	50%	40%	30%
Deadlines	50%	30%	20%	10%
Non-Writeable NVM	50%	30%	20%	0%
Writeable NVM	50%	50%	40%	30%
RAM	50%	50%	40%	30%
Data Interfaces	40%	30%	20%	10%

Margin is calculated using the formula: (total allocated resource – used resource)/total allocated resource

Total allocated resource = the total magnitude of the resource allocated for use by flight software.

Used resource is estimated, analyzed and/or measured.

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 of heritage code 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.

<u>Average CPU Usage:</u> This is the percentage of time the CPU is doing non-background processing work. Background processing may include tasks such as memory scrubbing, memory validation (such as memory checksum), or any process that is interruptible or has very loose timing requirements. This average should be estimated/measured over an interval that exceeds the longest real-time event rate under normal worst-case operating conditions.

<u>Deadlines:</u> 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% (60%). 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.

<u>Non-Writeable NVM:</u> Non-Volatile Memory (NVM) that cannot be modified in flight. Typical technologies include PROM, EEPROM, and MRAM. While EEPROM and MRAM are both reprogrammable technologies, if the underlying processing platform locks out ability to write once in flight, it is considered non-writeable for this rule.

<u>Writeable NVM</u>: Non-Volatile Memory that can be modified in flight. Typical technologies include EEPROM, NOR Flash, NAND Flash, and MRAM. Used resources should include memory space allocated for code updates.

<u>RAM</u>: Volatile memory where the executing code and data are stored. This memory is always on the processor's local bus. Typical technologies include SRAM, SDRAM and DDR SDRAM. 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 (or writeable NVM). In this case, the software team should track margins on this combined RAM/NVM/bulk memory space.

<u>Data Interfaces</u>: Any external interface used by the processing system to exchange data. Typical examples include PCI, PCIe, 1553, UART, SpaceWire, SerDes, Ethernet. Usage calculations should include 1 retry for each transaction, where

applicable (if protocol allows), 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).

For software resources that do not appear in the table, use an analogous resource that does appear or work with the project systems engineer to define acceptable margins for that unique resource.

3.10	Flight Operations Preparations and Team Development		Software
Rule:	It is best practice that experienced operations personnel 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). Ideally, the Flight Operations Team (FOT) will supply Test Conductors to support Observatory I&T, which will serve to prepare and train the FOT. As a minimum, the FOT should participate in flight operations readiness tests as specified in Table 3.10. Note that these serve as descriptive guidelines and are not intended to be prescriptive.		
Rationale:	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.		
Revision Status: Rev. E, Updated Rev. H		**Owner:** Flight Systems Integration and Test Branch (568) Software Systems Engineering and Operations Branch (581, Primary)	**Reference:**

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/simulations	2 tests/simulations	1 test/simulation	1 test/simulation
Day-in-the-life (focused on spacecraft)	3 tests/simulations	2 tests/simulations	1 test/simulation	1 test/simulation
Launch & early-orbit phase	4 tests/simulations	3 tests/simulations	2 tests/simulations	2 tests/simulations
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:	It is best practice that test of the fully integrated FSW and ground system include demonstration of error free operations using flight-like scenarios over an **extended time period.** It is recommended that 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. Planetary missions should consider test durations longer than the above guidance commensurate with the planned Operations Concept			
Rationale:	Certain problems, such as memory leaks, slow occurring race conditions, etc. can only be detected with long duration testing. During these long runs, it is also imperative that realistic "day in the life of" type scenarios and stress conditions are run. As further rationale, it is prudent to note that frequent restarts of FSW and the ground system during ground tests may serve to mask problems which will only occur following extended execution of these systems. The number of hours specified is based on discussion with senior-level engineers, and reflect best practices accumulated over a period of 15 years.			
Revision Status: Rev. E		**Owner:** Software Systems Engineering and Operations (581) Flight and Ground Software Systems Branch (582, Primary)		**Reference:**

3.13	Maintaining Adequate Resources for Mission Critical Components	Software
Rule:	It is best practice that the updating of mission critical components during the mission operations phase (including any combination of hardware platforms, hardware devices, and software code) be done in such a way as to not compromise the capability of the system to meet mission requirements. In general, it is recommended that there are sufficient hardware platforms (which includes specific workstations) to allow one to be updated, while the other remains operational. After an appropriate time of testing, a switchover can be effectuated.	
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.	

Revision Status:	**Owner:**	**Reference:**
Rev. F, Updated Rev. G	Software Systems Engineering Branch (581, Primary) and Mission Engineering and Systems Analysis Division (590)	

3.14	Command Procedure Changes		Software
Rule:	It is best practice that command procedures and/or scripts, and mission databases (onboard and ground) be controlled using formal methods and processes. These include 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	It's important that proper configuration control, and auditing be used to maintain flight operations tools (procedures, databases, etc.). This is done (1) to ensure that only tested procedures (and their corresponding databases) are used in talking to the operational spacecraft. (2) Procedures and databases are kept in sync with changes to the Flight Software which may have happened, and finally (3) so that operationally the FOT is always knowledgeable of what is being commanded at all times.		
Revision Status: Rev. E		**Owner:** Software Systems Engineering and Operations (581, Primary) Flight and Ground Software Systems Branch (582)	**Reference:**

4.01	Contamination Control, Planning, and Execution		Mechanical
Rule:	Specific contamination control requirements and processes (such as analytical modeling, laboratory investigations, and contamination protection and avoidance plans) that support mission objectives should be identified.		
Rationale:	Contamination sensitive components are often critical elements that directly affect system performance. It is essential that critical component performance be preserved and not allowed to degrade due to contamination exposure & accumulations. Early attention to pinpointing susceptibilities to contamination degradation in the design as well as iterating allowable degradation due to contamination in the science performance requirements allows project management to identify risks and mitigations with the least impact to cost and schedule. Monitoring early on-orbit performance and documenting lessons learned benefits all future GSFC missions.		
Revision Status: Rev H	**Owner:** Materials Contamination and Coatings Branch (541)		**Reference:** GEVS 2.8.1

<table>
<tr><td>4.03</td><td colspan="2">Factors of Safety for Structural Analysis and Design, and Mechanical Test Factors & Durations</td><td>Mechanical</td></tr>
<tr><td>Rule:</td><td colspan="3">Structural analysis and design factors of safety should 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.</td></tr>
<tr><td>Rationale:</td><td colspan="3">The use of these factors provides confidence that the hardware will not experience failure or detrimental permanent deformation under test, ground handling, launch, or operational conditions. The test factors have been selected to provide appropriate margin over the predicted flight or operational environment to demonstrate hardware robustness and account for uncertainties in the environment and the limitations in simulating the environments in ground test. The analysis factors of safety have been defined such that prototype/protoflight hardware can be tested without experiencing detrimental yielding and provide adequate spacing between yield and ultimate failure modes to ensure the hardware will not experience a structural failure under test loading conditions.</td></tr>
<tr><td colspan="2">Revision Status:
Rev. E</td><td>Owner:
Mechanical Engineering Systems and Analysis Branch (542, Primary)</td><td>Reference:
GEVS 2.2.4 & 2.2.5</td></tr>
</table>

4.06	Validation of Thermal Coatings Properties	Mechanical
Rule:	All thermal coatings properties that drive thermally significant performance should be determined, measured and validated to be accurate for materials and mission flight parameters over the lifecycle of the mission. All thermal analysis shall employ these properties. The GSFC Coatings Committee (chaired by Code 546) shall review and approve the coatings properties.	
Rationale:	Thermal coatings properties directly affect Mission success through S/C or instrument thermal design. Early assessment of thermal coating ensures the mission objectives will be met. Assess proposed thermal coatings for the mission design parameters. needed environmental tests on thermal coatings. Determine appropriate BOL and EOL coatings properties to be used in the thermal analysis. Determine mission specific thermal coating requirements. Verify through peer review/GSFC Coatings Committee, test results, analysis and at PDR and CDR. Update thermal coatings properties as coatings selection matures. Measure coatings properties when appropriate as determined by the Thermal Engineer/Coatings Engineer. Develop notional plan for assessing in flight. Verify at PER as determined by the Thermal Engineer/Coatings Engineer. Assess thermal coatings performance through flight data as appropriate. Confirm performance with available flight data as appropriate. Reference to baseline coating properties can be found in NASA/TP-2005-212792	

Revision Status:	**Owner:**	**Reference:**
Rev. E, Updated Rev. H	Materials Contamination and Coatings Branch (541)	NASA/TP-2005-212792

<table>
<tr><td>4.10</td><td colspan="2">Minimum Workmanship</td><td colspan="2">Mechanical</td></tr>
<tr><td>Rule:</td><td colspan="4">All electrical, electronic, and electro-mechanical components should be subjected to minimum workmanship test levels as specified in GEVS Section 2.4.2.5.</td></tr>
<tr><td>Rationale:</td><td colspan="4">The minimum workmanship random vibration levels defined in GEVS Section 2.4.2.5 have been found to be the minimum input level necessary to adequately screen the hardware types above for workmanship flaws. The minimum workmanship level has been derived based on an evaluation of a large database of random vibration tests to screen for failures in electronics boards at the component levels of assembly. Units tested below the minimum workmanship level were found to have higher failure rates in upstream testing and operation due to failure to expose the hardware to sufficient input energy to screen for workmanship flaws. While the minimum workmanship level is primarily defined to identify flaws in solder joints on circuit boards, it has been found to provide an adequate screen for the mechanical build quality at the component level of assembly.</td></tr>
<tr><td colspan="2">Revision Status:
Rev. E</td><td colspan="2">Owner:
Mechanical Engineering Systems and Analysis Branch (542, Primary) and Electrical Engineering Division (560)</td><td>Reference:
GEVS Section 2.4.2.5</td></tr>
</table>

<table>
<tr><td>4.12</td><td colspan="2">Structural Proof Testing</td><td>Mechanical</td></tr>
<tr><td>Rule:</td><td colspan="3">Primary and secondary structures fabricated from nonmetallic composites (including metal matrix), beryllium, or containing bonded joints, bonded inserts, or critical welds should be proof tested in accordance with GSFC-Std-7000 Section 2.4.1.4.1. The following definitions should be used to interpret this GOLD Rule:
<u>Primary Structure</u> – Structure in the primary load path that carries the operational or test loads of the system to the structural boundary and whose failure would result in loss of structural integrity.
<u>Secondary Structure</u> – Structure that is not in the primary load path and whose failure would not result in loss of structural integrity but would result in an unacceptable loss of capability for the system to meet functional requirements. Secondary structure includes structure whose failure could result in damage to other hardware critical to meeting the functional requirements of the system.
<u>Tertiary Structure</u> – Structure not in the primary load path whose failure would not affect structural integrity or the ability of the system to meet functional requirements.
Note: Classification of structures should be evaluated at each level of assembly as defined in GEVS (system, subsystem, component).</td></tr>
<tr><td>Rationale:</td><td colspan="3">The rule identifies several different structure types where the mechanical strength is dependent on material processing, fabrication method, and workmanship. The strength capability of these items can only be verified by testing the flight build to the expected loads with margin. Coupon testing and testing of flight-like units is not sufficient to screen these types of structures for strength as the flight structure may fail below predicted capability due to workmanship or fabrication flaws.</td></tr>
<tr><td colspan="2">Revision Status:
Rev. E, Updated Rev. H</td><td>Owner:
Mechanical Engineering Systems and Analysis Branch (542)</td><td>Reference:
GEVS 2.4.1.4.1</td></tr>
</table>

4.14	Structural and Mechanical Test Verification		Mechanical
Rule:	Structural and Mechanical Test Verification program should 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. The overall structural and mechanical verification requirements defined in GEVS are summarized in Table 2.4-1. The verification tests shown in the table have been identified as the minimum necessary to demonstrate that the flight hardware can meet requirements after being exposed to expected loads and environments with appropriate test margin. The table also defines the required testing at each level of assembly (component, subsystem, and system). Performing the defined tests at the levels of assembly shown in the table demonstrates the hardware design is adequate, that the flight build will perform as expected after exposure and reduces overall mission risk to acceptable levels.		
Revision Status: Rev. E	**Owner:** Mechanical Engineering Systems and Analysis Branch (542)		**Reference:** GEVS Sections 2.4.1

<table>
<tr><th>4.15</th><th colspan="2">Torque/Force Margin</th><th>Mechanical</th></tr>
<tr><td>Rule:</td><td colspan="3">The Torque/Force Margin (TM) requirement defined in NASA-STD-5017, Section 4.3 should apply to all mechanical functions, those driven by motors as well as springs, phase change devices, 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 as well as the service environment. Note: use higher safety factors as appropriate for immature mechanism designs with no engineering test data to significantly substantiate resistive torque/force loads. See NASA-STD-5017 Table 1 for minimum factors to be applied by hardware development maturity.</td></tr>
<tr><td>Rationale:</td><td colspan="3">Torque/force margin is a measure of the excess capability of a mechanism to impart, maintain, or prevent motion, or to provide required acceleration. Torque/force margin is intended to ensure that a mechanism retains reserve torque/force that can be applied in the event of an unforeseen effect that increases resistive torque/force or reduces motive torque/force within the mechanism, similar to the factor of safety used in a structural margin calculation. Torque/force margin is intended to ensure that the mechanism retains reserve torque/force that can be applied in the event of unforeseen circumstances. Worst-case conditions are defined as those that result in a combination of minimum driving torque/force and maximum resisting torque/force over the range of qualification environmental limits.

Therefore the torque/force margin needs to be sufficiently large to guarantee system-performance under worst-case conditions throughout its life by fully accommodating the uncertainty in the resisting forces/torques and in the source of energy. Therefore, as with any other capability of the mechanism, the minimum torque/force margin is verified prior to placement into service.</td></tr>
<tr><td colspan="2">Revision Status:
Rev. E, Updated in Rev H</td><td>Owner:
Mechanical Engineering Systems and Analysis Branch (542), Mechatronics and Robotics Branch (544, Primary)</td><td>Reference:
NASA-STD-5017, Section 4.3</td></tr>
</table>

4.18	Deployment and Articulation Verification	Mechanical
Rule:	All flight deployables, movable appendages, and mechanisms should demonstrate full range of motion and articulation under worst-case conditions, when being driven by the flight avionics (i.e., not EGSE) prior to flight.	
Rationale:	Environmental factors such as temperature, gravity, acceleration fields, wire bundle stiffness, and others can adversely affect successful deployment. Additionally, initiation of mechanism release with EGSE could result in masking system-level design issues. Verification should include exercising electronics and mechanical stops if applicable. Analysis and/or test should include range of motion assessment in 0-G environment. Verification of these systems under worst-case conditions will improve on-orbit success.	
Revision Status: Rev. E, Updated Rev. G	**Owner:** Mechanical Engineering Systems and Analysis Branch (542, Primary) and Electrical Engineering Division (560)	**Reference:**

4.20	Fastener Locking		Mechanical
Rule:	All threaded fasteners should employ a minimum of one locking feature that does not depend on fastener preload to function. Exception: Swagelock compression fittings are not required to have a locking feature, but it is recommended. See Code 543 for best practices/approaches for adding a secondary locking feature.		
Rationale:	If not locked in the torqued, preloaded position, threaded fasteners subjected to vibration and thermal cycling loads may experience a reduction in preload and fully back out potentially jeopardizing the mission.		
Revision Status: Rev. F, Updated in Rev H	**Owner:** Mechanical Engineering Systems and Analysis Branch (542, Primary), Mechatronics and Robotics Branch (544)		**Reference:** **NASA-STD-5020**

4.21	Brush-type Motor Use Avoidance		Mechanical
Rule:	Designs should 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.		
Revision Status: Rev. E		**Owner:** Mechatronics and Robotics Branch (544)	**Reference:**

4.22	Precision Component Assembly		Mechanical
Rule:	When precise location of a component is required, the design should 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, in optical systems, for example, the use of pinning or similar non-friction reliant method will help ensure alignment is maintained through all expected stresses.		
Revision Status: Rev. E	**Owner:** Mechatronics and Robotics Branch (544)		**Reference:**

4.23	Life Test	Mechanical	
Rule:	The life test requirement defined in NASA-STD-5017, section 4.19 should apply. Once requirements and design are stabilized to a high degree of certainty, a life test should be conducted, within representative operational environments, to at least 2x expected life (4x for human rated systems) for all repetitive motion devices. Life testing should include a number of cycles at the expected operating environmental extremes, loads, ranges of motion, and speeds that is representative of the number of cycles at those conditions expected in the service life of the mechanism. Flight-like drive electronics and the flight drive electronics should be used in the life-test so as to eliminate differences that could provide a false positive life result (e.g., voltage, current, rise time, duty cycle, etc.).		
Rationale:	Degradation in repetitive motion devices from wear, fatigue, lubrication degradation, etc., can have serious negative impacts on mission success. Continuing the life test post-launch, if required, provides valuable information of potential anomalous conditions that could be used to modify mechanism flight operations to meet minimum mission requirements. Temperature and vacuum conditions can both have significant effects on component life due to effects on lubrication, friction, and material properties. Not properly including these environments in the life tests can lead to test results that are not indicative of how the hardware will perform in service. In addition, the extent of motion must be accurately represented. For example, small or dithering motions can be more severe because they can wipe away liquid lubricant and create debris dams at the ends of the range of motion that prevent the flow of oil back into the contact zone. A life test that exercised only the full range of motion for such parts could give a false positive impression of life.		
Revision Status: Rev. H	**Owner:** Electromechanical Systems Branch (544, Primary), Mechanical Engineering Systems and Analysis Branch (542)		**Reference:** GEVS 2.4.5.1 and NASA-STD-5017, Section 4.22.1

4.24	Mechanical Clearance Verification	Mechanical
Rule:	Verification of mechanical clearances and margins (e.g., potential reduced clearances after blanket expansion) should 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. Rigid structure features (i.e, dimensions, shape, etc) that is not susceptible to environment induce changes can be verified analytically with as-built data. This rule applies to both stationary and deployable hardware.	

Revision Status:	**Owner:**	**Reference:**
Rev. E	Mechatronics and Robotics Branch (544)	

4.25	Thermal Design Margins		Mechanical
Rule:	Thermal design should provide adequate margin between stacked worst-case flight predictions and component allowable flight temperature limits per GEVS 2.6 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.		
Revision Status: Rev. E, Updated Rev. G	**Owner:** Thermal Engineering Branch (545)		**Reference:** GEVS 2.6

<table>
<tr><td>4.27</td><td colspan="2">Test Temperature Margins</td><td>Mechanical</td></tr>
<tr><td>Rule:</td><td colspan="3">Components and systems should be tested beyond allowable flight temperature limits, to proto-flight or acceptance test levels as specified in GEVS section 2.6.3.2 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 should be approved by the GSFC Project, and should be presented at the earliest possible formal review, no later than PER.</td></tr>
<tr><td>Rationale:</td><td colspan="3">The test program ensures 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.)</td></tr>
<tr><td colspan="2">Revision Status:
Rev. H</td><td>Owner:
Thermal Engineering Branch (545, Primary) and Electrical Engineering Division (Code 560)</td><td>Reference:
GEVS 2.6.3.2</td></tr>
</table>

4.28	Thermal Design Verification		Mechanical
Rule:	All subsystems/systems having a thermal design with identifiable thermal design margins should be subject to a Thermal Balance Test at the appropriate assembly level per GEVS Section 2.6.4.		
Rationale:	This test provides an empirical verification of the subsystem/system's thermal design margin. In addition, steady state temperature data from this test is used to validate subsystem/system thermal math models (TMMs).		
Revision Status: Rev. E		**Owner:** Thermal Engineering Branch (545)	**Reference:** GEVS 2.6.4

4.29	Thermal-Vacuum Cycling	Mechanical
Rule:	All systems flying in unpressurized areas should 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 should be performed at the instrument level of assembly. 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.	
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).	
Revision Status: Rev. F, Updated Rev. G	**Owner:** Mission Systems Engineering Branch (599, Primary) and Thermal Engineering Branch (545)	**Reference:** GEVS 2.6.3.2.2

4.30	Materials Engineering Implementation		Mechanical
Rule:	Materials and processes intended for use in flight designs should be validated by Materials Engineering to be appropriate for the flight configuration, from concept through delivery of hardware, by establishing the discipline as a part of the engineering team pre-Phase A. Materials properties testing and verification needed to inform engineering analyses as well as Non-Destructive Evaluation (NDE) of hardware, should be identified.		
Rationale:	Early integration of materials engineering expertise throughout the project lifecycle—from concept through hardware delivery—is critical for ensuring proper materials selection, verification, and performance in the intended flight environment. Comprehensive materials validation, testing, and documentation prevents costly redesigns while providing essential data to support engineering decisions at all development phases. Involving materials engineers in design reviews, manufacturing process assessments, and testing activities safeguards mission success by ensuring reliable flight hardware that meets performance requirements while controlling costs and schedules.		
Revision Status: Rev. H		**Owner:** Materials Contamination and Coatings Branch (541)	**Reference:** GEVS 2.4 NASA-STD-6016

4.31	Planetary Protection, Planning, and Execution	Mechanical
Rule:	All missions, spacecraft, and hardware should meet planetary protection requirements if this rule is applicable, independent of Mission Classification (A-D). Applicability: • This rule applies to all spacecraft and spaceflight hardware that is sent outside of Earth's orbit and all spacecraft and spaceflight hardware returning to Earth or Earth's orbit from another planetary body. • This includes: missions launched from human-rated spacecraft and platforms, secondary payloads, payloads deployed from Earth-orbiting robotic missions, missions to and from the Earth's Moon. All sample return missions to Earth, Earth-Moon System and to platforms orbiting Earth and missions with heliocentric orbits.	
Rationale:	This rule provides additional guidance and best practices in accordance with NPR 8715.24 and NASA-STD-8719.27. Guidance and best practices assume familiarity with planetary protection and biology. For some missions, this will include insuring access to a lab capable of processing samples in accordance with NPR 8715.24 and NASA-STD-8719.27 (culture based sample collection and processing). Provide within the conceptual study the preliminary planetary categorization and requirements that will drive mission cost, schedule, design and implementation. Draft level 2 requirements for requested categorization in collaboration with MSE, contamination control lead, and science team or PDLs as applicable. Submit request for planetary protection categorization and finalize L2s subsequent to receipt of final planetary protection categorization, with appropriate CDRLs/other input included in MAR. Derive L3 and L4 requirements with allocation budget for bioburden (Cat III, Cat IV and some Cat IV missions) and verification points as part of the Planetary Protection Implementation Plan and overall requirements tracking process. Baseline planetary protection implementation plan 30 days prior to PDR and include in PDR. Update L3 and L4 requirements and inputs to planetary protection implementation plan prior to CDR and present at CDR. Implement all elements of the planetary protection implementation plan. Prior to pre-ship, prepare end item data package with requirement verification data, waivers, and any other applicable data (bioburden accounting, assay results, organic contam sampling, archiving) and decisions regarding planetary protection. Release pre-launch report in CM system 30 days prior to (SMSR), Pre and post launch, monitor system performance for evidence of planetary protection related deviations and off nominal conditions and prepare mitigation plans if necessary, conducting verification sampling or other verification methods consistent with L2-L4 requirements. Release post-launch report. Prepare Lessons learned for future projects post launch and release to CM. Submit End of Mission report to CM system 30 days prior to End of Mission. Status archiving of materials, as appropriate to categorization. Release Extended Mission Report in project CM system 30 days prior to Extended Mission Review.	
Revision Status: Rev I	**Owner:** Materials, Contamination Control, and Coatings Branch (541)	**Reference:** NPR 8715.24 NASA-STD-8719.27

5.04	Instrument Testing for Multipaction		Instruments
Rule:	Active RF components, such as radars, that develop significant RF power should be designed and tested for immunity to multipaction. If multipaction immunity is demonstrated by test alone, the test should be performed at least 6dB above the nominal power level. If satisfied by analysis and test, the analysis should show at least 10dB of margin above the nominal power level and the test should be performed at least 3dB above the nominal power level. Due to the inherent uncertainty in the analysis at these power levels, satisfaction by analysis alone is not recommended.		
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.		
Revision Status: Rev. E, Updated Rev. G	**Owner:** Microwave Instrument Technology Branch (555)		**Reference:**

5.05	Fluid Systems GSE		Instruments
Rule:	Fluid systems GSE used to pressurize flight systems should 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. It is advisable to have the preliminary design at PDR and completion and certification of the GSE by CDR.		
Revision Status: Rev. E	**Owner:** Cryogenics and Fluids Branch (552)		**Reference:** NPR 8715.3

5.06	Flight Instrument Detector Characterization Standard		Instruments
Rule:	Instrument detector systems (and associated components) should demonstrate performance via test over the expected operating temperature range before the Pre-Environmental Review (PER) to establish a performance baseline and provide a provisional verification of performance prior to exposure to non-operational environments, such as vibration, acoustics, non-operational temperatures, or other conditions required to demonstrate survival. At the conclusion of environmental testing, performance should again be characterized via test and the results compared to the baseline results.		
Rationale:	Instrument detector systems are mission critical to performance, and timely characterization over stressing environments is a critical risk reduction activity. Detector performance falls off 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. It is advisable to have critical parts and components tested over the flight operational range plus margin by MDR/SDR, and flight-like subsystem and components tested by PDR.		
Revision Status: Rev. E, Updated Rev. G		**Owner:** Instrument Systems and Technology Division (550)	**Reference:**

5.10	**Early Demonstration of Instrument Opto-Mechanical System Alignment and Test**	**Instruments**
Rule:	For instrument opto-mechanical systems that have not been demonstrated at TRL-9 within 10 years of SRR, an early Engineering Development Unit (EDU) or Engineering Test Unit (ETU) should be used to demonstrate the capability to fabricate, assemble, align, and test the opto-mechanical system. Optics, mechanisms, structures, and other components relevant to the instrument system, including all opto-mechanical features and interfaces, using components of the approximate fit, form, and function of the flight hardware should be part of the early demonstration. The hardware configuration for the demonstration should be agreed to by all stakeholders and phased with the flight unit to ensure that demonstration occurs early enough to be valuable.	
Rationale:	1) Early demonstration of the capability to fabricate, assemble, align and test opto-mechanical systems saves cost and mitigates schedule risks 2) Even with systems that have flight heritage, it is important that some members of the project team have experience with the relevant opto-mechanical system.	

Revision Status:	**Owner:**	**Reference:**
Rev. G	Optics, Lasers and Integrated Photonics Branch (551)	

<table>
<tr><td>5.11</td><td colspan="2">Instrument System Performance Margins</td><td>Instrument Systems</td></tr>
<tr><td>Rule:</td><td colspan="3">Instrument performance budgets should be developed for instrument systems and their sub-systems. The performance budgets should account for uncertainties including, but not limited to, fabrication, assembly, stability and test/verification. The project should have justification for the adequacy of their margins; test demonstration of predicted on-orbit performance with margins against the performance budgets is the preferred justification.</td></tr>
<tr><td>Rationale:</td><td colspan="3">Failure to properly allocate uncertainties in the fabrication, assembly, stability and test/verifications of instrument systems can result in an instrument that does not meet its performance requirements on orbit.</td></tr>
<tr><td colspan="2">Revision Status:
Rev. G</td><td>Owner:
Mission Engineering and Analysis Division (590, Primary) and Instrument Systems and Technology Division (550)</td><td>Reference:</td></tr>
</table>

5.12	Instrument/Subsystem Alignment, Integration, and Test Planning	Optics
Rule:	Instruments/subsystems containing optics systems should develop an alignment plan in Phase A which will be refined and tracked throughout the project life cycle. The alignment plan should address such considerations as: alignment philosophy including the number of datasets required for appropriate statistics to verify requirements; cross-checks for critical data; leveling the instrument to gravity during metrology as appropriate; fiducials and other references; and authority to proceed before breaking an alignment configuration. In addition, consideration should be given to likely failure modes during testing to ensure that the hardware and test design is adequate to determine test failure causes and corrective action.	
Rationale:	Projects that do not incorporate, alignment, integration and test planning early into the concept and design phases increase risk to cost, schedule, and overall instrument performance including risk to performance on orbit.	

Revision Status:	**Owner:**	**Reference:**
Rev. G	Optics, Lasers and Integrated Photonics Branch (551)	

5.13	Laser Life Testing		Instruments
Rule:	There should be a project-approved and peer-reviewed plan, consistent with the mission risk profile, for life-testing a laser prototype to a minimum of 1x of the mission lifetime requirement at stressing environments. The life-test unit should be a high-fidelity representation of the flight laser and any differences between the life test unit and the flight laser should be delineated in the plan. The plan should include system and component-level testing and/or analysis. Any components that have a wear-out or failure mechanism should be addressed in the plan either by testing or with justification for why testing is unnecessary. Accelerated tests are permitted (and even encouraged) if the acceleration factors are understood and justified. The plan should include technical, budget, schedule and resource assumptions upon which the plan is based.		
Rationale:	Lasers are often a new technology development area for a mission, and life limited; life testing is a risk reduction for these missions. There are unique requirements for laser life testing that differ significantly from those of electro-mechanical life-testing (GR 4.23). It is advisable to present life test conclusions and compare to mission performance requirements by PER.		
Revision Status: Rev. G	**Owner:** Optics, Lasers and Integrated Photonics Branch (551)		**Reference:**

5.14	Cryogenic Thermal Margins				Instruments		
Rule:	The Cryogenic Thermal Design should provide adequate margin to account for increased heat load or decreased cooling capability from conceptual design to implementation. This is applicable to passive systems operating below 120K and actively cooled systems below 200K.						
Rationale:	Knowledge of heat loads can be very uncertain at early design stages, so cryogenic thermal design should be done with appropriate amount of margin to ensure a viable design.						
Phase:	**<A**	**A**	**B**	**C**	**D**	**E**	**F**
Activities:	The cryogenic thermal design should have a 100% design margin on the current best estimate of the heat loads on the cryogenic subsystem.	The cryogenic thermal design should have a 100% design margin on the current best estimate of the heat loads on the cryogenic subsystem.	The cryogenic thermal design should have a 80% design margin on the current best estimate of the heat loads on the cryogenic subsystem.	The cryogenic thermal design should have a 50% design margin on the current best estimate of the heat loads on the cryogenic subsystem.	The cryogenic thermal design should have a 40% design margin on the current best estimate of the heat loads on the cryogenic subsystem.	The cryogenic thermal design should have a 33% design margin on the current best estimate of the heat loads on the cryogenic subsystem.	N/A
Revision Status: Rev. H		**Owner:** Cryogenics and Fluids Branch (Code 552, Primary) and Thermal Engineering Branch (Code 545)				**Reference:** NASA-GSFC Cryogenics and Fluids Branch/552	

Notes:
1) Margin% = (Cooling Capability – Current Best Estimate) / Current Best Estimate
2) Parasitic load margins are applied at the location in which they are incurred.

5.15	Stray Light Modeling and Mitigation			Instruments/Optical
Rule:	All optical systems should have an end-to-end stray light modeling and test campaign performed at the system level to identify background due to stray light effects and develop appropriate mitigation strategies to keep stray light effects within documented requirements. Throughout the life cycle, the model and test configuration should be continually updated to reflect the current state of the design, ultimately accurately capturing the as-built flight hardware*. "End-to-end" is defined as the entire path from the observed target to the detecting surface. "Optical systems" include, but are not necessarily limited to scientific instruments, guiders, cameras or other vision-type systems, lidar instruments, star trackers, and sun sensors.			
Rationale:	Stray light is a system issue that requires early awareness and continual coordination among various disciplines to ensure mitigation and system performance. End-to-end stray light modeling provides accurate estimates of background due to sources such as scattering from optical and hardware surfaces and background due to thermal self-emission, and guards against unintended optical paths, hardware glints and vignetting that may not be accurately identified or quantified through modeling of individual subsystems. Testing provides model validation and the ultimate requirement verification. Mitigation involves proactive modification of design as well as inspection of as-built hardware to assure that the hardware reflects the design intent. *Note: In this text, "as-built" refers to the extent that properties of mechanical, optomechanical, and optical surfaces are relevant to stray light performance of the system. An example of a relevant properties is coatings selection whereas a mechanical deviation within tolerance would not be relevant.			
Revision Status: Rev. G		**Owner:** Optics, Lasers and Integrated Photonics Branch (551)		**Reference:**

GLOSSARY AND ACRONYM GUIDE

AIAA	American Institute of Aeronautics and Astronautics
Anomaly	An unexpected event that is outside of certified design/performance specification limits. NOTE: Certified design limits are those identified in approved design-level documents
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 hazard, condition or event that could result in a mishap causing fatal injury to personnel and/or loss of spacecraft, launch vehicle or ground facility
CCP	Contamination Control Plan
CCSDS	Consultative Committee for Space Data Systems
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 7120.5)

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
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, Electronic, and Electromechanical
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 1-4)
ESD	Electro-Static Discharge

Established Reliability	Demonstrated operation (of a standard product or COTS assembly, component, or spacecraft) over years and production over multiple units by the same vendor, including possible changes due to obsolescence and modernization. May be quantified by risk classification using the Inherited Standard Products row in Table 1 along with Appendix D from GPR 8705.4A.
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 View
FPGA	Field Programmable Gate Array
FRR	Flight Readiness Review
FSW	Flight Software
GEVS	General Environmental Verification Standard
GN&C	Guidance, Navigation, and Control
GOLD	Goddard Open Learning Design
GPR	Goddard Procedural Requirement

GRT	Ground Readiness Test
GSE	Ground Support Equipment
Heritage hardware	Hardware from a previous project, program, or mission
High fidelity	Addresses form, fit, and function. Equipment that can simulate and validate all system specifications within a laboratory setting (Ref: Defense Acquisition University)
HW	Hardware
I&T	Integration and Test
ICD	Interface Control Document
I/F	Interface
I/O	Input / Output
ISR	Interrupt Service Routine
ITU	Integrated Test Unit
IVT	Interface Verification Test
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)
L&EO	Launch and Early Orbit
LRR	Launch Readiness Review

OS	Operating System
Margin	The amount by which hardware capability exceeds requirements (Ref: GEVS 1-7)
MDR	Mission Definition Review
MCR	Mission Concept Review
MEL	Mission Exceptions List
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 Reqs	Level 1 Mission Requirements or minimum mission success criteria for a project or program.
MOR	Mission Operations Review
MRR	Mission Readiness Review
MRT	Mission Readiness Test
ms	milliseconds
M&P	Materials and Processes
MSPSP	Missile System Prelaunch Safety Package
NDE	Non-Destructive Examination
NPR	NASA Procedural Requirements
ORR	Operational Readiness Review

OS	Operating System
Payload	An integrated assemblage of modules, subsystems, etc., designed to perform a specified mission in space (Ref: GEVS 1-6)
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)
POC	Point Of Contact
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 1-5)
PSR	Pre-Ship Review
RAM	Random Access Memory
RF	Radio Frequency
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 7120.5)

SAR	System Acceptance Review
S/C	Spacecraft
SDR	System Design Review
SEMP	Systems Engineering Management Plan
Simulation	The imitation of the behavioral characteristics of a system, entity, phenomenon or process. (Ref: NASA-STD-7001)
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
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 Space Flight Program and Project Management 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)
TAYF	Test As 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:
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
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

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	07-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.
E	21-Feb-12	Administrative Changes Only – Rule 1.06 (pages 12 - 13); reverts to previous version, in its entirety, for immediate near-term efficiency of mission application.
		Glossary and Acronym Guide – changed definition of Catastrophic Hazard (ref. Rule 1.26), for consistency with NASA-STD 8719.24.
F	10-Dec-12	New Rules 1.39, 2.23, 2.24, 2.25; Added Rule 4.01 Introduction and elsewhere as needed: Removed Rev. E delineation between Rules and Principles to identify all rules; rule = requirement Updated all GEVS references to align with latest version (TBD) of GEVS Updated owner organization throughout. Glossary – corrected definitions of anomaly and EEE CCR-D-0047
F	22-Jan-13	Administrative Change Only – Table 1.06-1: Phase B in Power line changed from 15% to 20%
F1	8-Feb-2013 6-Nov-2015	Administrative Change Only – Table 1.09: Note corrected to "not a global approval to waive TAYF for all elements". Acronym TYF corrected to TAYF. Rev G is an extensive revision

G		**Deleted The Following Rules:** 1.34 Close-out Photo Documentation Of Key Assemblies 2.02 EEE Parts Program For Flight Missions 2.03 Radiation Hardness Program 2.12 Printed Circuit Board Analysis 2.15 Flight and Ground Electrical Hardware 4.07 Solder Joint Intermetallics Mitigation 4.08 Space Environments Effects on Material Selection **Merged the Following "duplicate" Rules:** 2.07 End-to-End Test of Release Mechanism For Flight Deployable) merged with 4.18 (Deployment and Articulation Verification) and 2.07 removed 2.18 (Implementation of Redundancy) merged with 1.25 (Redundant Systems) and 2.18 removed **Revised The Following Rules (not a complete list):** 1.05 Single Point Failures – Clarified Wording 1.06 System Margins – Revised calculation to be consistent with industry practices; clarified margin and contingency to remove double bookkeeping 1.08 End-To-End Testing – Clarified Wording 1.23 Spacecraft "Off" Command – Simplified and clarified wording 1.40 Maintaining Command Authority of a Passive Spacecraft – significant rewrite 2.05 System Grounding Architecture – Added requirement to include GSE 2.24 – Solar Arrays – Significant Rewrite to give more detail on cell qualification and panel testing 3.07 Flight Software Margins – Rewrite of Table 3.07-1 to define verification methods 4.06 Validation of Thermal Coatings Properties – added detail on how to validate 4.23 Life Test – Added consideration for differences between drive electronics used in the life test versus the flight drive electronics 5.04 Instrument Testing for Multipaction – Significant rewrite 5.06 Flight Instrument Detector Characterization Standard – Added detector to title since that was the intent of the rule; added detail **Added The Following New Rules:** New Systems Engineering Rule 1.41 GSE Use At Launch Site New Systems Engineering Rule 1.42 Powering Off RF Command Receiver New Systems Engineering Rule 1.43 Flight Software Update Demonstration New Systems Engineering Rule 1.44 Early Interface Testing

		New Systems Engineering Rule 1.45 System Alignments New Systems Engineering Rule 1.46 Use of Micro-Switches New Systems Engineering Rule 1.47 Design Deployables for Test New Systems Engineering Rule 1.48 Space Data Systems Standards New Electrical Rule 2.26 Power-On Reset Visibility New Electrical Rule 2.27 Spacecraft Strip-Charting Capability New Instrument Rule 5.10 Early Demonstration of Instrument Opto-Mechanical Alignment and Test New Instrument Rule 5.11 Instrument System Performance Margins New Instrument Rule 5.12 Instrument Alignment, Integration and Test New Instrument Rule 5.13 Laser Life Testing
H	**Oct 2022**	Rev H is an extensive revision **Deleted the Following Rules:** 1.26 Safety Inhibits and Fault Tolerance – Covered by Safety Requirements 1.33 Polarity Checks of Critical Components – Merged with 1.07 1.35 Maturity Of New Technologies – Covered by NPR7123.1 5.08 Laser Development Contamination Control – Covered by 4.01 5.09 Cryogenic Pressure Relief – Covered by Safety Requirements **Revised The Following Rules (not a complete list):** 1.06 Resource Margins – Revised to Align with AIAA S-120A-2015 1.09 Test As You Fly – Added option to document via an Engineering Peer Review 2.22 Corona Region Testing Of High Voltage Equipment – Defined High Voltage 2.23 RF Component Testing For Multipaction and Corona – Rewrite For Clarity 3.05 Flight/Ground System Test Capabilities – 3.06 Dedicated Engineering Test Unit For Flight Software Testing – 4.15 Torque Margin – Revised with additional guidance **Added The Following New Rules:** 4.30 Materials Engineering Implementation 5.14 Cryogenic Thermal Margins 5.15 Stray Light Modeling and Mitigation
I	**August 2025**	Rev I is an extensive revision The introduction has been rewritten to reflect significant update to review and assessment process and general removal of waiver process.

		The rules have been reworded to reflect their status as design guidelines instead of requirements. In many cases, rationales have been updated to better reflect the thinking behind the rule. In most cases, mission phase-specific guidance has been removed. This was done in an attempt to provide better clarification regarding what the actual guidelines were, versus a recommended path for implementation. Rule 1.25 (Redundant Systems) has been merged into 1.05 (Single Point Failures) Rules 1.23 (Spacecraft “Off”) and 1.42 (Command Receiver “Off”) have been merged into 1.40 (Maintain Command Authority) Rule 3.01 has been removed Rule 4.11(Testing in Flight Configuration) has been merged into 1.09 (Test As You Fly) Rule 4.31 (Planetary Protection) has been added Branch codes and names updated to reflect ETD reorganization announced August 24, 2025