Science Mission Directorate
Standard
Mission Assurance Requirements
Payload Classification: D

REVISION HISTORY

Version	Date	Description

TABLE OF CONTENTS

1 GENERAL 5
1.1 Safety and Mission Assurance Program 6
1.2 Management 6
1.3 Reporting 6
1.4 Surveillance 6
1.5 Requirements Flow-down 7
1.6 Suspension of Work Activities 7
1.7 SUSPICION OF FRAUD, WASTE, OR ABUSE 7
1.8 SMA acceptance of Inherited, build-to-print, or Modified Heritage Items 7
2 QUALITY MANAGEMENT SYSTEM 9
2.1 General 9
2.1.1 Quality Assurance 9
2.1.2 Control of Nonconforming Product 10
2.1.3 Material Review Board (MRB) 10
2.1.4 Reporting of Failures and Anomalies 11
3 SYSTEM SAFETY 11
3.1 General 11
3.1.1 Applicable Safety Requirements 12
3.2 System Safety Deliverables 13
3.2.1 System Safety Plan (Formal delivery required) 13
3.2.2 Tailored Payload (Spacecraft/Instrument) Safety Requirements and Compliance List (Formal delivery required) 14
3.2.3 Safety Variance 14
3.2.4 Preliminary Hazard Analysis 14
3.2.5 Project Integration and Test Safety Analysis 14
3.2.6 Safety Data Package (SDP) (Formal Delivery Required) 14
3.2.7 Hazardous Procedures for Payload I&T and Pre-launch Processing (Formal Delivery required) 15
3.2.8 Mishap Reporting and Investigation (Formal delivery required) 15
3.2.9 Orbital Debris Assessment Report (ODAR) and End of Mission Plan (EOMP) (Formal delivery required) 15
4 RISK ANALYSIS AND RELIABILITY 15
4.1 Reliability Program 15
4.2 Parts Stress Analysis 16
4.3 Limited Life Items 16
5 SOFTWARE ASSURANCE (FLIGHT AND GROUND SUPPORT SEGMENTS) 16
5.1 Software Assurance 16
6 GROUND SUPPORT EQUIPMENT (GSE) 16
6.1 PROTECTION of flight hardware 16
6.2 Lifting and Handling Equipment 17
7 WORKMANSHIP 17
7.1 General 17

7.2 Electrostatic Discharge Control (ESD) 18
8 EEE PARTS 18
8.1 General 18
8.2 Parts Control Board 18
8.3 EEE Parts Reporting 18
8.3.1 As-Built Parts List (ABPL) 19
8.4 Radiation 19
9 MATERIALS AND PROCESSES (M&P) 19
9.1 General 19
9.2 Life Test Plan and Reports for Lubricated Mechanisms 19
9.3 Materials Usage Agreement (MUA) 19
9.4 Materials Identification and Usage List (MIUL) 19
9.5 Printed Wiring Board Test Coupons 20
9.6 Lead-free and Tin Whisker Control 20
10 CONTAMINATION CONTROL 20
10.1 Contamination Control Plan 20
11 METROLOGY AND CALIBRATION 20
11.1 Metrology and Calibration Program 20
11.2 Use of Non-calibrated Instruments 20
12 GIDEP ALERTS AND PROBLEM ADVISORIES 20
12.1 Government-Industry Data Exchange Program (GIDEP) 20
12.2 Review 21
12.3 Actions 21
12.4 GIDEP Reporting 21
12.5 Reporting 21
13 DIGITAL ELECTRONICS 21
13.1 General 21
14 PLANETARY PROTECTION 21
15 CYBERSECURITY AND COMMAND LINK PROTECTION 22
16 END ITEM ACCEPTANCE DATA PACKAGE (EIDP) 22
APPENDIX A: SAFETY AND MISSION ASSURANCE RELATED DRDS 23
APPENDIX B: SAFETY AND MISSION ASSURANCE RELATED DRD DETAILS 28
APPENDIX C: MISSION ASSURANCE COMPLIANCE MATRIX 57
APPENDIX D: ISS PAYLOAD SUPPLEMENT 63
APPENDIX E: GOVERNMENT PROCUREMENT-RELATED REQUIREMENTS 68

PREAMBLE

The Science Mission Directorate (SMD), along with other organizations within the agency, has identified that opportunities to launch missions are limited by high costs and lengthy development times associated with spacecraft development under prescriptive requirements and high levels of process control and oversight. In particular, Class D (defined in NPR 8705.4 for missions required to follow NPR 7120.5), is now intended to cover those missions that may have very high scientific payoff, but rank lower in priority science according to references such as the Decadal Survey. In recent years, SMD has elected to make this class of missions cost-capped. This new, distinct Class D is largely characterized by developers using their own proven successful processes in their most cost-effective way, without detailed prescription and excessive approval barriers in development and where actions are taken mostly based on risk vs traditional requirements. The following Mission Assurance Requirements emphasize insight (NASA knowledge of development activities and team participation) as opposed to oversight (NASA approval and extensive process control of development activities), but they maintain sound risk management principles, which become more important when the levels of process control are reduced. This document ensures compliance to NASA requirements covering key areas in spacecraft development, while both authorizing and encouraging creative ways to achieve mission success and maintain overall safety. Since this document is intended to represent a single source to cover SMD's Class D risk posture, various application constraints, such as those that apply to cubesats, International Space Station (ISS) payloads, and larger smallsats will require discretion and explicit use of engineering judgment to identify areas that may not be practical or effective ways to buy down risk. Class D missions may encumber increased risk against mission success, but safety, including not harming host platforms and facilities, may not be compromised, and some requirements from host platforms, in launch or in space, may apply that are not addressed in this MAR. Accordingly, there is an expectation for the developer to apply the requirements to the specific mission attributes with an emphasis on prioritizing the highest risk areas for the mission.

1 GENERAL

This MAR is written to provide proposers the baseline Safety and Mission Assurance (SMA) scope and requirements for a Class D space flight mission implementation for the Science Mission Directorate (SMD) of the National Aeronautics and Space Administration (NASA). Upon selection, tailoring discussions for a specific project may be initiated. This document should be interpreted with practical thought for application and engineering judgment, and should emphasize teamwork between NASA and other organizations involved in the development. This document takes a different tact from past Program-level MARs typical in NASA, where in this case the emphasis is on implementing developer practices that have been proven successful, using teamwork between NASA and the developer to assure mission success, and driving efforts more based on characterization and management of risk than enforcement of broad, but prescriptive, requirements. This approach by no means encourages ignoring risks, but on the contrary emphasizes using rigorous understanding of risk to guide development and testing efforts. In this document, "NASA" refers to either the pertinent Program Office or the pertinent Project Office, located at a NASA Center or the Jet Propulsion Laboratory (JPL). The "Developer" refers to the organization that has Project Management responsibility for the mission or instrument. The Developer may be a NASA Center, JPL, or an outside institution. In

cases where the Developer is a NASA Center, or JPL, the Developer may employ their own local *command media* [1]on a case-by-case basis to those specified in the document. When NASA Centers, or JPL, are involved as partners, principal investigators, project managers, or support organizations to the Program Office, the pertinent Center/JPL with the highest level SMA authority in the project retains the Data Requirements Description deliverables and approves the tailoring to the document expressed in the MAR compliance matrix. With approval from NASA, the Developer may choose to combine deliverables with the required content. Appendix E provides procurement requirements that are used by government Program or Project Offices to manage flow down of higher level quality requirements into contracts associated with this Announcement.

1.1 SAFETY AND MISSION ASSURANCE PROGRAM

The Developer shall prepare, document, and implement a Mission Assurance Implementation Plan (MAIP) and MAR Compliance Matrix (Data Requirements Description (DRD) MA-1).
The mission assurance requirements compliance matrix shall accompany the MAIP submittal (MA-1) – identify variances along with supporting rationale for internal processes and procedures, as well as alternate standards that are proposed as alternatives to those specified. A sufficiently documented alternative process in the MAIP can take the place of a waiver/deviation. While the MAIP represents how the developer will meet the MAR Requirements using their internal documentation, it does not supersede those requirements.

1.2 MANAGEMENT

The Developer's SMA Manager shall have an independent reporting path to the NASA SMA technical authority (TA) and shall not be directly responsible for design or development efforts that could be viewed as a conflict of interest.

1.3 REPORTING

The Developer shall present status and information of the MAR deliverables and related activities at milestone reviews during monthly management reviews or equivalent, beginning with the System Requirements Review (SRR).

1.4 SURVEILLANCE

The Developer shall grant access for NASA and NASA assurance representatives to conduct an audit, assessment, or survey. The Developer shall supply documents, records, equipment, support personnel, and a work area within the Developer's facilities.

NASA has the right to specify Government Mandatory Inspection Points (GMIPs) or JPL Mandatory Inspection Points (JMIPs), as applicable. The Developer should provide documentation indicating both Project and subcontractor workflow to NASA with any planned inspection points to facilitate efficient assignment. GMIPs/JMIPs will be assigned as a result of an upfront negotiation based on (1) assessment of developer's own inspection points, (2) developer identified risks, (3) project identified risks; and furthermore, in response to events, such as failures, anomalies, and process shortfalls that prompt a need for further inspection.

1 Command media refers to written documentation that describes a process or standard for performing work that has been vetted through the organization.

NASA will coordinate the scheduling of any NASA-directed audits and inspections with the Developer (at Developer and Subcontractor facilities) to the greatest extent possible in order to maximize efficiency and minimize impact to schedule. NASA shall submit results of Audits and Assessments performed by NASA into the Agency's Supplier Assessment System (SAS).

1.5 REQUIREMENTS FLOW-DOWN

The Developer shall ensure flow down of SMA requirements to all suppliers based on the work to be performed and establish a process to verify compliance, with the exception of Inherited Items following the process in 1.8. The Developer's contract review and purchasing processes shall indicate the method for documenting, communicating and reviewing requirements with sub-tier suppliers to ensure requirements are met. The Developer shall ensure that quality plans, processes, procedures, hardware and software submitted by the Developer's sub-tier suppliers are compliant with the requirements in this MAR, as applicable.

1.6 SUSPENSION OF WORK ACTIVITIES

The Developer or any contractors performing supporting work shall direct the suspension of any work activity that indicates a present hazard, imminent danger or future hazard to personnel, property or mission operations resulting from unsafe acts or conditions that are identified by inspection, test or analysis.

1.7 SUSPICION OF FRAUD, WASTE, OR ABUSE

Any individual that suspects fraud, waste, or abuse are occurring shall report the concern to NASA's Office of the Inspector General, Acquisition Integrity Program at 202-358-2262.

1.8 SMA ACCEPTANCE OF INHERITED, BUILD-TO-PRINT, OR MODIFIED HERITAGE ITEMS

For products that have either been previously developed and exist (e.g., spares), or will be built-to-print (BTP) or are commercial-off-the-shelf (COTS), the Developer may follow an inherited items review process, in which NASA will perform an inheritance risk assessment on the selected Developer's heritage products, as an alternative to pursuing waivers to requirements in other sections of this MAR document. This process establishes a potential risk and consequence for using the item and may avoid routine waiver processing, based on the established prior history, the change in the design, environment, or operations, and the information provided about the processes used to develop the product. The risk determined shall be primarily based on prior usage, changes, and the approach to changes in standard products. Just as with waivers, NASA determines whether risks are acceptable or if mitigations are required. The developer shall assume ownership and responsibility for mitigation of any such risks. The risks that are determined from the inheritance risk assessment shall be brought in to the project risk board for disposition.

If the Developer elects to pursue this process in lieu of other requirements in this MAR to cover internal attributes of an inherited item, the developer should provide sufficient data from Table 1-1 and 1-2 to substantiate the item as a product that is at a level of risk commensurate with the Class D risk posture. After the first deliverable package, NASA has 30 days to review the package and provide a recommendation to the developer as to whether the risk is likely to be acceptable for each item based on the prior history combined with the availability of other options to provide the pertinent function. Table 1-1 is typically considered the minimum information set needed to characterize the risk of the current application of the item based on its

history, while additional information from Table 1-2 should be provided as available to further reduce the risk to NASA. The developer shall provide the initial Inherited Items package at 60 days after contract award and the final package at SRR + 60 days. Inherited components should demonstrate at least 50 hours of failure-free testing for each year of required operation on orbit to mitigate infant mortality concerns.

Use of this process does not alleviate the developer from meeting spacecraft/observatory technical functional or performance requirements.

Table 0-1. Inherited Items Data List

No.	Data Needed for Inherited Items
1	List of inherited items and statement of approach – rebuild, modification of previous build, or use of existing hardware
2	Summary results of qualification, acceptance, and/or prototype/protoflight testing completed, or comparison of current qualification/protoqual requirements and what was performed/realized on the inherited design, including environments, required design margins, and life
3	Flight history of the items and specific attributes for each flight, including environments (compare previous environment to current, including duty cycle and general concept of operations)
4	Ground and on-orbit anomaly and failure history including the determination of root causes or information that root cause was not determined. Ground anomalies may be restricted to major anomalies, where component performance requirements were violated
5	The reliability analyses performed for the most recent version of the product.
6	Identification of significant changes in manufacturing from qualified unit to current unit (facility, process, sub-tier supplier, testing changes, company change of ownership, etc.), and any changes in design or materials, including electronic parts, printed circuit boards, and standards used (changing from an older revision of a standard to the latest revision need not be discussed).
7	Deviations of each item from original design (white wires, cut traces, splices, etc., if not objectively clear to be part of the design) and reasons for each deviation. If the design has been qualified on a previous NASA project in the same environment and same risk posture, then the deviations may be declared relative to the previously qualified design.

Table 0-2. Inherited Items Supplementary Information

No.	Supplement Information for Inherited Items
1	Specifications and/or standards used to develop the items (e.g., IPC, J-STD, NASA requirements, including fastener integrity approach, or company standards). For items with minimal prior flight history, company standards or detailed synopses of such should be provided, if such are used to develop the product
2	Previous as-built parts list, including lot date codes, and the differences for new inherited item. This should include evidence that Government Industry Data Exchange Program (GIDEP) alerts and advisories have been properly

No.	Supplement Information for Inherited Items
	dispositioned, if the parts have already been procured. Note that GIDEP should always be used as an aid in procuring new parts or pulling parts from inventory. Reference to prior project deliveries to NASA is acceptable, in which case, an amendment may be delivered to indicate any changes
3	Known obsolete parts that are intended to be supplied out of existing inventory, along with quantity required vs available in inventory. Sparing plan if available (including quantity required, quantity available, and sparing philosophy)
4	Materials list and approved Material Usage Agreements (MUAs). Materials list includes lot date codes and evidence that GIDEP alerts and advisories have been properly dispositioned, if the materials have already been procured. Such evidence should be encompassed in GIDEP closure records for each of the items that have impacts. Reference to prior project deliveries to NASA is acceptable, in which case, an amendment may be delivered to indicate any changes
5	List of major electrical and mechanical analyses completed and summary of results.
6	Identification of any limitations on shelf life

2 QUALITY MANAGEMENT SYSTEM

2.1 GENERAL

The Developer shall have a Quality Management System that meets the intent of SAE AS9100 Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations, or ISO 9001 Quality Management Systems Requirements. This requirement may be limited to the developer or Subcontractor responsible for the design and development of the developer hardware and software. The developer shall grant access to their Quality Manual or equivalent means to meet the intent of AS9100 or ISO 9001 to NASA (DRL/DRL MA-2). The developer's quality system shall follow a consistent approach during the term of the contract. NASA reserves the right to audit the developer quality system at any time, but consistent with paragraph 1.4. This section is not meant to preclude the use of AS9100. As an alternative to the requirements in Section 2.1, the developer may follow AS9100D, sections 8.7 and 10.2 to address nonconforming product, failures and anomalies, and root cause and corrective action. In such case, the notification time frames in pertinent subsections below apply.

2.1.1 Quality Assurance

The Project Office shall establish a Quality Assurance (QA) Program that is sufficiently resourced throughout the life cycle. The Project Office shall provide objective evidence of QA Program maturity at life cycle reviews. The Project Office shall flow down product acceptance requirements as applicable. Configuration audits should be used as a prerequisite for product acceptance at the instrument and subsystem levels.

2.1.2 Control of Nonconforming Product

The Developer shall have a documented closed loop system for identifying, reporting, and correcting non-conformances. The system shall ensure that the adequacy of corrective action is determined by internal audit, inspection, or test, that objective evidence is collected, that preventive action is implemented to preclude recurrence; and that a Material Review Board is convened, as required.

2.1.3 Material Review Board (MRB)

The Developer shall have a documented process(es) for the establishment and operation of an MRB to process non-conformances. The Developer shall appoint a MRB chairperson who is responsible for implementing the MRB process and for appointing Developer representatives as MRB members. The MRB shall consist of a team that includes a Developer Safety and Mission Assurance representative and other appropriate personnel to ensure timely, accurate and appropriate determinations, implementation and close-out of MRB dispositions. For each reported nonconformance, the developer shall perform an investigation and engineering analysis sufficient to determine cause and corrective action that is commensurate with the criticality of the nonconformance if determined to be necessary by the Developer or by the NASA project office or program office. The MRB close out disposition shall include documented objective evidence of the verification of effective corrective actions.
The MRB operations shall be described in the Developer's Mission Assurance Implementation Plan.
The MRB shall process non-conformances using the following dispositions:

- Scrap — the product is not usable
- Re-work/Re-test — the product will be re-worked/re-tested to conform to requirements (sometimes referred to as "return to print")
- Return to supplier — the product will be returned to the supplier
- Repair — the product will be repaired using a repair process approved by the MRB to restore the item to acceptable use
- Use as is — the product will be used as is

Non-conformances submitted to the MRB and resulting in a disposition of "Use as is" or "Repair" shall be classified as follows:

- **Type I (Major):** Non-conformances in flight hardware that adversely affect safety, reliability, durability, performance, interchangeability, weight, or requirements of the contract or is the result of an unexplained anomaly. Specifically, Type I nonconformances affect form, fit, or function, or require changes to flight software or the concept of operations. Type I non-conformances shall require approval by the Developer MRB and notification to NASA within one week of identification.

- **Type II (Minor):** Non-conformances other than those specified in Type I. Type II non-conformances shall be approved by the Developer according to the Developer's non-conformance and MRB process and will not require immediate NASA reporting or approval.

The Developer shall provide meeting notice, technical data and an agenda to NASA with sufficient advance notice to permit NASA participation for Type I non-conformances MRB meetings.

The Developer shall provide NASA access to all non-conformances as requested and provide a summary list of all non-conformances as required in the Monthly Project Status Report.

The Developer shall provide NASA access to all Type II (minor) non-conformances for status and review of the non-conformance classification. A summary will be provided in the Monthly Project Status Report.

The Developer shall allow NASA to attend or participate via teleconference in Type II MRBs meetings/discussions at their discretion for the purposes of insight.
The Type I MRB process and documentation shall serve in lieu of a project waiver of nonconformance.

2.1.4 Reporting of Failures and Anomalies

The Developer shall have a documented process for reporting failures, including anomalies that occur on the ground during development, integration and test, during launch (payload failures and anomalies only), or on-orbit. An anomaly is defined as a deviation of system, subsystem, and/or hardware or software performance outside certified or approved design/performance specification limits. The Developer shall report to NASA hardware failures beginning with the first application of power at the box level (DRD MA-5) or mechanical actuation. The Developer shall document and report within 24 hours these hardware failures to NASA.

The Developer shall prepare an anomaly/failure report for any departure from design, performance, testing, or handling requirement that affects the function of flight equipment, or ground support equipment that interfaces with flight equipment, or that could compromise mission objectives, or alternatively, the Developer may document the failure or anomaly and corrective action in a problem reporting and corrective action system. The Developer shall perform a Failure Analysis on all parts/components that fail after the final assembly of flight components and subsystems has been started, if required by the anomaly/failure review team.
Review/disposition/approval of failure reports shall be described in the MAIP. NASA shall be notified of all Failure Review Boards and have the opportunity to attend. The documented failure reporting process shall provide the cause and suitability of corrective action for each failure during testing and ensure proper closure of all reported failures, either as part of the failure report or in another tracking system. The Developer shall provide access to all failure reporting records either by providing reports to NASA or by providing access to the problem reporting and corrective action system. The Developer shall maintain failure-reporting records of problems encountered at the lower levels of assembly for information. Failures that either cannot be duplicated, that have unknown root cause, cannot be verified, or have uncertainty in corrective action shall be analyzed for residual risk and consequence, declared as red flag problem failure records (PFRs).

3 SYSTEM SAFETY

3.1 GENERAL

The Developer shall document and implement a system safety program in accordance with NPR 8715.3, NASA General Safety Program Requirements, NPR 8715.7, Expendable Launch Vehicle

Payload Safety Program, launch service provider requirements, and launch range safety requirements.
The Developer shall participate in and support all required safety reviews.

3.1.1 Applicable Safety Requirements

- NPR 8715.7, Expendable Launch Vehicle Payload Safety Program
- NPR 8715.3, NASA General Safety Program Requirements (applicable sections only)
- LSP-REQ-317.01, Launch Services Program
  Program Level Poly Picosatellite Orbital Deployer (PPOD) and CubeSat Requirements Document (for cubesats being launched on PPODs by LSP)

Note: The Developer shall implement launch range safety requirements as applicable for the specific launch site. The most stringent applicable safety requirement shall take precedence in the event of conflicting requirements.

The following represent pertinent requirements documentation for common ranges used by NASA missions. Others may apply.

ELV Eastern Test Range (ETR) or Western Test Range (WTR) Missions

- NASA-STD 8719.24 (with Annex) NASA Expendable Launch Vehicle Payload Safety Requirements
- KNPR 8715.3, "KSC Safety Practices Procedural Requirements" (applicable at KSC property, KSC-controlled property, and offsite facility areas where KSC has operational responsibility)
- NPR 8715.7, "Expendable Launch Vehicle Payload Safety Program"
- Launch Site Facility-specific Safety Requirements, as applicable (e.g., Astrotech)

ISS Mission-related Safety Requirements Documentation

- SSP 51700 Payload Safety Policy and Requirements for the International Space
- NSTS/ISS18798 Interpretations of NSTS/ISS Payload Safety Requirements
- SSP 30599 ISS Safety Review Process

Payloads Processed at KSC

- KNPR 8715.3 KSC Safety Practices Procedural Requirements

Dragon

- SSP 57012 Dragon Interface Definition Document
- SSP 50835 Common Interface Requirements Document (Dragon)

HTV

- JSX-2008041B, "HTV Cargo Safety Review Process"
- JMR-002B, "Launch Vehicle Payload Safety Standard"
- JSX-2009059A, "HTV Cargo Safety Certification Process for Disposal"

Wallops Flight Facility (WFF) Missions

- NASA-STD 8719.24 (with Annex) NASA Expendable Launch Vehicle Payload Safety Requirements
- GSFC-STD-8009, "Range Safety Manual for GSFC/WFF"

Japanese Missions

- NASA-STD 8719.24 (with Annex) NASA Expendable Launch Vehicle Payload Safety Requirements, as negotiated with JAXA and NASA project or program office
- JMR 002, "Launch Vehicle Payload Safety Requirements"
- JERG-1-007, "Safety Regulations for Launch Site Operations/Flight Control Operations"
- KDP-99105, "Safety Guide for H-II/H-IIA Payload Launch Campaign"

European Missions

- NASA-STD 8719.24 (with Annex) NASA Expendable Launch Vehicle Payload Safety Requirements, as negotiated by each project with ESA and NASA project or program office
- ECSS-E-10A, "Space Engineering – System Engineering"
- ECSS-Q-40-02A, "Space Product Assurance – Hazard Analysis"
- ECSS-Q-40, "Space Product Assurance: Safety"
- CSG-RS-09A-CN, "Centre Spatial Guyanais (CSG) Safety Regulations Volumes and Parts List"
- CSG-RS-10A-CN, "Centre Spatial Guyanais (CSG) Safety Regulations Vol. I: General Rules"
- CSG-RS-21A-CN, "CSG Safety Regulations Vol. 2 Pt. 1: Specific Rules: Ground Installations"
- CSG-RS-22A-CN, "CSG Safety Regulations Vol. 2 Pt. 2: Specific Rules: Spacecraft"
- CSG-RS-33A-SE, "CSG Safety Regulations Vol. 3 Pt. 3: Substantiation and Data Sheets Concerning Payloads"
- CSG-SBU-16687, CNES, "Payload Safety Handbook"
- CNES/PN 2010 Operations of the Guiana Space Centre Facilities

Russian Missions

- P32928-103 Requirements for International Partner Cargoes Transported on Russian Progress and Soyuz Vehicles

3.2 SYSTEM SAFETY DELIVERABLES

3.2.1 System Safety Plan

The Developer shall implement a System Safety Program Plan (DRD MA-8). The System Safety Program Plan shall encompass all project contract activities. The System Safety Program Plan

content in NPR 8715.7, “Expendable Launch Vehicle Payload Safety Program” may be used as a guide.

3.2.2 Payload (Spacecraft/Instrument) Safety Requirements and Compliance List

The Developer shall prepare a Safety Requirements Compliance Checklist (DRD MA-6) to demonstrate that the project complies with NASA and range safety requirements.
Noncompliances to safety requirements will be documented in waivers and submitted for approval.
The Developer shall add to the Payload (Spacecraft/Instrument) Safety Requirements List a compliance status column to demonstrate the project complies with the tailored safety requirement. The Developer shall also include the status of the safety verifications in the project’s hazard reports.

3.2.3 Safety Variance

The Project shall submit Request for Safety Variance for waivers and non-conformances to the applicable safety requirements associated only with personnel or range safety, not those associated with mission success or programmatic risks (DRD MA-7).

3.2.4 Preliminary Hazard Analysis

The Developer shall document a Preliminary Hazard Analysis (PHA) (DRD MA-9). Based on the PHA, the following requirements apply:

- The Developer shall incorporate three independent inhibits in the design (dual fault tolerant) if a system failure may lead to a catastrophic hazard. A catastrophic hazard is defined as a condition that may cause death or a permanent disabling injury or the destruction of a major system or facility on the ground. An inhibit is a design feature (hardware or software) that prevents operation of a function.
- The Developer shall incorporate two independent inhibits in the design (single fault tolerant) if a system failure may lead to a critical hazard. A critical hazard is defined as a condition that may cause a severe injury or occupational illness to personnel or major property damage to facilities.
- The Developer shall adhere to specific detailed safety requirements, including compliance verification that must be met for design elements with hazards that cannot be controlled by failure tolerance. These design elements, e.g., structures and pressure vessels, are called "Design for Minimum Risk" areas.

3.2.5 Project Integration and Test Safety Analysis

The Developer shall perform sufficient safety analyses to evaluate activities for hazards introduced during project integration and testing at the Developer’s facility and to evaluate the adequacy of inhibit designs, and operational and support procedures used to eliminate, control, or mitigate hazards.

3.2.6 Safety Data Package (SDP)

A. For spacecraft development efforts: The Developer shall prepare a Safety Data Package (SDP)

B. For Instrument development efforts: The Developer shall prepare an Instrument Safety Assessment Report (ISAR) that will be an input to the spacecraft (SDP) as applicable. (DRD MA-11)

3.2.7 Hazardous Procedures for Payload I&T and Pre-launch Processing (Formal Delivery required)

The Developer shall prepare hazardous procedures that comply with applicable installation safety requirements for integration and test activities on the spacecraft and pre-launch activities at the launch site (DRD MA-12).

3.2.8 Mishap Reporting and Investigation

The Developer shall report mishaps, incidents, and close calls as defined in NPR 8621.1, NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping to NASA.

The Developer shall prepare and implement a Mishap Preparedness and Contingency Plan (DRD MA-13). This plan will be delivered as an appendix to the SMD MPCP that will be provided to the Developer by NASA.

The Developer may include the Mishap Preparedness and Contingency Plan deliverable in the System Safety Program Plan (DRD MA-8) in lieu of a separate deliverable as long as the preparation information contained in DRD MA-13 is included.

3.2.9 Orbital Debris Assessment Report (ODAR) and End of Mission Plan (EOMP) (Formal delivery required)

The Developer shall provide an ODAR and the EOMP per the content defined in NPR 8715.6/NASA-STD 8719.14, (DRD MA-27) unless the project is an International Space Station (ISS) project, in which case it is exempt from delivering these documents. The Developer shall comply with the pertinent requirements in NASA-STD-8719.14.

4 RISK ANALYSIS AND RELIABILITY

Risk Analysis and reliability activities should be tightly linked with the project's Risk Management processes. For example, risks that evolve from reliability analyses that affect overall mission objectives should be managed in the project's risk database. Likewise, safety risks (threats to personnel, the public, the environment, hosts, and facilities) should be maintained in the risk database when not eliminated or mitigated to noncredible likelihood levels.

4.1 RELIABILITY PROGRAM

At least 90 days prior to PDR, the Developer shall complete a reliability analysis, such as fault tree analysis or failure modes and effects analysis for faults that may result in injury to personnel or the public, producing orbital debris, or threaten assets on the ground that are not owned by the Developer. Likewise, the reliability analysis shall be used to implement means to prevent faults from propagating into host platforms, such as from instrument to spacecraft or to another external host platform. The results of these analyses should be linked to hazard and other safety analyses

in Section 3, in particular the inhibit requirements in section 3.2.4. Reliability analysis to establish acceptable risk to mission success is recommended, and may be performed per developer standard practices.

4.2 PARTS STRESS ANALYSIS

Parts stress and de-rating analyses for electrical, electronic, and electromechanical (EEE) parts and circuits shall be performed (DRD MA-15) in accordance with GSFC EEE-INST-002 Instruction for EEE Parts Selection, Screening, Qualification, and De-rating, JPL D-20348, or other standard developer practices for EEE parts. No formal submittal is required; however, NASA is to be provided access to requisite analyses.

4.3 LIMITED LIFE ITEMS

The developer shall document and implement a plan to identify and manage limited life items, with an emphasis on items with a shelf life, in cases of storage. Records shall be maintained for limited-life and presented at PDR, CDR, and PSR.

Limited Life items are generally defined as items subject to degradation or wear-out that have a limited shelf life, operational life, or cycle life whose life expectancy is less than 2x the required life to assess the risk and /or the mitigation plans for continued use of the item. Potential limited-life items include, but are not necessarily limited to: selected consumables; mechanisms; batteries; seals; thermal control surfaces; solar arrays; and, electromechanical mechanisms.

5 SOFTWARE ASSURANCE (FLIGHT AND GROUND SUPPORT SEGMENTS)

5.1 SOFTWARE ASSURANCE

The Developer shall perform software assurance activities that comply with applicable software assurance requirements in the NASA-STD-8739.8, NASA Standard for Software Assurance.

The Developer shall prepare and implement a Software Assurance Plan for software, which includes Government off-the-shelf software (GOTS), modified off-the-shelf software (MOTS), and commercial off-the-shelf software (COTS) (DRD MA-18).

The Developer may include the Software Assurance Plan deliverable in the Mission Assurance Implementation Plan (DRD MA-1) instead of a separate deliverable as long as the preparation information contained in DRD MA-18 is included.

The Developer shall provide advance notification of software reviews as scheduled and NASA retains the right to attend as an observer at any such representative reviews that present or assess software related matters at the various contract and sub-project levels.

6 GROUND SUPPORT EQUIPMENT (GSE)

6.1 PROTECTION OF FLIGHT HARDWARE

The Developer shall evaluate the potential for GSE to damage flight hardware by electrical or mechanical means, use appropriate means to prevent such damage from occurring, and present the approach at PDR and CDR.

6.2 LIFTING AND HANDLING EQUIPMENT

The developer shall include reference to command media or a detailed process to describe formal organizational lifting practices with an overview of successful lifting history in the System Safety Program Plan (DRL/DRD MA-7). The developer process is subject to NASA insight and verification for lifting and handling of sensitive flight hardware or critical ground support equipment (GSE). Developers that lack documented, successful lifting history shall follow NASA-STD-8719.9, Lifting Standard, for all lifting and handling of flight hardware or critical GSE.

7 WORKMANSHIP

7.1 GENERAL

The Developer shall implement a workmanship program to assure that electronic packaging technologies, processes, and workmanship meet mission objectives for quality and reliability. The following standards are recommended (but not required) and provided as guidance for implementing a workmanship program to assure that electronic packaging technologies, processes, and workmanship meet mission objectives.

- IPC- 610 Acceptability of Electronic Assemblies, or proven, comparable company practices
- J-STD-001X or J-STD-001XS or proven, comparable company practices, where X represents revision E or later
- NASA-STD-8739.1 Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies
- NASA-STD-8739.4 Crimping, Interconnecting Cables, Harnesses, and Wiring
- NASA-STD-8739.5 Fiber Optic Terminations, Cable Assemblies, and Installation
- IPC/WHMA-A-620B, Requirements and Acceptance for Cable and Wire Harness Assemblies
- IPC-2221 Generic Standard on Printed Board Design
- IPC-2222 Sectional Design Standard for Rigid Organic Printed Boards
- IPC-2223 Sectional Design Standard for Flexible Printed Boards
- IPC-2225 Sectional Design Standard for Organic Multichip Modules (MCM-L) and MCM-L Assemblies
- IPC A-600 Acceptability of Printed Boards (Class 3 requirements)
- IPC-6011 Generic Performance Specification for Printed Boards (Class 3 requirements)
- IPC-6012 Qualification and Performance Specification for Rigid Printed Boards (Class 3 requirements) or MIL-PRF-55110
- IPC-6013 Qualification and Performance Specification for Flexible Printed Boards (Class 3 requirements)
- IPC-6015 Qualification and Performance Specification for Organic Multichip Module (MCM-L) Mounting and Interconnecting Structures
- IPC-6018 Microwave End Product Board Inspection and Test (Class 3 requirements)

- GSFC-STD-6001 Ceramic Column Grid Array Design and Manufacturing Rules for Flight Hardware

7.2 ELECTROSTATIC DISCHARGE CONTROL (ESD)

The Developer shall implement an ESD Control Program that conforms to the requirements of ANSI/ESD S20.20-2007, Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices).

8 EEE PARTS

8.1 GENERAL

The Developer shall document and implement a Parts Control Plan (PCP) (DRD MA-19). Per NASA-STD-8739.10, Level 4, or Commercial-Off-The-Shelf (COTS) parts may be used without additional screening.

The Developer should address the following for part selection, screening and usage in the PCP when information is available:

1. Prior usage of the part and qualification for the specific application
2. Manufacturing variability with lots and from lot to lot for parts
3. Traceability and pedigree of parts
4. Reliability basis for parts.
5. Parts stress/application conditions

The PCP shall address counterfeit parts in accordance with SAE AS5553.

The Developer may include the Parts Control Plan deliverable in the Mission Assurance Implementation Plan (DRD MA-1) in lieu of a separate deliverable as long as the preparation information contained in DRD MA-19 is included.

8.2 PARTS CONTROL BOARD

The Developer shall establish a process for the planning, management, and coordination of the selection, application, and procurement requirements of EEE parts. This process shall be implemented through a Parts Control Board (PCB) or an equivalent body and shall be described in the Parts Control Plan (PCP) (DRD MA-19). When using the Inherited Items Process in Section 1.8, the PCB shall determine if any mitigating actions are required for approval based on the requirements stated in the PCP. Example concerns include the lack of internal parts list, derating analysis, use of Pb-free solder, etc. The recommended approach would be to have a member of the PCB as a participant in the pertinent inheritance risk assessment, from which associated risks and mitigations will be identified.

8.3 EEE PARTS REPORTING

The Developer shall provide NASA access to the EEE parts list (DRD MA-20) in lieu of a formal submittal.

The Developer shall have a regular teleconference with NASA to discuss EEE parts status, issues, risks and upcoming work.

8.3.1 As-Built Parts List (ABPL)

The Developer shall make available a list of EEE parts used in the flight hardware (DRD MA-21) and include the list in the Developer's EIDP (DRD SE-2).

8.4 RADIATION

Effects of radiation shall be mitigated either by the use of radiation-tolerant designs that are substantiated by analyses and testing as needed or by part-by-part, board-level, or box-level radiation hardness or radiation tolerance demonstrated by analysis or testing. Information shall be included in DRD MA-19.

9 MATERIALS AND PROCESSES (M&P)

9.1 GENERAL

The Developer shall prepare and implement a Materials and Processes (M&P) Selection, Control, and Implementation Plan (DRD MA-22) that is consistent with the mission requirements and risk posture. The Developer shall implement an M&P Control Board process or similar Developer process, which defines the planning, management, and coordination of the selection, application, procurement, control, and standardization of M&P for the contract and for directing the disposition of M&P problem resolutions.

The Developer shall implement and make available to NASA a Fastener Control Program that meets the requirements of NASA-STD-6008 (or equivalent proven developer practices that ensure that there is a rigorous process to procure aerospace-grade fasteners), NASA Fastener Procurement, Receiving Inspection, and Storage Practices for Spaceflight Hardware.

9.2 LIFE TEST PLAN AND REPORTS FOR LUBRICATED MECHANISMS

The Developer shall implement and make available to NASA a Life Test Plan for Lubricated Mechanisms (DRD MA-23). No formal submittal is required for the test reports. NASA is to be provided access to the test reports.

9.3 MATERIALS USAGE AGREEMENT (MUA)

The Developer shall prepare and have available to NASA Materials Usage Agreements for any M&P that do not comply with the requirements in the project M&P plan, but may still be acceptable in the actual hardware applications (DRD MA-24).

9.4 MATERIALS IDENTIFICATION AND USAGE LIST (MIUL)

The Developer shall prepare a Materials Identification and Usage List (DRD MA-25). No formal submittal is required. Government is to be provided access to the data.

The Developer shall also provide NASA access to the Developer-generated Program Approved Parts List (PAPL) (DRD-MA-25).

9.5 PRINTED WIRING BOARD TEST COUPONS

The Developer shall maintain either spare printed wiring boards or printed wiring board test coupons until mission disposal to be used only as needed for ground-based or on-orbit anomaly or failure resolution.

9.6 LEAD-FREE AND TIN WHISKER CONTROL

The Developer shall provide NASA access to a whisker mitigation plan or cite other applicable controls for solders and surface finishes that are less than 3% lead by weight for items that are not inherited or commercial-off-the-shelf (DRD MA-26). The following standards provide reference documentation for developing such a plan.

- GEIA –STD-0005-1: Performance Standard for Aerospace and High-Performance Electronics Systems Containing Lead-free Solder
- GEIA-STD-0005-2: Standard for Mitigating the Effects of Tin Whiskers in Aerospace and High Performance Electronic Systems, per Control Level 2
- ESA-STM-28: Guidelines for Creating a Lead-Free Control Plan

10 CONTAMINATION CONTROL

10.1 CONTAMINATION CONTROL PLAN

The Developer shall prepare and implement a contamination control program that meets the project requirements in accordance with DRD SE-1.

11 METROLOGY AND CALIBRATION

11.1 METROLOGY AND CALIBRATION PROGRAM

The Developer shall comply with one of the following ANSI/NCSL Z540.1, ISO 17025, ANSI/NCSL-Z540.3 for the calibration of measurement and test equipment. Products may be calibrated in accordance with Original Equipment Manufacturer (OEM) Calibration Standards, where evidence of traceability and documented test data shall be obtained from the OEM, in lieu of the aforementioned standards.

11.2 USE OF NON-CALIBRATED INSTRUMENTS

The Developer shall limit the use of non-calibrated instruments to applications where substantiated accuracy relative to a standard reference is not required and for indication-only purposes in non-hazardous, non-critical applications.

12 GIDEP ALERTS AND PROBLEM ADVISORIES

12.1 GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM (GIDEP)

The Developer may participate in GIDEP per the GIDEP Operations Manual located at http://www.gidep.org if desired. For Class D projects in institutions that are not GIDEP participants, the Developer may coordinate with NASA SMA for GIDEP content.

For inherited components accepted for approval through the inherited items process in Section 1.8 or for other commercial-off-the-shelf assemblies, the requirements in this section only apply to advisories related to the component or assembly as a whole.

12.2 REVIEW

The Developer shall review the following, hereafter referred to collectively as Alerts, for effects on the project: GIDEP Alerts; GIDEP SAFE-ALERTS; GIDEP Problem Advisories; GIDEP Agency Action Notices; NASA Advisories and component issues as distributed by NASA.

12.3 ACTIONS

The Developer shall take action to mitigate the effects of Alerts on the project when Alerts involve elevated risk.

12.4 GIDEP REPORTING

The developer shall prepare and submit (or support NASA SMA for preparation and submission of) failure experience data and safety issue reports per the requirements of S0300-BT-PRO-010 and S0300-BU-GYD-010 whenever failed or nonconforming items that are available to other buyers are discovered.

12.5 REPORTING

The Developer shall report the status of the GIDEP reviews on EEE parts and materials, list products used for the project that are affected by Alerts or by significant EEE parts, materials, and safety problems and any mitigations performed in Project Monthly Status Reports or at Milestone Reviews.

13 DIGITAL ELECTRONICS

13.1 GENERAL

The Developer shall document and implement an assurance plan for digital electronic components and designs that do not have flight heritage in a comparable space environment (DRD MA-28). EEE parts aspects of digital electronic parts are addressed in Section 8.

Covered digital electronic components are:

- Gate array technologies, including mask programmed gate arrays, field programmable gate arrays, custom ASICs, and the digital sections of mixed-signal ASICs
- And-Or plane devices, such as PALs and PLAs

The plan does not apply to software or firmware executed on processors or memory devices. The developer shall identify the person responsible for directing and managing the digital electronic components assurance program and interfacing with government assurance personnel.

14 PLANETARY PROTECTION

For missions outside of Earth orbit, the Developer shall take measures to address forward contamination (transmittal from Earth to a targeted Solar System body) and backward

contamination (transmittal to Earth from the targeted body) with respect to other Solar System bodies.

The following documents apply:

- NPD 8020.7G, *Biological Contamination Control for Outbound and Inbound Planetary Spacecraft*
- NID 8020.109, *Planetary Protection Provisions for Robotic Extraterrestrial Missions*
- NASA-HDBK-6022, *NASA Handbook for the Microbiological Examination of Space Hardware*

Note that forward contamination is of particular concern for Mars, Europa, Enceladus, and for possible liquid water bodies within other icy satellites. For additional information, Developers should contact the NASA Planetary Protection Officer, Dr. Lisa Pratt (Telephone: 202-358-4427; E-mail: lisa.m.pratt@nasa.gov) while the requirements are in development.

15 CYBERSECURITY AND COMMAND LINK PROTECTION

The Developer shall take measures to protect the integrity of on-board and ground control data systems based on risks present.
Spacecraft capable of maneuvering shall incorporate command link protection compliant with FIPS 140-2.
All command information shall be protected as SBU.

16 END ITEM ACCEPTANCE DATA PACKAGE (EIDP)

The Developer shall prepare and maintain a project EIDP until the mission is decommissioned. (DRD SE-16).

APPENDIX A: SAFETY AND MISSION ASSURANCE RELATED DRDS

No.	DOCUMENT	SUBMITTAL SCHEDULE	COMMENTS	INFORMATION (I), REVIEW (R), OR APPROVAL (A) (Program Office Determination)
MA-1	Mission Assurance Implementation Plan (MAIP)	30 days after contract award (DACA), Final Update as needed		
MA-2	Quality Manual	No formal submittal required; NASA provided access to Manual 60 DACA.		
MA-5	Reporting of Failures and Anomalies	48 hours after occurrence, Initial 2 weeks after determination of root cause, Closure Report		
MA-6	Payload (Spacecraft/Instrument) Safety Requirements & Compliance Checklist	45 days prior to CDR		
MA-7	Request for a Safety Variance	30 days after identifying variance need		
MA-8	System Safety Program Plan	30 days prior to SRR		
MA-9	Preliminary Hazard Analysis	30 days prior to PDR		

No.	DOCUMENT	SUBMITTAL SCHEDULE	COMMENTS	INFORMATION (I), REVIEW (R), OR APPROVAL (A) (Program Office Determination)
MA-11	Safety Data Package	30 days prior to PDR, Preliminary 30 days prior to CDR, Update 120 days prior to shipment, Final		
MA-12	Hazardous Procedures for Payload Integration and Test (I&T) and Pre-launch Processing	30 days prior to SIR or PSR		
MA-13	Mishap Preparedness and Contingency Plan	30 days prior to SRR		
MA-15	Parts Stress Analysis	No formal submittal required; Government provided access to the analysis. 45 days prior to CDR, Final 30 days after changes		
MA-18	Software Assurance Plan (Part of MA-1)	30 days prior to SRR 15 days prior to implementation, Update		
MA-19	EEE Parts Control Plan (PCP)	30 days prior to SRR 15 days prior to implementation, Update	Can be included in MAIP.	

No.	DOCUMENT	SUBMITTAL SCHEDULE	COMMENTS	INFORMATION (I), REVIEW (R), OR APPROVAL (A) (Program Office Determination)
MA-20	Monthly Parts Listed Submittal	No formal submittal required; Government provided access to the data. Monthly until no more changes are made; starting as soon as available, but no later than 6 months prior to PDR		
MA-21	As Built Parts List (ABPL)	30 days prior to SIR or PSR		
MA-22	Materials and Processes (M&P) Selection, Control, and Implementation Plan	30 days prior to SRR		
MA-23	Life Test Plan and Reports for Lubricated Mechanisms	Life Test Plan is required to be submitted. No formal submittal required for test reports; Government provided access to data. Plan: 30 days prior to SRR Reports: 30 days after mechanism acceptance test completion		

No.	DOCUMENT	SUBMITTAL SCHEDULE	COMMENTS	INFORMATION (I), REVIEW (R), OR APPROVAL (A) (Program Office Determination)
MA-24	Materials Usage Agreement (MUA)	30 days prior to CDR, All MUAs prepared to that date 30 days after identification, Update 15 days prior to SIR or PSR, Final		
MA-25	Materials Identification and Usage List (MIUL)	No formal submittal required; Government provided access to data. Program Approved Parts List: 30 days prior to PDR Quarterly after PDR until there are no more changes MIUL: 30 days prior to PDR 30 days prior to CDR 30 days after identification of changes		
MA-26	Lead-free and Tin whisker control plan	No formal submittal required; Government provided access to data 30 days prior to PDR		

No.	DOCUMENT	SUBMITTAL SCHEDULE	COMMENTS	INFORMATION (I), REVIEW (R), OR APPROVAL (A) (Program Office Determination)
MA-27	Orbital Debris Assessment Report (ODAR) and End of Mission Plan (EOMP)	1. Deliver preliminary ODAR inputs to the Project Office at MCR 2. Deliver ODAR interim inputs to the Project Office sixty (60) days prior to mission CDR for information. Deliver the final/updated ODAR and EOMP inputs to the Project Office 90 days prior to PSR for information.	ODAR and EOMP developed per NPR 8715.6/NASA-STD 8719.14	
SE-1	Contamination Control Plan	30 days prior to SRR, Initial 30 days prior to PDR, Preliminary 30 days prior to CDR, Final 3. Update, as needed		
SE-2	End Item Data Package	Final – 30 days prior to Project flight hardware delivery		

APPENDIX B: SAFETY AND MISSION ASSURANCE RELATED DRD DETAILS

MA-1 MISSION ASSURANCE IMPLEMENTATION PLAN AND MAR COMPLIANCE MATRIX

1. DRL/DRD No.:

MA-1

2. Title:

Mission Assurance Implementation Plan (MAIP) and MAR Compliance Matrix

3. Reference:

MAR 1.1

NPR 8735.2, Management of Government Quality Assurance Functions for NASA Contracts

Applicable:

NPR 8715.3, NASA General Safety and Program Requirements

NPR 8705.4, Risk Classification of NASA Payloads

NPD 8730.5 NASA Quality Assurance Program Policy

NASA-STD-8739.8, Software Assurance Standard

NPD 8720.1 NASA Reliability and Maintainability Policy

4. Use:

Documents the Project's plan for implementing a system safety and mission assurance program consistent with Project's Quality Management System, contract Statement of Work, and the Mission Assurance Requirements (MAR). Documents the compliance to this MAR document.

5. Preparation Information:

The MAIP scope shall cover:

(A) The planning, execution, monitoring and control of reliability, quality assurance, workmanship, safety, parts and materials, software development, contamination control, non-conforming material, and failure investigation and reporting.

(B) All phases of the Project's efforts, including, but not limited to, requirements definition and verification, design and development, procurement, manufacturing and fabrication, assembly, and integration and test. This may include in special cases, payload processing in preparation for launch, ground systems, and mission operations assurance.

(C) All flight hardware and software that is designed, built, developed or provided by the Project and its subcontractors or furnished by NASA, from project initiation through launch and mission operations.

(D) All ground support equipment (GSE), including software that interfaces with flight equipment to the extent necessary to assure the integrity and safety of flight items. Parts and materials selection are excepted for GSE, provided safety is not impacted and the deliverable flight item contamination requirements are not compromised.

The MAIP shall include reference to the Project's internal procedure for each Product Assurance function/element and deliverable and have brief description of the respective procedure. The MAIP shall include a more detailed description for the following areas as a minimum:

(A) Material Review Board

(B) Reliability Program

(C) EEE Parts Control Board (if not included in a separate EEE Parts Plans)
(D) Software Assurance Plan (if no separate SA Plan is delivered)
(E) EEE Parts Plan (If no separate EEE Parts Plan is delivered)

The MAR Compliance matrix shall specify which requirements will be met, per the structure in Appendix C.

MA-2 Quality manual

1. DRL/DRD No.:

MA-2

2. Title:

Quality Manual

3. Reference:

MAR 2.1

ISO 10013 Quality Manual Development Guide

Applicable:

SAE AS9100 Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations

4. Use:

Documents the developer's quality management system

Preparation Information:

Prepare a Quality Manual addressing applicable requirements of AS9100; refer to ISO 10013 Quality Manual Development Guide for guidelines on preparation of a quality manual. Acceptable to use an equivalent means to demonstrate meeting intent of AS9100.

MA-5 REPORTING OF FAILURES AND ANOMALIES

1. DRL/DRD No.:

MA-5

2. Title:

Reporting of Failures and Anomalies

3. Reference:

MAR 2.1.3

Applicable:

SAE AS9100, Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations

4. Use:

Document failures, anomalies, investigative activities, rationale for closure, and corrective and preventive actions.

5. Preparation Information:

Documents failures, anomalies, changes in status, or purposed closure to identify the following information:

(A) Identification of project, system, or sub-system;

(B) Identification of failed item (e.g., assemble, sub-assembly, or part);

(C) Description of item;

(D) Identification of next higher assembly;

(E) Description of anomaly, including activities leading up to anomaly, if known;

(F) Names and contact information of individuals involved in anomaly;

(G) Date and time of anomaly;

(H) Status of item;

(I) Contact information for personnel who originated the report;

(J) Date of original submission;

(K) Anomaly cause;

(L) Corrective actions implemented;

(M) Retesting performed and results;

(N) Other items affected; and

(O) Risk ratings-mission impact and certainty in corrective actions.

MA-6 TAILORED PAYLOAD (SPACECRAFT/INSTRUMENT) SAFETY REQUIREMENTS & COMPLIANCE CHECKLIST

1. DRL/DRD No.:

MA-6

2. Title:

Tailored Payload (Spacecraft/Instrument) Safety Requirements & Compliance Checklist

3. Reference:

MAR 3.2.2

Applicable:

NASA-STD-8719.24

NPR 8715.3, NASA General Safety Requirements

4. Use:

The overall intent of the ELV payload safety requirements tailoring process and compliance checklist is to ensure appropriate inclusion of applicable Range Safety requirements into the Project safety tasks, and compliance status of those requirements. Tailoring is defined as the process of assessing the applicability of safety requirements within NASA-STD-8719.24 for a space flight project and evaluating the project's potential implementation in order to generate a set of specific safety requirements for the contract.

5. Preparation Information:

Tailored Payload Safety Requirements shall:

a. Document all safety requirements that apply to a payload mission.

b. In the event of conflicting requirements, incorporate the more stringent.

c. Document the applicability of safety requirements to specific situations within a mission.

d. Document the interpretation of requirements as needed.

e. Address any recommendations, interpretations, or resolutions of safety concerns provided by the Project Team and each authority involved in the mission.

f. Identify any change to a requirement (i.e., any addition or deletion from the source requirement) and include sufficient rationale for the tailored change.

g. Identify potential areas of noncompliance with applicable requirements.

h. Reference any waivers identified during the tailoring

The compliance checklist indicates for each requirement whether the proposed design is compliant, non-compliant but meets intent, non-compliant, or if the requirement is not applicable. An indication other than compliant shall include rationale.

The compliance checklist shall include all design, test, analysis, and data submittal requirements required to support the Safety Data Package (DRD MA-11). The checklist shall include:

1. Criteria and requirement;
2. System;
3. Indication of compliance, non-compliance, or not applicable;
4. Resolution;
5. Reference;
6. Copies of all Range Safety approved non-compliances, including waivers and equivalent levels of safety certifications.

MA-7 REQUEST FOR SAFETY VARIANCE

1. DRL/DRD No.:

   MA-7

2. Title:

   Request for a Safety Variance

3. Reference:

   MAR 3.2.3

   Applicable:

   NASA-STD-8719.24, Range Safety User Requirements

   NPR 8715.3, NASA General Safety Program Requirements

4. Use:

   A Safety Waiver documents a safety requirement that cannot be met and the rationale for approval of a waiver, as defined in NPR 8715.7.

5. Preparation Information:

   Information from the review of a waiver request shall include:

   (A) A statement of the specific safety requirement and its associated source document name and paragraph number for which a waiver is requested.

   (B) A technical justification for the waiver.

   (C) Analyses to show the mishap potential of the proposed alternate requirement, method, or process as evaluated against the specified requirement.

   (D) An assessment of the risk involved in accepting the waiver; when it is determined that there are no hazards, the basis for such determination should be provided.

   (E) A narrative on possible ways of reducing hazards severity and probability and existing compliance activities.

   (F) Starting and expiration for waiver, if applicable.

   Note: a waiver may require Range Safety concurrence.

MA-8 SYSTEM SAFETY PROGRAM PLAN

1. DRL/DRD No.:

   MA-8

2. Title:

   System Safety Program Plan

3. Reference:

   MAR 3.2.1
   NPR 8715.7, Expendable Launch Vehicle Payload Safety Program

   Applicable:

   NPR 8715.3, NASA General Safety Program Requirements
   NASA-STD-8719.24, "Range Safety User Requirements"

4. Use:

   The System Safety Program Plan (SSPP) describes the tasks and activities of system safety management and engineering required to identify, evaluate, and eliminate or control hazards to the hardware, software, and system design by reducing the associated risk to an acceptable level throughout the system life cycle, including launch range safety requirements.

5. Preparation Information:

   The SSPP shall describe the system safety program utilizing the content contained in NPR 8715.7, "Expendable Launch Vehicle Payload Safety Program."

   The SSPP shall:

   (A) Define the roles and responsibilities of personnel

   (B) Define required documents, applicable documents, and completion schedules for analyses, reviews, and safety packages.

   (C) Address support for Reviews, Safety Working Group Meetings, and Technical Interchange Meetings (TIMs).

   (D) Provide for early identification and control hazards to personnel, facilities, support equipment, and the flight system during product development, including design, fabrication, test, transportation, and ground activities.

   (E) Address compliance with the launch range safety requirements.

   (F) Include Safety review process that meets the intent of NPR 8715.7.

   (G) Address compliance with industrial safety requirements imposed by NASA and Occupational Safety and Health Administration (OSHA) design and operational needs and contractually imposed mission unique obligations.

   (H) Address software safety to identify and mitigate safety-critical software products by the following:

(i) Identification of software related hazards;

(ii) Identification of hazard controls that are implemented with software;

(iii) Identification and tracking of software safety requirements;

(iv) Verification results and approved waivers and expectations for software safety requirements; and

(v) Verification of safety discrepancy disposition approvals.

MA-9 PRELIMINARY HAZARD ANALYSIS

1. DRL/DRD No.:

MA-9

2. Title:

Preliminary Hazard Analysis

3. Reference:

MAR 3.2.4
MIL-STD-882, Standard Practice for System Safety

Applicable:

NASA-STD-8719.24, "Range Safety User Requirements"
NPR 8715.3, NASA General Safety Program Requirements

4. Use:

The Preliminary Hazard Analysis (PHA) is used to obtain an initial risk assessment and identify safety critical areas of concept system. It is based on the best available data, including mishap data from similar systems and other lessons learned. The PHA is used to evaluate hazards associated with the proposed design or function for seventy, probability, and operational constraints. The PHA is also used to identify safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to an acceptable level.

5. Preparation Information:

The PHA shall identify safety critical areas, provide an initial assessment of hazards, and identify requisite hazard controls and follow-on actions. The PHA results provide guidance for the tailoring of NASA-STD-8719.24 and the SDP deliverable. The PHA shall incorporate on the best available data, including mishap data from similar systems and other lessons learned, The PHA shall include evaluations of the hazards associated with the proposed design or function for hazards severity, hazard probability, and operational constraint. The PHA shall include safety studies identifying provisions and alternatives needed to eliminate hazards or reduce their associated risk to an acceptable level. At a minimum the PHA shall include the following, as applicable:

(A) Hazardous components such as fuels, propellants, lasers, explosives, toxic substances, hazardous construction materials, pressure systems, and other energy sources.

(B) Safety related interface considerations among various elements of the system such as material compatibility, electromagnetic interference, inadvertent activation, fire and explosive initiation and propagation, and hardware and software controls. This shall include consideration of the potential contribution by software, including software developed by other Projects and sources, to subsystem and system mishaps.

(C) Identification of safety design criteria to control safety-critical software commands

and responses such as inadvertent command, failure to command, untimely command or responses, inappropriate magnitude, or designated undesired events and appropriate action taken to incorporate them in the software and related hardware specifications.

(D) Environmental constraints including the operating environments such as drop, shock, vibration, extreme temperatures, humidity, noise, exposure to toxic substances, health hazards, fire, electrostatic discharge, lightning, electromagnetic environmental effects, ionizing and non-ionizing radiation including laser radiation.

(E) Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures (human factors engineering, human error analysis of operator functions, tasks, and requirements; effect of factors such as equipment layout, lighting requirements, potential exposures to toxic materials, effects of noise or radiation on human performance; explosive ordnance render safe and emergency disposal procedures; life support requirements and their safety implications in manned systems, crash safety, egress, rescue, survival, and salvage).

(F) Those test unique hazards that will be a direct result of the test and evaluation of the article or vehicle.

(G) Facilities, real property installed equipment, support equipment such as provisions for storage, assembly, checkout, proof testing of hazardous systems and assemblies that may involve toxic, flammable, explosive, corrosive, or cryogenic materials and wastes; radiation or noise emitters; and electrical power sources.

(H) Training and certification pertaining to hazardous and safety critical operations and maintenance of hazardous and safety critical systems.

(I) Safety related equipment, safeguards, and possible alternate approaches such as interlocks; system redundancy; fail-safe design considerations using hardware or software controls; subsystem protection; fire detection and suppression systems; personal protective equipment; heating, ventilation, and air-conditioning; and noise or radiation barriers.

(J) Specify each malfunction to the system, subsystems, or software, the cause and resulting sequence of events determined, and the degree of hazard.

(K) Identify Government Mandatory Inspections Points (GMIP) for all safety critical attributes that support hazard control/mitigation verifications.

MA-11 SAFETY DATA PACKAGE

1. DRL/DRD No.:

   MA-11

2. Title:

   Safety Data Package

3. Reference:

   MAR 3.2.6

   Applicable:

   NASA-STD-8719.24

4. Use:

   The Safety Data Package (SDP) documents the comprehensive evaluations of hazards and the risk being assumed prior to the testing or operations of the payload. The spacecraft Project will use the SDP as an input to the Missile System Pre-launch Safety Package (MSPSP) or equivalent Range Safety document. The verification portion of the SDP provides documentation of Hazard Control Verification status at time of payload delivery.

5. Preparation Information:

   The Safety Data Package will identify hardware, and software related hazards that may be present in the payload and operations and the safety feature, hazard controls and inhibits to control the identified hazards. This includes specific procedural controls and precautions.

   The Safety Package will include the following information:

   (A) The safety criteria and methodology used to classify and rank hazards, including assumptions upon which the criteria or methodologies were based or derived, to include the definition of acceptable risk as specified by Range Safety

   The Safety Data Package delivered shall contain:

   (A) Hazard Analysis Summaries, Hazard Reports, and safeguards and mitigation strategies pertaining to the following:

      (i) Flight payload;

      (ii) Critical payload Ground Support Equipment, including software;

      (iii) Payload Lifting Hardware;

      (iv) Payload and Ground Support Equipment Hazardous Materials and Processes;

      (v) Hazards to the Observatory, resulting from presence of payload; and

      (vi) Personnel.

   (B) Utilization of an Operations/Operations and Support Hazard Analysis to identify and document payload-related hazardous or safety-critical operations that are or may potentially be used during the following:

(i) Payload fabrication and testing;

(ii) Observatory integration and testing;

(iii) Launch site operations; and

(iv) On-orbit operations.

(C) The plan shall include the results of the Software Safety Analysis

(D) The results of hazard analyses and tests used to identify hazards in the system including those hazards that still have a residual risk, actions that have been taken to reduce the associated risk to a level contractually specified as acceptable, results of tests conducted to validate safety criteria, requirements, and analyses of any hazardous materials generated by or used in the system

(E) Recommendations applicable to hazards at the interface of Range User systems with other systems, as required.

(F) Identification of the hazardous operations and procedures.

The final submission of the SDP shall contain hazard verification information. The verification information shall provide documentation that demonstrates the process of verifying the control of all hazards by test, analysis, inspection, similarity to previously qualified hardware, or any combination of these activities. All verifications that are listed on the hazard reports shall reference the tests/analyses/inspections. The Project shall submit results of these tests/analyses/inspections for review in accordance with the contract schedule and applicable launch site range safety requirements. The Verification Tracking Log (VTL) shall contain the following information in tabular format:

(A) Hazard Report Number.

(B) Safety Verification Number.

(C) Description (Identify procedures/analyses by number and title).

(D) Constraints on Launch Site Operations.

(E) Independent Verification Required (e.g., mandatory inspection points).

(F) Scheduled Completion Date.

(G) Completion Date.

(H) Method of Closure

MA-12 HAZARDOUS PROCEDURES FOR PAYLOAD INTEGRATION AND TEST (I&T) AND PRE-LAUNCH PROCESSING

1. DRL/DRD No.:

MA-12

2. Title:

Hazardous Procedures for Payload Integration and Test (I&T) and Pre-launch Processing

3. Reference:

MAR 3.2.7

Applicable:

NPR 8715.3, NASA General Safety and Program Requirements

NASA-STD-8719.24, "Range Safety User Requirements"

4. Use:

Documents hazardous procedures and associated safeguards that the Project will use for launch vehicle payload integration and test activities and pre-launch activities that comply with the applicable safety requirements of the installations where the activities are performed.

5. Preparation Information:

Operational Procedures for hazardous systems shall include provisions for the hazard controls, and verifications identified in the Safety Data Package (SDP). The following list is to be considered when determining if hazardous procedures need to be developed. The list is typical of space flight hazardous systems, but is not all inclusive:

(A) Pressurized propellant systems - pressurization (pneumatic and hydrostatic), loading and unloading, sampling, leak testing, venting.

(B) Launch vehicle and payload systems - pressurization, loading and unloading, leak test, erection and lifting with ordnance and/or propellant, application of power with ordnance and/or propellant, safe and arm pin removal, mate and de-mate operation.

(C) Hazardous facilities - high pressure systems, propellant flows in ground systems, propellant cart loading, ordnance checkout and installation, X-ray operations, cryogenic operations, fixture proof tests, emergency blackout procedures.

(D) Ordnance - bore scope, X-ray, continuity test, propellant trimming, installation, electrical connection and disconnection.

(E) Work involving lasers, high energy RF emissions, radioactive materials, and hazardous materials.

(F) Date of original submission;

(G) Anomaly cause;

(H) Corrective actions implemented;

(I) Retesting performed and results;

(J) Other items affected; and Risk ratings—mission impact and certainty in corrective actions

MA-13 MISHAP PREPAREDNESS AND CONTINGENCY PLAN

1. DRL/DRD No.:

   MA-13

2. Title:

   Mishap Preparedness and Contingency Plan

3. Reference:

   MAR 3.2.8

   Applicable:

   NPR 8621.1, NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping

4. Use:

   Ensure NASA requirements for mishap reporting are met.

5. Preparation Information:

   The Mishap Preparedness and Contingency Plan shall address all applicable requirements of NPR 8621.1 and include a call list.

MA-15 PARTS STRESS ANALYSIS

1. DRL/DRD No.:

   MA-15

2. Title:

   Parts Stress Analysis

3. Reference:

   MAR 4.5

   Applicable:

   GSFC EEE-INST-002 http://nepp.nasa.gov/DocUploads/FFB52B88-36AE-4378-A05B2C084B5EE2CC/EEE-INST-002_add1.pdf

   JPL D-20348 https://nepp.nasa.gov/DocUploads/8DB633E8-7AA9-4A1C.../JPL-D-20348.doc

   NASA Parts Selection List <http://nepp.nasa.gov/npsl/index.htm>

4. Use:

   Provides EEE Parts stress analyses for verifying circuit design conformance to de-rating requirements, demonstrates that environmental operational stresses on parts comply with project de-rating requirements

5. Preparation Information:

   The Parts Stress Analysis shall contain:

   (A) Analysis ground rules

   (B) Reference documents and data used

   (C) Results and conclusions

   (D) Design trade study results

   (E) Parts stress analysis results impacting design or risk decisions

   (F) Analysis worksheets; the worksheets at a minimum shall include:

      (i) Part identification (traceable to circuit diagrams)

      (ii) Assumes environmental (consider all expected environments)

      (iii) Rated stress

      (iv) Applied stress (consider all significant operating parameter stresses at the extremes of anticipated environments)

      (v) Ratio of applied-to-rated stress

MA-18 SOFTWARE ASSURANCE PLAN

1. DRL/DRD No.:

   MA-18

2. Title:

   Software Assurance Plan

3. Reference:

   MAR 5.2
   Institute of Electrical and Electronics Engineers (IEEE) Standard 730-2002, Software Quality Assurance Plans

   Applicable:
   NASA-STD-8739.8, NASA Standard for Software Assurance

4. Use:

   Documents the Project's Software and Complex Electronics Assurance roles and responsibilities, surveillance activities, supplier controls, recorded collection, maintenance and retention, training and risk management.

5. Preparation Information:

   The Software Assurance Plan shall contain the following:

   (A) Purpose:
   (B) Reference documents and definitions;
   (C) Management;
   (D) Documentation;
   (E) Standards, practices, conventions, and metrics;
   (F) Software Reviews;
   (G) Test;
   (H) Problem Reporting and Corrective Action;
   (I) Tools, techniques, and methodologies;
   (J) Media control;
   (K) Supplier control;

(L) Records, collection, maintenance, and retention;

(M) Training;

(N) Risk Management; and

(O) SQAP Change procedure and history.

MA-19 EEE PARTS CONTROL PLAN (PCP)

1. DRL/DRD No.:

MA-19

2. Title:

EEE Parts Control Plan (PCP)

3. Reference:

MAR 8.1
S-311-M-70 Specification for Destructive Physical Analysis

GSFC EEE-INST-002 Instructions for EEE Parts Selection, Screening, Qualification, and De-rating
SAE AS5553 Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition

4. Use:

Development and implementation of an EEE Parts Control Plan that addresses the system requirements for mission lifetime and reliability

5. Preparation Information:

The PCP shall address the following:

(A) Parts control process, including Parts Control Board (PCB) charter, roles, and responsibilities as applicable (includes meeting schedule, notices, distribution of data and agenda, review and approval process)

(B) Shelf life control

(C) Parts application de-rating

(D) Supplier and manufacturer surveillance

(E) Qualification

(F) ASICs, Gate Arrays, System-on-chip, Custom ICs

(G) Incoming inspection and test

(H) Destructive Physical Analysis

(I) Defective parts controls program

(J) Radiation hardness assurance

(K) Handling, preservation, and packing

(L) Contamination control

(M) Alternate quality conformance inspection and small lot sampling

(N) Traceability and lot control

(O) Failure analysis

(P) Counterfeit parts control plan per AS5553

(Q) Can be included in the MAIP

MA-21 AS BUILT PARTS LIST (ABPL)

1. DRL/DRD No.:

   MA-21

2. Title:

   As Built Parts List (ABPL)

3. Reference:

   MAR 8.4.1

4. Use:

   A final list of EEE parts that are used in the flight hardware

5. Preparation Information:

   The As Built Parts List (ABPL): shall contain all the fields/data included in the Monthly Parts List submittal (DRD MA-20) plus the following minimum information:

   (A) Assembly Name/name & Assembly serial number

   (B) Item revision

   (C) Next Level of Assembly & Next Level of Assembly serial number

   (D) Lot/Date/Batch/Heat/Manufacturing Code, as applicable

   (E) Manufacturer's CAGE Code (specific plant location preferred)

   (F) Distributor/supplier, if applicable

   (G) Part number

   (H) Part serial number (if applicable)

MA-22 MATERIAL AND PROCESSES (M&P) SELECTION, CONTROL, AND IMPLEMENTATION PLAN

1. DRL/DRD No.:

   MA-22

2. Title:

   Material and Processes (M&P) Selection, Control, and Implementation Plan

3. Reference:

   MAR 9.1

   NASA-Technical Memorandum (TM)-86556, Lubrication Handbook for the Space Industry (Part A: Solid Lubricants, Part B: Liquid Lubricants)

   NASA/Project Report (CR)-2005-213424, Lubrication for Space Applications

   NASA-STD-6016, Standard Materials and Processes Requirement for Spacecraft

4. Use:

   Defines the implementations of NASA-STD-6016 or vendor-proven practices with prescribed changes as described in the Preparation Information

5. Preparation Information:

   The Materials and Processes (M&P) Selection, Control, and Implementation Plan shall address the following

   (A) Materials and Processes Control process, including Materials and Processes Control Board charter, roles, and responsibilities, as applicable (or similar proposed Project process).

   (B) Organizational authority and responsibility for review and approval of M&P specified prior to release of engineering documentation.

   (C) Identification, tracking, and documentation of Materials and Processes

   (D) Conformance to the requirements of NASA-STD-6016 or the vendor command media and identification of process specifications used to implement requirements in the M&P Plan

   (E) Procedures and data documentation for proposed test programs to support materials screening and verification testing

   (F) Details of the Project's Fastener Control Program (if not included in the MAIP (DRD MA-1) Next Level of Assembly & Next Level of Assembly serial number

MA-24 MATERIALS USAGE AGREEMENT (MUA)

1. DRL/DRD No.:

   MA-24

2. Title:

   Material Usage Agreement (MUA)

3. Reference:

   MAR 9.3

   NASA-STD-6016, Standard Materials and Processes Requirement for Spacecraft

MSFC-STD-3029, Guidelines for the Selection of Metallic Materials for Stress Corrosion Cracking Resistance in Sodium Chloride Environments

Materials and Processes Technical Information System (MAPTIS) - MAPTIS is accessible via the Internet at http://maptis.nasa.gov

4. Use:

   Establishes the process for submitting an MUA for material or process that does not meet the requirements of NASA-STD-6016 (or Government approved equivalent) and does not affect reliability or safety when used per the Materials and Processes Selection, Control, and Implementation Plan.

5. Preparation Information:

   The MUA package shall include the technical information required by the Related Documents listed above to justify the application. MUAs for stress corrosion shall include a Stress Corrosion Cracking Evaluation Form per MSFC-STD-3029 and a stress analysis. (see NASA-STD-6016). The MUA shall include the results of acceptance testing on selected sample lots of procedure materials per approved procedure.

MA-25 MATERIALS IDENTIFICATION AND USAGE LIST (MIUL)

1. DRL/DRD No.:

   MA-25

2. Title:

   Material Identification and Usage List (MIUL)

3. Reference:

MAR 9.4

NASA-STD-6016, Standard Materials and Processes Requirement for Spacecraft

4. Use:

Establishes the Materials Identification and Usage List (MIUL) including Material Selection List for Metals, Fasteners, Plastic Films, Foams, and Adhesive Tapes submitted to Launch Range Safety for assessment of flammability.

5. Preparation Information:

The Project shall deliver the MIUL in a MAPTIS compatible form. The MIUL shall identify the following information as applicable to the material process:

(A) Material form;

(B) Material manufacturer and manufacturer's designation;

(C) Material specification;

(D) Process specification;

(E) Environment;

(F) Weight;

(G) MAPTIS Material code (if data are to be provided in a form compatible with MAPTIS);

(H) Standard/commercial part number;

(I) System and subsystem;

(J) Maximum and minimum temperature (required based on requests by NASA);

(K) Fluid type;

(L) Surface Area and thickness;

(M) Project;

(N) Cure schedule; and

(O) GIDEP Alert Information

(P) Detailed drawing and dash number

(Q) Next Assembly and dash number

(R) Change letter designation

(S) Drawing source

(T) Project (supplier)

(U) Overall evaluation

(V) Overall Configuration Test

(W) MUA # or rationale

(X) Materials rating

MA-26 LEAD-FREE AND WHISKER CONTROL PLAN

1. DRL/DRD No.:

   MA-26

2. Title:

   Lead-free and whisker control plan

3. Reference:

   MAR 9.6

   - GEIA–STD-0005-1: Performance Standard for Aerospace and High-Performance Electronics Systems Containing Lead-free Solder
   - GEIA-STD-0005-2: Standard for Mitigating the Effects of Tin Whiskers in Aerospace and High Performance Electronic Systems, per Control Level 2
   - ESA-STM-28: Guidelines for Creating a Lead-Free Control Plan

4. Use:

   Provides a plan to prevent whisker formation when solder containing less than 3% lead by weight is used (non-inherited products).

5. Preparation Information:

   The reference standards above may be used to form a plan. Plan is made available to the government, not formally delivered.

MA-27 ORBITAL DEBRIS ASSESSMENT REPORT (ODAR) AND END OF MISSION PLAN (EOMP)

1. DRL/DRD No.:

MA-27

2. Title:

Orbital Debris Assessment Report (ODAR) and End of Mission Plan (EOMP)

3. Reference:

MAR 3.2.9

Applicable:
NPR 8715.6A NASA Procedural Requirements for Limiting Orbital Debris
NASA-STD-8719.14 Process for Limiting Orbital Debris

4. Use:

Ensure NASA requirements for post mission orbital debris control are met.

5. Preparation Information:

(A) The assessment shall be done in accordance with NPR 8715.6 NASA Procedural Requirements for Limiting Orbital Debris and NASA-STD-8719.14 Process for Limiting Orbital Debris.
(B) The preliminary assessment is conducted to identify areas where the project may contribute debris and to assess this contribution relative to the guidelines.
(C) The final assessment is conducted shall include comments on changes made since the preliminary assessment.
(D) The detail should be consistent with the available information of design and operations.
(E) The developer shall submit updates to the final assessment for design changes after CDR that impact the potential for debris generation.
(F) The End of Mission Plan will be developed per NPR 8715.6/NASA-STD 8719.14.
NOTE: Orbital Debris Assessment Software is available for download from Johnson Space Center at URL: http://sn-callisto.jsc.nasa.gov/mitigate/das/das.html.

MA-28 DIGITAL ELECTRONICS ASSURANCE PLAN

1. DRL/DRD No.:

MA-28

2. Title:

Digital Electronics Assurance Plan

3. Reference:

MAR 13.1

4. Use:

To outline the plan for assuring the integrity of digital electronics design and implementation

5. Preparation Information:

The plan should address: parts selection; version control; timing verification; routing analysis verification; monitoring, witnessing, and inspection points; system safety; reliability; peer reviews.

SE-1 CONTAMINATION CONTROL PLAN

6. DRL/DRD No.:

SE-1

7. Title:

Contamination Control Plan

8. Reference:

MAR 10.1

ASTM E595 Standard Test Methods for Total Mass Loss and Collected Volatile Condensable Materials from Outgassing in a Vacuum Environment

Outgassing Data for Selecting Spacecraft Materials (URL: http://outgassing.nasa.gov/)

9. Use:

To outline the plan for controlling payload contamination to acceptable levels over the payload lifecycle. To establish contamination allowances/budgets, plans/methods and schedules for controlling contamination to those allowances/budgets, and plans for recording/tracking/trending contamination measurement/testing results.

10. Preparation Information:

The Contamination Control Plan shall demonstrate how the project's contamination control practices are sufficient to meet project requirements.

SE-2 END ITEM DATA PACKAGE

1. DRL/DRD No.:

SE-16

2. Title:

End Item Data Package

3. Reference:

MAR 14

4. Use:

To ensure that the deliverable contract end-items are in accordance with contract requirements prior to Government acceptance. The End Item Data Package documents the design, fabrication, assembly, test, and integration of the hardware and software being delivered and is included with the end item delivery.

5. Preparation Information:

The End Item Data Package (EIDP), as a minimum, shall include:

(A) The deliverable item name, serial number, part number, and classification status (e.g., flight, non-flight, ground support, etc.).

List of shortages or open items at the time of acceptance with supporting rationale.

As-built serialization.

As-built configuration.

Drawing List and/or Tree.

Specification List and/or Tree.

As-built Engineering Drawings.

As-built Final Assembly Drawings.

As-built EEE parts lists.

As-built materials and processes lists.

PWB coupon analysis/results.

Test Log Book (including total operating time and cycle records).

Chronological history, including:

(i) Total operating hours of operation.

(ii) Total failure-free hours of operation.

Limited life items listings and status, including "life used and remaining" data.

Non-conformance, Anomaly/Problem, and Failure Database and Reports with root cause and corrective action dispositions (including reasons/justifications and plan to close for any that is open).

As-run test procedures.

Functional tests results and reports.

Performance tests results and reports.

Performance analysis results and reports.

Environmental tests results and reports.

Characterization and Calibration tests results and reports.

Trend data and reports.

Correlated models and supporting documentation.

Spare parts list and status.

Technical Budgets and Metrics, including final mass properties

Performance Budgets and Metrics

Photographic documentation of hardware (pre and post-conformal coating for printed wiring assemblies, box or unit, subsystem, system, harness, structure, etc.).

All verification artifacts/documents, including waivers (listed in the V&V Matrix), and the final V&V Matrix.

Certificate of Compliance (properly executed).

Documentation delivered under a separate DRD is not expected to be included in the EIDP.

APPENDIX C: MISSION ASSURANCE COMPLIANCE MATRIX

Enter *Yes* or *No* regarding compliance with the requirements:

- A response of ***Yes*** indicates full compliance with the requirements. ***The Comment column shall be used to indicate how compliance will be achieved***, e.g., through a specified requirements document or equivalent procedure.
- A response of ***No*** indicates less than full compliance with the requirements and ***requires an entry in the Comment column to explain the deviation from full compliance***.

Paragraph or DID	Title	Comply Y / N	Document Number, Title, Revision and Comments
1 GENERAL			
1.1	Safety and Mission Assurance Program		
1.2	Management		
1.3	Reporting		
1.4	Surveillance		
1.5	Requirements Flow-down		
1.6	Suspension of Work Activities		
1.7	Suspicion of Waste, Fraud, and Abuse		
1.8	SMA acceptance of inherited, build-to-print, or modified heritage items		
2 QUALITY MANAGEMENT SYSTEM			
2.1	General		
2.1.1	Quality Assurance		
2.1.2	Control of Nonconforming Product		
2.1.3	Material Review Board (MRB)		

2.1.4	Reporting of Failures and Anomalies		
3 SYSTEM SAFETY			
3.1	General		
3.1.1	Applicable Safety Requirements		
3.2	System Safety Deliverables		
3.2.1	System Safety Plan		
3.2.2	Tailored Payload (Spacecraft/Instrument) Safety Requirements and Compliance List		
3.2.3	Safety Variance		
3.2.4	Preliminary Hazard Analysis		
3.2.5	Project Integration and Test Safety Analysis		
3.2.6	Safety Data Package (SDP)		
3.2.7	Hazardous Procedures for Payload I&T and Pre-launch Processing		
3.2.8	Mishap Reporting and Investigation		

3.2.9	Orbital Debris Assessment Report (ODAR) and End of Mission Plan (EOMP)		
4 RISK ANALYSIS AND RELIABILITY			
4.1	Reliability Program		
4.2	Parts Stress Analysis		
4.3	Fault Tree Analysis (FTA)		
4.4	Limited Life Items		
5 SOFTWARE ASSURANCE (FLIGHT AND GROUND SUPPORT SEGMENTS)			
5.1	Software Assurance Guidelines		
5.2	Software Assurance		
5.3	Software Reviews		
5.4	Government Furnished, Existing, or Purchased Software		
5.5	Surveillance of Software Development		
5.6	Software Safety Analysis		
6 GROUND SUPPORT EQUIPMENT (GSE)			
6.1	Protection of flight hardware		

6.2	Lifting and Handling Equipment		
7 WORKMANSHIP			
7.1	General		
7.2	Electrostatic Discharge Control (ESD)		
8 EEE PARTS			
8.1	General		
8.2	Parts Control Board		
8.3	EEE Parts Reporting		
8.3.1	As-Built Parts List (ABPL)		
8.4	Radiation		
9 MATERIALS AND PROCESSES (M&P)			
9.1	General		
9.2	Life Test Plan and Reports for Lubricated Mechanisms		
9.3	Materials Usage Agreement (MUA)		
9.4	Materials Identification and Usage List (MIUL)		
9.5	Printed Wiring Board Test Coupons		
9.6	Lead-free and Tin Whisker Control		

10 CONTAMINATION CONTROL			
10.1	Contamination Control Plan		
11 METROLOGY AND CALIBRATION			
11.1	Metrology and Calibration Program		
11.2	Use of Non-calibrated Instruments		
12 GIDEP ALERTS AND PROBLEM ADVISORIES			
12.1	Government-Industry Data Exchange Program (GIDEP)		
12.2	Review		
12.3	Actions		
12.4	GIDEP Reporting		
12.5	Reporting		
13 DIGITAL ELECTRONICS			
13.1	General		
14 Planetary Protection			
15 Cybersecurity and Command Protection			
16 End Item Acceptance Data Package			

APPENDIX D: ISS PAYLOAD SUPPLEMENT

At the time of development of this MAR, unique ISS payload requirements exist that supersede those in the safety section. Therefore, for ISS Payloads, it would be convenient to replace Section 3 with the following.

---

3 SYSTEM SAFETY

3.1 GENERAL

The developer shall document and implement a system safety program in accordance with ISS safety requirements, including payload as cargo requirements.

Specific safety requirements include the following:

- The developer shall incorporate three inhibits in the design (dual fault tolerant) if a system failure may lead to a catastrophic hazard. A prelaunch catastrophic hazard is a payload-related hazard, condition, or event occurring prior to launch that could result in a fatal injury to personnel or loss of a ground facility. A post-launch catastrophic hazard is a payload-related hazard, condition, or event occurring after launch and up to payload separation that could result in a fatal injury or loss of flight termination system. For safety failure tolerance considerations loss of the ISS is to be limited to those conditions resulting from failures or damage to elements of the ISS that render the ISS unusable for further operations, even with contingency repair or replacement of hardware, or which render the ISS in a condition which prevents further rendezvous and docking operations with ISS launch elements.
- The developer shall incorporate two inhibits in the design (single fault tolerant if a system failure may lead to a critical hazard. A critical hazard is defined as a hazard, condition or event that may cause severe injury or occupational illness, or major property damage to facilities.
- For safety failure tolerance considerations, critical hazards include loss of ISS elements that are not in the critical path for station survival or damage to an element in the critical path that can be restored through contingency repair.
- The developer shall adhere to specific detailed safety requirements, including compliance verification that must be met for design elements with hazards that cannot be controlled by failure tolerance. These design elements, e.g., structures and pressure vessels, are called “Design for Minimum Risk” areas.

3.2 ISS MISSION-RELATED SAFETY REQUIREMENTS DOCUMENTATION (FLIGHT, GROUND, AND LAUNCH VEHICLE)

- SSP 51700, “Payload Safety Policy and Requirements for the International Space”

- SSP 30599, “ISS Safety Review Process”
- SPX-00008487 Range Safety Documentation for Dragon Cargo
- SPX-00008488 Integrated Safety Checklist for ISS Cargo at Launch Site (KSC FORM 1000)
- KNPR 8715.3 Chapter 20 “KSC Safety Practices Procedural Requirements”

3.3 SYSTEM SAFETY DELIVERABLES

Unless otherwise noted formal delivery items in this section shall be made available for government review.

3.3.1 System Safety Plan (Formal delivery required)

The developer shall prepare a System Safety Program Plan (SSPP) (DRD MA-8) that describes the tasks and activities of system safety management and engineering required to identify, evaluate, and eliminate or control hazards to the hardware, computer-based control systems, and system design by reducing the associated risk to an acceptable level throughout the system life cycle, including ISS safety requirements.

Tailored Payload (Spacecraft/Instrument) Safety Requirements and Compliance List (Formal delivery required)

The Developer shall prepare a Safety Requirements Compliance Checklist (DRD MA-6) to demonstrate that the project is in compliance with NASA and range safety requirements. Noncompliances to safety requirements will be documented in waivers and submitted for approval.
The Developer shall add to the Tailored Payload (Spacecraft/Instrument) Safety Requirements List a compliance status column to demonstrate the project is in compliance with the tailored safety requirement. The Developer shall also include the status of the safety verifications in the project’s hazard reports.

3.3.2 Safety Variance

The Project shall submit Request for Safety Variance for waivers and non-conformances to the applicable safety requirements associated only with personnel or range safety, not those associated with mission success or programmatic risks (DRD MA-7).

3.3.3 Preliminary Hazard Analysis

The Developer shall document a Preliminary Hazard Analysis (PHA) (DRD MA-9). Based on the PHA, the following requirements apply:

- The Developer shall incorporate three independent inhibits in the design (dual fault tolerant) if a system failure may lead to a catastrophic hazard. A catastrophic hazard is defined as a condition that may cause death or a permanent disabling injury or the destruction of a major system or facility on the ground. An inhibit is a design feature (hardware or software) that prevents operation of a function.
- The Developer shall incorporate two independent inhibits in the design (single fault tolerant) if a system failure may lead to a critical hazard. A critical hazard is defined as a condition that may cause a severe injury or occupational illness to personnel or major property damage to facilities.
- The Developer shall adhere to specific detailed safety requirements, including compliance verification that must be met for design elements with hazards that cannot be controlled by failure tolerance. These design elements, e.g., structures and pressure vessels, are called "Design for Minimum Risk" areas.

3.3.4 Project Integration and Test Safety Analysis

The Developer shall perform sufficient safety analyses to evaluate activities for hazards introduced during project integration and testing at the Developer's facility and to evaluate the adequacy of inhibit designs, and operational and support procedures used to eliminate, control, or mitigate hazards.

3.3.5 Safety Data Package (SDP)

3.3.5.1 Descriptive Volume

The developer shall generate a descriptive volume describing payload content and function. The developer shall create a record in the ISS Hazard System titled [insert payload name] Safety Data Package. Attach the descriptive volume to this record. Specify on the cover of the attachment the level of the safety review (Phase I, II, or III) when it is attached to the record.

3.3.5.2 Hazard Reports

The developer shall generate hazard reports as individual records to be entered into the ISS Hazard System with the "In Work" status. They will be approved by Government and changed to "Review" status.

The developer shall create a record for each individual hazard report and shall ensure that each hazard report record is linked to the Safety Data Package record for that payload. The standard hazard report (Form 1298) is already present in the system (causes and controls present, verifications shall be provided by the developer).

For each unique hazard report, the developer shall create and link a new record for each hazard cause. The controls and verifications for a cause shall be entered in the record for that cause. Relevant figures and tables shall be attached to the cause record.

For each required NCR, the developer shall create a new record and link it to the relevant hazard report and cause records and to the Safety Data Package record.

Each record has a status of "In Work" when created and being edited. When approved by the Government, the PSM will change the status to "Review". This shall be done for every record in the Safety Data Package. Review signifies that the ISS Payload Safety Review Panel PSRP may begin formal review of the hazard report.

Note: All ISS Hazard System products have a "print PDF" function that automatically creates a report that may be used by the Payload Developer CM Office.

3.3.6 Hazardous Procedures for Pre-Launch Processing

The developer shall submit, in accordance with the contract schedule, all hazardous ground operations procedures to be used at the launch site (DID 3-3). All launch site procedures shall comply with the launch site and NASA safety regulations, including the designation of hazardous procedures and hazard blocks within hazardous procedures.

The developer shall provide safety support for hazardous operations at the launch site payload processing facilities and launch pad.

3.3.7 Mishap Reporting and Investigation

The developer shall prepare a Mishap Preparedness and Contingency Plan (MPCP) that describes the appropriate mishap and close call notification, reporting, recording, and investigation procedures (DID 3-5).

3.3.8 Safety Review Meeting Support

The developer shall provide technical support to and present their hazard reports in the three flight phased safety reviews at JSC, and any delta reviews when necessary.

Additionally, in the software section, we would add the following paragraph:

5.2 Computer-Based Control System

The developer shall develop an avionics architecture that complies with the computer-based control system requirements of SSP 50038 for inhibit controls.

The developer shall present the architecture to the JSC Computer Safety Panel (CSP) for approval.

The developer shall present verification of the independence of inhibit controls to the JSC CSP for approval as part of a hazard report that documents hazardous circuits.

The developer shall incorporate the results from the Computer-Based Control System analyses and reviews, including references to the associated software requirements, into the hazard reports required by Section 3.3.4.2 of this document.

APPENDIX E: GOVERNMENT PROCUREMENT-RELATED REQUIREMENTS

The following requirements apply to government procurement offices (ref. NPR 8735.2).

The Project Office provides “higher level” quality requirements to the Contracting Officer (FAR pt 46)
Procurements shall be pre-screened using GIDEP and the Supplier Assessment System (SAS)
Pre-award audit is required when govt has no prior assessment record less than 3yrs old
A Project Quality Assurance Surveillance Plan (PQASP) is required
Product acceptance requirements shall be defined
Objective evidence of product acceptance must be required, acquired, and evaluated
Use NFS clause 1852.246-72 when DD250 will be used for acceptance
The Project Office shall manage Government Contract Quality Assurance delegations to DCMA including annual budget call and monthly coordination processes.