



## Goddard Procedural Requirements (GPR)

**DIRECTIVE NO.** GPR 8730.10 **APPROVED BY Signature:** \_\_\_\_\_  
**EFFECTIVE DATE:** \_\_\_\_\_ **NAME:** Judith N. Bruner  
**EXPIRATION DATE:** \_\_\_\_\_ **TITLE:** Director, Safety and Mission Assurance

### COMPLIANCE IS MANDATORY

**Responsible Office:** 300/Safety and Mission Assurance Directorate

**Title:** Safety and Mission Assurance Implementation Over Flight Project Lifecycles

### PREFACE

#### P.1 PURPOSE

This GPR defines how flight projects and the Safety and Mission Assurance (SMA) Directorate interact throughout the project lifecycle, from the start of the proposal process or authority to proceed through mission disposal. This directive also serves to identify the pertinent Goddard Space Flight Center (GSFC) and National Aeronautics and Space Administration (NASA) requirements that emanate from GSFC and NASA standards and directives that require project-unique actions.

#### P.2 APPLICABILITY

- a. This directive applies to all GSFC-managed space flight projects at Greenbelt and Wallops Flight Facility under NPR 7120.5. This directive is optional guidance for other projects, such as research and development projects under NPR 7120.8, “Do No Harm” projects, and suborbital and atmospheric projects. Projects managed outside of GSFC under a GSFC program office may use this as a guidance document.
- b. In this directive, all document citations are assumed to be the latest version unless otherwise noted.
- c. In this directive, all mandatory actions (i.e., requirements) are denoted by statements containing the term “shall.” The terms “may” or “can” denote discretionary privilege or permission; “should” denotes a good practice and is recommended but not required; “will” denotes expected outcome; and “are/is” denotes descriptive material.

#### P.3 AUTHORITIES

NPD 8730.5, NASA Quality Assurance Program Policy

#### P.4 APPLICABLE DOCUMENTS AND FORMS

- a. NPR 7120.5, NASA Space Flight Program and Project Management Requirements
- b. NPR 7120.8, NASA Research and Technology Program and Project Management Requirements

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

- c. NPR 8705.4, Risk Classification for NASA Payloads
- d. GPR 5330.1, Work Order Authorization (WOA) Process
- e. GPR 8621.4, GSFC Mishap Preparedness and Contingency Plan
- f. GPR 8705.4, Risk Classification Guidelines and Risk-Based SMA Practices for GSFC Payloads and Systems
- g. GPR 8730.5, SMA Acceptance of Inherited and Build-to-Print Items
- h. NASA-STD-6016, Standard Materials and Processes Requirements for Spacecraft
- i. NSTS/ISS 13830, "Payload Safety Review and Data Submittal Requirements"
- j. SSP 51700, "Payload Safety Policy and Requirements"
- k. 300-PG-7120.4.2, Risk Management Plan
- l. 372-PG-7120.2.1, Procedure for Planning and Implementing Software Assurance Programs
- m. 380-WI-7120.1.1, Project and/or Program Mission Assurance Requirements (MAR) Preparation
- n. EEE-INST-002, "Instructions for EEE Parts Selection, Screening, Qualification, and Derating"
- o. GPR 7150.4 Software Safety and Software Reliability Process
- p. NPR 8621.1 NASA Procedural Requirements for Mishap and Close Call Reporting, Investigating, and Recordkeeping

**P.5 CANCELLATION**

NONE

**P.6 SAFETY**

NONE

**P.7 TRAINING**

NONE

**P.8 RECORDS**

NONE

**P.9 MEASUREMENT/VERIFICATION**

NONE

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

## PROCEDURES

### 1.0 Background

This document defines how the SMA Directorate and flight projects will cooperate throughout the lifecycle of an instrument, spacecraft, or space mission to enable and achieve mission success in a robust and affordable manner. The purpose is to help a project avoid common hurdles and pitfalls in the safety and mission assurance area to make productive and strategic use of SMA expertise and capabilities. See Appendix F for a description of the Code 300 organization's goals and positions.

The SMA Directorate is structured to maximize the chances for mission success by implementing and influencing key processes (planning, design, production, manufacturing, test, operations, etc.) based on characterization, communication, and mitigation of risk.

### 2.0 Proposal phase

Following a decision to submit a mission or instrument proposal to an Announcement of Opportunity (AO) or notification of a new directed mission or instrument, the Code 380 New Business Coordinator will coordinate an SMA strategy meeting with project representatives (preferably, the Principal Investigator, the Project Manager, and the Mission Systems Engineer at a minimum) and the Codes 380, 370, and 360 Division Chiefs along with the applicable Branch Chiefs in Code 300. This strategy meeting will outline the basics of the SMA approach regarding staffing, planning, and risk.

At a minimum, the participants should include:

- a. Code 380 New Business Coordinator – Schedules and facilitates SMA Strategy session as new business opportunities develop.
- b. Program Chief Safety and Mission Assurance Officer (CSO) or SMA Lead –Coordinates the SMA team strategy to address assurance priorities and challenges consistent with risk posture and project attributes.
- c. Capture/Project Manager – Provides the mission and system design conceptual details and expected procurement strategy.
- d. Code 300 Executive Review Representative – Responsible for giving final directorate concurrence on SMA approach and proposal rider at the Center-level Executive Review.
- e. Code 300 Chief Engineer – Discovers technical and risk challenges associated with the mission design that must be addressed by the SMA strategy, recommends and assesses the balance among the disciplines to make the strategy consistent with risk posture and project attributes.

**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

Page 4 of 24

- f. Division Chiefs – Explains and coordinates division resources that can be applied to the SMA team to realize the identified strategy including reuse of previously developed information or deliverables, supports the CSO and the Code 300 Chief Engineer in discovering technical and risk challenges associated with the mission design that must be addressed by the SMA strategy.
- g. Branch Chiefs – Explains and coordinates branch resources that can be applied to the SMA team to realize the identified strategy including reuse of previously developed information or deliverables, supports the CSO and the Code 300 Chief Engineer in discovering technical and risk challenges associated with the mission design that must be addressed by the SMA strategy, explains lessons learned and best practices that can be leveraged for the benefit of SMA strategy development. Reliability Branch explains Fault Management strategy appropriate to the proposal.
- h. Standard Components Commodity Risk Assessment Engineer (CRAE) – Identifies standard components named or likely to be used to realize the mission, advises SMA team regarding strategy for inherited/heritage items reviews and risk mitigation indicated by prior usage records.
- i. Systems Review Manager – Identifies review approach most appropriate for the mission. Identifies risks and challenges associated with the mission design as it pertains to implementing the systems review process.

This meeting should involve a discussion of the following key attributes and how they should be used to shape the mission assurance strategy:

- a. The mission or instrument concept
- b. Preliminary design information, if known
- c. Heritage elements known at this time
- d. Inherited or build-to-print hardware or software brought to the table
- e. Known critical functions
- f. New developments or technology
- g. Architectural Concepts and Trade Studies conducted to date
- h. Known specialized EEE (electrical, electronic, and electromechanical) parts or components (e.g., custom detectors, high voltage devices, propulsion, etc.)
- i. Vendors, if known, for key elements
- j. Known aspects of the thermal and vibration environment, in testing and on-orbit
- k. Fault Management should have a basis when the proposal features lights-out autonomous operation, commensurate with time-to-effect analysis for hazards to the asset

In most cases a reliability/risk assessment should be proposed that considers the critical items and inherent fault-tolerance and margins in the design. This limited scope assessment will help to identify where limited resources may be applied most effectively to enable a robust design. The assessment should include Fault Management in the design.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

Page 5 of 24

The results of the meeting and upfront reliability/risk assessments, if performed, will be used by the Program CSO or assigned SMA lead to articulate a properly scoped SMA strategy for the project, including a budget, as well as to draft the inputs into the project proposal, as applicable. The SMA new business coordinator produces an informal project planning report that captures the basis of the SMA strategy (i.e., results of the meeting, reliability analyses, and strategic plan) as well as key recommendations from the team for use by the future Project CSO who is named upon project execution.

When a draft Mission Assurance Requirements (MAR) document is required during the proposal process, (e.g., to facilitate teaming and procurement purposes), the SMA lead or Program CSO will use the project information known-to-date, the project planning report, and the most relevant Code 380 Baseline MAR that is applicable to that mission type and classification and that aligns with the guidelines and requirements of GPR 8705.4 (these MARs are located at <https://spaces.gsfc.nasa.gov/display/SMA300/MAR+Preparation>). The SMA lead will coordinate with all of the SMA branches to tailor the baseline to the mission in each of the specific subject matter areas. A version of this document will be made available to the Project for use in competitive procurements or for requesting industry feedback as needed.

### 3.0 Project formulation phase

After a project is selected or directed, the Code 383 Branch Chief will assign a CSO, and the appropriate SMA branch managers will work with the CSO to assign the proper cadre of discipline experts to serve as the SMA team to cover the discipline areas required for the project. The typical SMA team consists of: Systems Safety (Code 360), Reliability (Code 371), , Software Assurance (Code 372), Quality Engineering (Code 373), Materials and Processes Assurance Engineer (Code 373), Parts and Radiation Assurance Engineer (Code 373), Supply Chain Manager (Code 382). Under the leadership of the CSO, the project information already collected will be combined with the risk posture and risk classification, and any upfront reliability /risk assessments, and used in concert with the following documents to create a project-specific MAR document and SMA Plan (SMAP):

- a. SMA Strategy Meeting Project Planning Report (see previous section)
- b. Pertinent risk classification and mission-attribute-specific MAR Baseline (or draft proposal MAR if one was developed during the proposal process)
- c. GPR 8705.4
- d. Commodity Usage Guidelines (CUG)
- e. Other broadly applicable directives and standards<sup>1</sup>,

The SMAP is a requirement of NPR 7120.5. Initial design information will be used to establish the relevant parts and materials lists, standard components, environmental test strategies, and other mission

---

<sup>1</sup> See Appendix C for the list of broadly applicable directives and standards, many of which will be captured in the baseline MAR

**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

design parameters that drive SMA planning. The risk classification (per NPR 8705.4 for projects governed by NPR 7120.5), upfront reliability/risk assessments, and GPR 8705.4 inform further definition and tailoring of requirements. EEE-INST-002 and the CUG will be used to aid in selection of heritage parts and components and in identifying part and component level requirements (qualification, screening, contamination, workmanship, etc.). The CSO should ensure that the project MARs and SMAPs are representative of the risk classification and have requirement thresholds tuned for the criticality determined from the reliability analysis. Reliability analysis should include an assessment of the benefits of Fault Management, particularly if lights-out operations are proposed to reduce overall projected cost. For in-house projects, the SMAP will contain, on behalf of the supplier, who is Code 500, Code 600, or Code 800, minimum requirements implemented by GSFC through the Quality Management System (QMS) documentation to achieve the MAR requirements. The project MAR requirements should be synchronized with environmental test requirements as the two are developed together.

Once a draft project MAR is produced based on all considerations above, it is essential that it be discussed with all Prime contractors prior to holding a MAR Roundtable. See 380-WI-7120.1.1 for instructions on how to prepare a MAR. The CSO, in coordination with the assigned Supply Chain Manager (SCM), is responsible for gathering feedback from the Prime contractors and known subcontractors to determine their ability and intent for meeting or not meeting the requirements. In order to ensure the highest likelihood of receiving the best product from a provider, the intent should be to establish requirements that recognize and allow suppliers' equivalent approaches while minimizing formal waivers. In general, imposing requirements on the suppliers at their objection involves risk, so careful investigation is required to identify the risks associated with the gap between the requirements and the suppliers' processes and to identify effective risk mitigations where the gaps are critical. Viable trades apply at the MAR Roundtable discussion. For example, Fault Management might be best hosted on-board the flight asset or alternatively within the Ground Segment, wherein different suppliers may be applicable and different suppliers may have significant constraints. No efforts should be made to influence the vendor to follow different requirements without performing a risk assessment that includes a risk statement, likelihood and consequence, and a risk mitigation sequence. The CSO shall be responsible for ensuring this risk assessment is performed by the appropriate SMA subject matter experts for the areas and requirements being evaluated. The CSO coordinates any additional resources that may be needed to perform this evaluation with the Project.

A system review plan should be developed that will apply the guidelines from GSFC-STD-1001 with requirements from NPR 7120.5, NPR 7123.1, GPR 8700.4, and GPR 7123.1 to establish the milestone reviews and identify responsibilities. This plan should be a joint effort between the System Review function, the project, and the program office. Note that the system review plan is not part of the project SMA activities, but it is part of an independent review function covering engineering, SMA, and project management activities. Other plans may be developed when required by applicable NASA or GSFC directives, generally based on risk classification or other mission attributes.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

#### 4.0 Early Design Phase

Elements of early design may occur before and/or after selections have been made from an AO or GSFC has been assigned a directed mission. Upfront involvement of some key SMA and engineering functions in early design work is essential to prevent later problems that may be very costly to recover from. The level of GSFC involvement will depend upon the extent of GSFC's role in the development of the products. The following organizations should participate in early design activities as highlighted below:

- a. Parts and Radiation Assurance Engineer (PRAE) (373): assesses risk in parts selection, screening, testing, manufacturing, and nonconformances, to avoid unnecessary risk and minimize challenges in having parts approved for usage
- b. Materials & Processes Assurance Engineer (MPAE) (373): assesses risk in materials selection, manufacturing and testing nonconformances, process development, drawing development
- c. Reliability (371): fault-tolerance, expected lifetime, qualification for flight, identification of the key commodities, Fault Management architecture, and Ground Segment Availability requirements.
- d. Software Assurance (372): identification of safety critical and mission critical software, fault management testing, evaluation of software heritage or new technology
- e. Quality (373): design for manufacturability, quality controls, critical supplier capabilities for realizing the design, critical sensitivity to workmanship issues, capture of relevant defects and development unit test results
- f. System Safety (360): interface with US Air Force and NASA/ Kennedy Space Center (KSC) through Payload Safety Introduction Briefing (PSIB) to external Payload Safety Working Group (PSWG) in System Requirements Review (SRR) timeframe, tailoring of range safety requirements for particular project, fault tolerance / safety inhibits
- g. CSO (383): identify areas where SMA experts can help the project, share SMA lessons learned, identify system constraints that impact quality and reliability of the new design, and identify alternate sources and paths for critical Research and Development (R&D) products.
- h. Supply Chain Manager (382): provide historical knowledge about external suppliers

The upfront efforts of these organizations come at a small direct cost, but will likely obviate significant project expenditures through the prevention and avoidance of problems later in the project lifecycle. At this point the mission systems engineer, CSO, I&T lead or other project representative shall create a brief plan that establishes the intended uses for Engineering Models, Engineering Development Units, and Engineering Test Units, and defines its alignment with guidance in NPR 8705.4<sup>2</sup>.

#### 5.0 Project Implementation (development) phase

Parts Control Boards (PCBs) and Materials and Process Control Boards (MPCBs) are formed to approve all parts, materials, and processes against guidelines and requirements in EEE-INST-002, NASA-STD-

---

<sup>2</sup> Appendix D includes guidance for developing an Engineering Unit Plan.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

6016 or the associated GSFC standard, when developed, the Workmanship Standards and other GSFC technical standards applicable to EEE parts and special processes, and establish criteria for qualifying and life testing parts, materials, and processes when needed, and disposition nonconforming, out-of-family, and unfamiliar items as they arise. The MPAEs and PRAEs will work with Codes 541 and 562 respectively to ensure that both Directorates have all of the pertinent information needed to complete their approvals and risk assessments. For in-house designs, Code 562 and Code 541 schedule and lead the control boards and the PRAE and MPAE are participating members representing the interests of SMA. For out-of-house designs, the PRAE and MPAE are generally participating members on control boards established and run by the prime contractor. The PRAE should support the PCB in cases to the greatest extent feasible, but at the very least where items are held up for over three weeks in the PCB without disposition or in cases where risk assessments are needed or where parts are proposed that are outside of GSFC's experience base. The MPAE from Code 373 should support the MPCB (or equivalent) to the greatest extent feasible, but at the very least in cases where items are held up for over three weeks in the MPCB without disposition or in cases where risk assessments are needed or where materials or processes are proposed that are outside of GSFC's experience base. The primary functions of the MPAE and PRAE are to perform risk assessments to determine whether products that are nonconforming, out-of-family, or outside of our experience base entail risk in the specific project environment and operation, and whether mitigations or more information are needed. It is essential that the risk assessments are performed and details captured to ensure that learning is continuous and that subsequent risk assessments are performed consistently, efficiently, and effectively. Electronic packaging and Workmanship risk assessments are the responsibility of the Electronic Packaging CRAE and Workmanship subject matter experts. For in-house production, support from the GSFC Workmanship Program Manager may also be required. Typically for Class A and Class B projects, applicable SMA personnel, e.g., Reliability Engineers (REs), CRAEs, and Software Assurance Engineers (SAEs), review and/or approve Engineering Change Requests (ECRs).

The project CSO (or SMA lead if no CSO is assigned) will submit the recommended SMA budget and planned SMA activities to the project and will facilitate negotiations between the Project and the SMA Division and/or Branch chiefs or their designee where adjustments are required and discussions are needed for further explanation or definition of the planned SMA activities. The final budget for SMA support to a project will define the SMA activities to achieve a given risk posture. After the final budget is determined per agreement between the SMA Divisions/Branches and project management, any requested change in budget will require a renegotiation and re-evaluation of the risk posture, and the new risk posture communicated to the project management.

## 5.1 Receipt of products

The details of handling nonconforming items are specified in GPR 8705.4, but will be addressed here for convenience to establish the SMA roles. With the exception of build-to-print and inherited items that are declared upfront to be built to different requirements (see 5.1.1), when an item is either received as nonconforming to the product specification or to other requirements in the project MAR or Statement of Work, or if it is determined to be nonconforming based on a test failure or anomaly, an acceptability

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

determination shall be made by the appropriate SMA discipline expert in consultation with the PDL. Also, if a determination is made that the nonconformance is likely to be attributed to a problem that originates with the vendor, pertinent information about the nonconformance will be provided to the SCM, Code 382, to follow up with the vendor by an appropriate means. The SMA discipline expert will be engaged to lead the effort of dispositioning the item, including the determination of elevated risk that may be present due to the non-conformance and available risk mitigations. The preliminary information and results will be provided to the SCM by an appropriate means such as email, hardcopy, or entry into the GSFC Management System Modernization (Meta) system to both avail to project of prior findings and solutions and to maintain the supplier history. The SCM screens and adjusts the data as they are received to ensure the records are relevant, current and accurate. Prior to returning to the vendor or a different vendor to make a repeated attempt to produce the same product, the project, with help from the SCM and subject matter experts if necessary, will ensure that cause for the nonconforming product is understood and that the problem has been corrected. In cases where there are insufficient data to make the determination, the project should disposition a risk in the project risk board that the same problem may recur. The SCM is to review the nonconforming product from an external supplier and address each of the following aspects:

- a. Identify potential need for an advisory in the form of (1) a Government-Industry Data Exchange Program (GIDEP) alert, (2) a GIDEP problem advisory, (3) a GIDEP lesson learned, (4) a NASA advisory, (5) a Code 300 watchlist item, or (6) other form of notification to projects. Collaboration with the GSFC GIDEP Program Manager may be required to determine (1) through (4).
- b. Submit issue into the Code 300 risk system if historical data indicate a systemic, recurring or crosscutting concern.
- c. Notify CSOs where the supplier is present on other Project supply chains.
- d. Provide input to the Project and CSO about the necessity and risk implications of the driving requirement to assess whether a requirement change should be considered.

### **5.1.1 Inherited and Build-to-Print Items**

Items that are built-to-print from an existing design or inherited from a previous development fall under the responsibility of the Standard Components (SC) CRAE and will implement GPR 8730.5 SMA Acceptance of Inherited and Build-to-Print Items.

## **5.2 SMA Directorate-Level Risk Management**

Risk management requirements for GSFC are baselined in GPR 7120.4. Local requirements for risk management within Code 300 are baselined in 300-PG-7120.4.2, but salient points are captured here to establish the processes for completing the disposition of nonconforming items. Code 300 employs a tiered, structured, risk management process (consisting of a Risk Advisory Committee and Risk Advisory Board) to capture, characterize, and manage SMA related concerns/risks/issues, primarily cross-cutting in nature, that impact multiple projects, programs, and/or organizations. When the determination is made from the project engineering or SMA teams that a concern, risk, or issue pertains

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

to other organizations inside or outside of GSFC, the item is brought before the Code 300 risk management board to make a directorate level assessment of recommended actions, including the possible alert mechanisms characterized earlier. This provides a structured approach to decide on whether an alert is necessary and what the best course of action is. Generally, the risks brought before the Code 300 risk management board are of a cross-cutting nature, affecting multiple projects or institutional capabilities, but on occasion, the board will monitor and track individual project risks that have very high visibility and impact to the agency, or in cases where there is disagreement or strong distinction of the details within the project about the risk.

### **5.3 Reliability/Maintainability/Risk Analysis**

The project RE will build upon the reliability, maintainability, and/or risk analysis performed in the early design phase and based on requirements established in the MAR (or as identified in the SMAP). This needs to include the Ground Segment as well as the flight segment, and should include time-to-effect analysis to substantiate the decision to host some Fault Management functions on-board and some Fault Management functions within the Ground Segment. Fault Management should fully utilize Probabilistic Risk Assessments (PRAs), Failure Modes Effects and Criticality Analyses (FMECAs), Critical Items or Single Point Failure Analyses, Worst Case Analyses, Parts Stress Analyses, or other similar products to support redundancy decisions and overall Fault Management architecture decisions. These analyses should leverage off of analyses from similar components from other projects, referencing pertinent Code 300 CUG if they are available, or existing analyses provided by suppliers, as available. Furthermore, they should always be performed prior to integration of the pertinent components and updated when newer information becomes available. The REs will work closely with the CRAEs, other SMA personnel, systems engineers or Product Design Leads (PDLs), and other project personnel to ensure that corresponding analysis reflects the latest knowledge/information available.

### **5.4 System Safety Analyses, Deliverables & Reviews**

The Project Safety Manager (PSM) will perform (or monitor performance of) hazard analyses and assure compliance to range safety requirements per NASA-STD-8719.24 “NASA Expendable Launch Vehicle Payload Safety Requirements”. Hazard analysis results will be documented in hazard reports that will be included in Safety Data Packages (SDPs) delivered to Launch Site Range Safety and will support the external safety review process defined in NPR 8715.7, “Expendable Launch Vehicle Payload Safety Program” for all Expendable Launch Vehicle (ELV) missions and instruments. Code 360 will maintain a database of hazard reports that are common across most missions and provide them to development teams for incorporation of mission specific elements. For example, it is common for a project to require powering of the spacecraft or Ground Support Equipment (GSE) at the range, while the vehicle or launch vehicle is fueled. Given that this environment is by definition an Occupational Safety and Health Administration (OSHA) Class I Division II environment, there will always be hazard associated with incandive devices at the range. For International Space Station (ISS) payloads, PSMs will perform hazard analyses and assure compliance to safety requirements per SSP 51700 “Payload Safety Policy and Requirements for the International Space Station” and will develop and deliver SDPs in support of

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.



**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

The PSM from Code 360 shall be responsible for providing system safety support to hazardous operations at the Payload Processing Facility (PPF) and the launch site, ensuring that a mishap GO-kit is available at the PPF and the launch site, and ensuring that an Interim Response Team is identified, trained, and present at launch site per the project Mishap Preparedness & Contingency Plan (MPCP). The MPCP thoroughly identifies the Interim Response Team's (IRT's) responsibilities. Typically the PSM or the CSO will serve as the IRT Chair. Outside of system safety, a subset of the mission assurance team, including the CSO, will support operations at the PPF, the launch site, and in the mission operations center until the mission completes commissioning. The CSO will Support Launch and Mission Operations, typically performing the role of "Spacecraft SMA" on console, and support planning meetings for spacecraft maneuvers and first time events. The CSO also manages Project/Program Mishap Preparedness Contingency Plan compliance per GPR 8621.4. The CSO's role is to ensure that all anomalies are captured and tracked in SOARS or the designated problem reporting system. Additionally, CSOs verify acceptable resolution of anomaly reports, often requiring the CSO to conduct or support anomaly resolution meetings. Ultimately, the CSO must verify acceptable resolution of anomaly reports and ensure that all critical anomalies are captured in the SOAR module in Meta (SOAR) at the completion of Spacecraft Commissioning. The SAE will provide support to the CSO for software-related anomalies, including Fault Management performance reporting. The SAE will provide continuity of support monitoring and validating configuration management changes to flight and ground software products, as well as completing knowledge transfer to the respective Mission Operations Assurance Engineer (MOAE).

## 8.0 Mission Operations

Beginning with the System Integration Review (SIR), the project will be supported by a Mission Operations Assurance Engineer (MOAE) from Code 372. The MOAE will work closely with the SMA team to ensure that the Fault Management autonomy has been thoroughly tested for 'Do No Harm' in and of itself and pre-launch readiness of operational products, personnel, and facilities, monitor PR/PFR closures, operational workarounds and waivers leading up to launch, and support critical end-to-end test campaigns. This low level of support is intended to facilitate mission knowledge transfer and ensure a smooth transition of SMA support into the operational phase. Post launch, the MOAE will evaluate on-orbit anomalies and resolutions, ensure that all on-orbit anomalies are entered in the Meta system, collaborate with CRAEs and REs in support of on-orbit failure and reliability analyses, evaluate change management processes, products, and system baselines, monitor and validate on-orbit flight software changes/uploads and ensure that all approved changes are documented and implemented, and report significant activities, cross-cutting trends, risks, and lessons learned to SMA Management and MOA customers. The MOAE remains with the operating mission until decommissioning.

## Appendix A – Definitions

- A.1 Anomaly** – An unexpected event that is outside of certified design/performance specification limits.
- A.2 Government-Industry Data Exchange Program (GIDEP)** – A cooperative program that collects and distributes Alerts, Safe Alerts, Problem Advisories, and Agency Action Notices to participating organizations.
- A.3 Inherited Item** - An item brought in to a project as a fully designed item that has some amount of prior history that may be built to different standards than those in project mission assurance requirements, and may not have had NASA insight into the design or construction.
- A.4 MAR** - Collection of tailored SMA requirements to be put on GSFC procurements.
- A.5 MPAE** – Engineer responsible for leading risk-based assessments and decisions on issues, concerns, and special applications of material and process requirements.
- A.6 Nonconformance** – A property that at least one requirement or specification is violated.
- A.7 Out-of-family**– Having the property that requirements are satisfied, but in instances where there are multiple copies of the same item or there is significant prior heritage basis for establishing in-family performance, one or more items indicate a performance bias, different trends, or other indicators that the item is different from the family.
- A.8 PRAE** - Engineer responsible for leading risk-based assessments and decisions on issues, concerns, and special applications of EEE parts and radiation requirements.
- A.9 Risk** - The combination of a) the probability (qualitative or quantitative) that an organization will experience an undesired event such as cost overrun, schedule slippage, safety mishap, or failure to achieve a needed technological breakthrough; and b) the consequences, impact, or severity of the undesired event were it to occur.
- A.10 CRAE** - Engineer responsible for tracking, qualifying, maintaining lessons learned on, and assessing risk on the use of standard spacecraft components used on multiple projects.
- A.11 SOAR** - On-orbit anomalies documented in the SOAR database when GSFC is performing the on-orbit operations.



**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

Page 15 of 24

<b>PSIB</b>	Payload Safety Introduction Briefing
<b>PSM</b>	Project Safety Manager
<b>PSWG</b>	Payload Safety Working Group
<b>QA</b>	Quality Assurance
<b>QE</b>	Quality Engineer
<b>QMS</b>	Quality Management System
<b>R&amp;D</b>	Research and Development
<b>RE</b>	Reliability Engineer
<b>SC</b>	Standard Components
<b>SCM</b>	Supply Chain Manager
<b>SDP</b>	Safety Data Package
<b>SIR</b>	System Integration Review
<b>SMA</b>	Safety and Mission Assurance
<b>SMAP</b>	Safety and Mission Assurance Plan
<b>SOARS</b>	Space On-orbit Anomaly Reporting System
<b>SRR</b>	System Requirements Review
<b>STEP</b>	Safety and Mission Assurance Technical Excellence Program
<b>SAE</b>	Software Assurance Engineer
<b>WOA</b>	Work Order Authorization

DRAFT FOR REVIEW

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

## Appendix C– Broadly Applicable Directives and Standards

### C.1 Purpose

The following is a list of NASA and GSFC directives and standards that require project-unique actions. This list shall serve as the flow down list for projects to help determine what to put in place on contracts via MAR, Statement of Work, or System Requirements Documents.

Table C.1 Broadly applicable directives and standards

Directive/Standard	Functional Area
NPR 7120.5	Project Management
NPR 7123.1	Systems Engineering
NPR 7150.2	Software Engineering
NPR 8621.1	Mishaps
NPR 8705.5	Probabilistic Risk Assessment
NPR 8715.3	General Safety
NPR 8735.1C	GIDEPs
NPR 8715.7	ELV Payload Safety Program
NPD 8730.2C	Parts Policy
NPD 8730.5B	Quality Assurance
NASA-STD-8719.13	Software Safety Standard
NASA-STD-8719.14	Orbital Debris
NASA-STD-8719.9	Lifting Standard
NASA-STD-8719.24	ELV Payload Safety Requirements
NASA-STD-8739.1,4,5,6	Workmanship Standards

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

NASA-STD-8739.8	Software Assurance Standard
IPC-J-STD-001ES	Space Applications Electronic Hardware Addendum to IPC J-STD-001E Requirements for Soldered Electrical and Electronic Assemblies
GPR 5340.3	Preparation and Handling of GIDEP Alerts, GIDEP Safe-Alerts, GIDEP Problem Advisories, GIDEP Agency Action Notices, and NASA Advisories
GPR 5340.4	Problem Reporting and Problem Failure Reporting
GPR 7120.4	Risk Management
GPR 7120.7	Schedule Margins and Budget Reserves to be Used In Planning Flight Projects and In Tracking Their Performance
GPR 7120.9	Project Scientist Roles and Responsibilities
GPR 7123.1	Systems Engineering
GPR 7150.1	Software Project Process Initiation
GPR 7150.2	In-house Software Development and Maintenance
GPR 7150.3	Software Acquisition
GPR 7150.4	Software Safety and Software Reliability Process
GPR 8700.4	Goddard Systems Reviews
GPR 8700.6	Engineering Peer Reviews
GPR 8700.7	Tool Control Program
500-PG-4520.2.1	Electrical, Electronic and Electromechanical (EEE)

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

	Counterfeit Parts Avoidance Plan (CPAP)
500-PG-8700.2.7	Design of Space Flight Field Programmable Gate Arrays (FPGAs)
500-PG-8700.2.8	Field Programmable Gate Array (FPGA) Development Methodology
540-PG-8072.1.2	Mechanical Fastener Torque Guidelines
541-PG-8072.1.2	Goddard Space Flight Center Fastener Integrity Requirements
GSFC-STD-1000	Rules for the Design, Development, Verification, and Operation of Flight Systems (GOLD rules)
GSFC-STD-7000	General Environmental Verification Standard (GEVS)
GSFC-STD-1001	Criteria for Flight and Flight Support System Lifecycle Reviews
GPR-5100.4E	Supplier Assessment Process

DRAFT FOR REVIEW

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

## Appendix D – Engineering Unit Plan Guidance

### D.1 Purpose

The purpose of this Appendix is to provide guidance for projects to use to establish a plan for the use of engineering models and engineering test units.

### D.2 EM/ETU/EDU practices

The project should establish the purpose up front for the use of engineering models and engineering units. The following is a list of the common purposes for the use of engineering units. The parenthetical comments indicate whether or not flight vendors are necessary to be used for the boards and parts, and whether Quality Assurance (QA) review/signoff should be required:

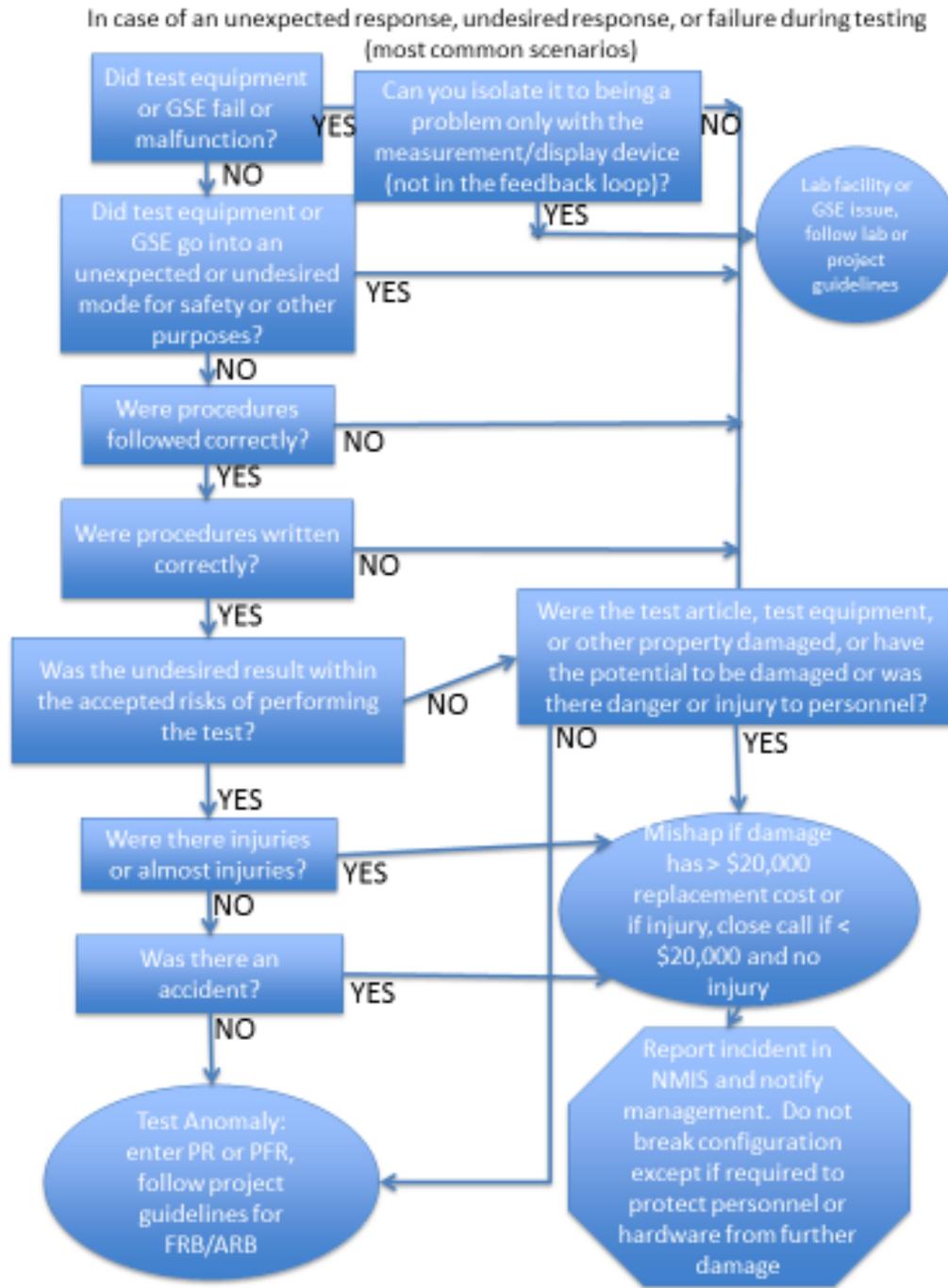
- a. Verify the parts fit together (flight vendor must be used, QA review may not be necessary)
- b. Prove the design (flight vendor may not be necessary, QA review not necessary)
- c. Practice for flight developments (flight vendor may not be necessary, QA review is necessary)
- d. Produce possible spares in case of emergency (flight vendor must be used, QA review is necessary)
- e. Determining manufacturability (flight vendor necessary, QA review desirable)
- f. Use as temporary inside spacecraft or instrument as a “placeholder” for integrated tests (flight vendor desirable, QA review is necessary)
- g. Parametric trades (flight vendor not necessary, QA review not necessary)
- h. Sensitivity or robustness analysis (flight vendor not necessary, QA review not necessary)
- i. Verify environmental performance (EMI, thermal, vacuum, mechanical) – (flight vendors are required, nonconformances documented, QA review desirable)

After Mission Concept Review, the project should establish an engineering unit guidelines document that highlights the purposes of the engineering unit work from the list above, and with additional items, if applicable. The purpose of this document is to establish the practices that will be applicable to the engineering unit development. Hence if a decision is made during the development phase to eliminate some of these practices, these guidelines can be used to decide whether there is sufficient justification to consider the engineering unit work.

**Appendix E – Mishap vs Test Anomaly logic flow diagram**

**E. 1 Purpose**

This appendix provides guidance for distinguishing between a mishap and a test anomaly.



CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT <http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

Page 21 of 24

## **Appendix F – New Positions and associated processes in the SMA organization**

Throughout the mission lifecycle the Chief Safety and Mission Assurance Officer (CSO) assigned to the Project by the Code 383 Branch Chief, recommends utilization of SMA technical experts, who form and are members of the Project SMA team, for identifying SMA requirements and techniques for assuring mission success.

The SMA team assigned to the Project typically utilizes conventional SMA discipline experts such as reliability, quality, and safety engineers as well as newly defined positions, such as the PRAEs (Parts and Radiation Assurance Engineers), Materials & Processes Assurance Engineers (MPAEs), Mission Operations Assurance Engineers (MOAEs), and CRAEs (Commodity Risk Assessment Engineers). The emphasis on continual learning as technologies evolve will result in the avoidance of overly expensive solutions typically employed when the risks are not understood. In addition, System Safety's involvement in International Space Station (ISS) instruments/payloads as early as possible in the process has been demonstrated as critical to help better understand ISS interfaces and the ISS safety review process.

Initially, the primary functions of the PRAEs and the MPAEs will be to review all of the items going into Parts Control Boards (PCBs) and Materials and Processes Control Boards (MPCBs) or other materials and processes reviews, making sure that they are prioritized by risk, that nothing bogs down the system that doesn't involve risk to the project, and that items involving higher risk (based on a specific review in context considering criticality, environment, and operation) get early attention and don't get set aside. Likewise they will be looking at GIDEPs from a cross-cutting perspective and identifying cross-cutting dispositions reducing duplication of effort and contradictory closure/resolution actions.

The Center uses the CRAE positions to perform risk assessments in those areas where they have deep expertise. This CRAE expertise provides the Center a thorough understanding of technical root cause, characterization of risk, and understanding risk mitigation options.

A CRAE provides technical expertise as it relates to quality, reliability, and mission assurance to Projects and CSOs in the technical area ("commodity") that they represent. This expertise spans across a wide range of technology and mission lifecycle topics. CRAEs address and resolve issues that are unique to one Project but also help to resolve technical issues that are crosscutting. CRAEs are responsible for conducting independent research to support Project needs or for technical policy development. CRAEs must be able to represent the Center's technical position and interests in their subject matter area to the SMA Chief Engineer and GSFC Project and Organizational managers as well as NASA's supply chain and Industry.

CRAEs are responsible for conducting independent research to support Project needs, as well as to provide new technical knowledge that is needed to address recurring or emerging issues. They are responsible for pushing this new technical knowledge into updated technical policy that flows either

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.

**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

from the NASA HQ or the GSFC Center level. The CRAEs will also maintain Commodity Usage Guidelines (CUGs) that document their commodity knowledge gained regarding risk, research, testing, and best practices to facilitate communication and archiving of their expertise and findings.

The MOAE supports the project beginning with the System Integration Review (SIR) and remains with the operating mission until decommissioning. The MOAE helps to ensure that Fault Management autonomy and pre-launch readiness of operational products has been thoroughly tested. The MOAE facilitates mission knowledge transfer to help ensure a smooth transition of SMA support into the operational phase. Post launch, the MOAE will evaluate on-orbit anomalies and resolutions, ensure that all on-orbit anomalies are entered in the Meta system, collaborate with CRAEs and REs in support of on-orbit failure and reliability analyses, evaluate change management processes, products, and system baselines, monitor and validate on-orbit flight software changes/uploads and ensure that all approved changes are documented and implemented, and report significant activities, cross-cutting trends, risks, and lessons learned to SMA Management and MOA customers.

The SMA team members and their assignments (i.e., roles and deliverables) reflect the GSFC “Mission Success” shown in Figure 1, which defines the relationships among the Technical experts, QE generalists, Mission Operations, and the Supply Chain management. Reach out to other disciplines is available as needed. This Mission Success model improves technical value to Projects, promotes capture and reuse of knowledge that is traditionally isolated in Project silos, and promotes continuous improvement.

DRAFT FOR REVIEW

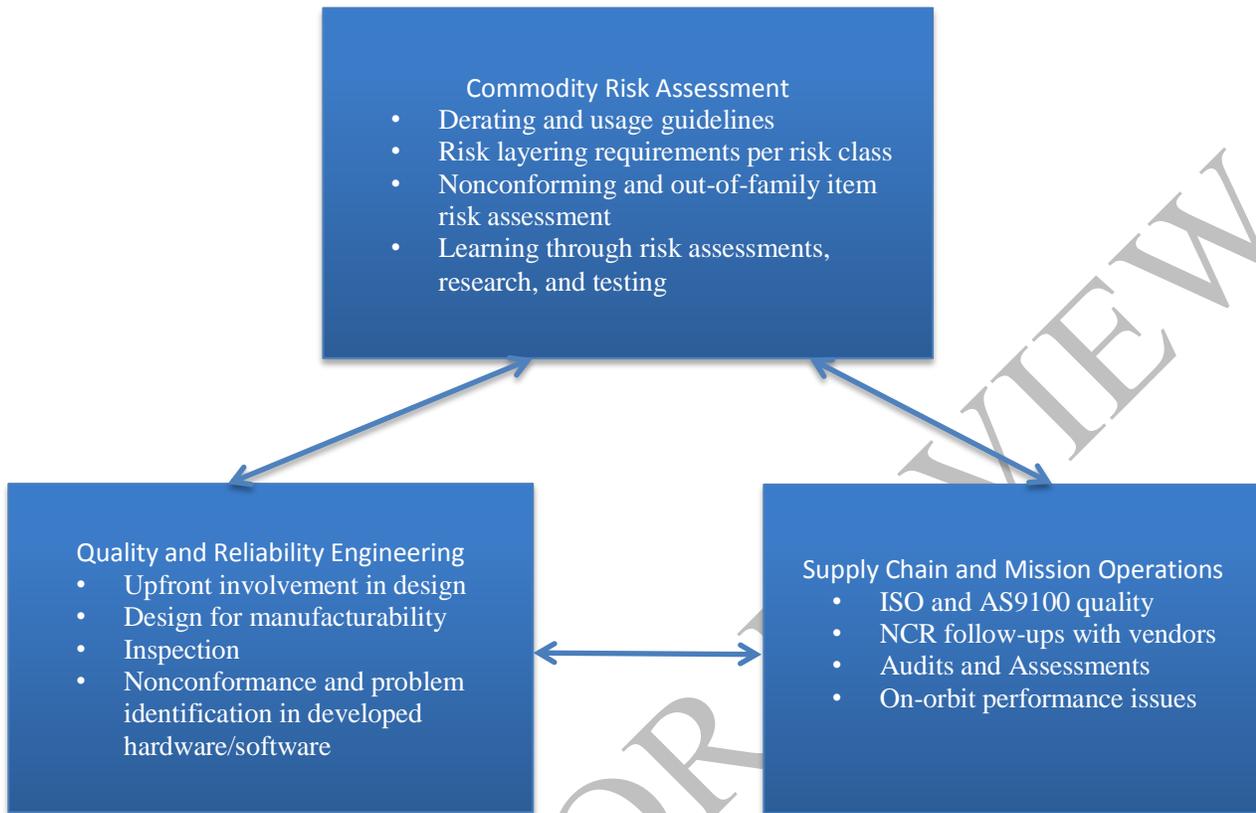


Figure 1. GSFC Mission Success Triangle

**DIRECTIVE NO.** GPR 8730.10  
**EFFECTIVE DATE:** \_\_\_\_\_  
**EXPIRATION DATE:** \_\_\_\_\_

**CHANGE HISTORY LOG**

<b>Revision</b>	<b>Effective Date</b>	<b>Description of Changes</b>
Baseline	TBD	Initial Release

DRAFT FOR REVIEW

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT  
<http://gdms.gsfc.nasa.gov> TO VERIFY THAT THIS IS THE CORRECT VERSION PRIOR TO USE.