

Contract NNG08CA01C
for
Environmental Test and Integration Services

Attachment K

**Mission Assurance Guidelines for GSFC
Projects**



Procedures and Guidelines

DIRECTIVE NO. 300-PG-7120.2.2E APPROVED BY Signature: Original signed by
 EFFECTIVE DATE: May 3, 2005 NAME: Abigail Harper
 EXPIRATION DATE: May 3, 2010 TITLE: Acting Director, OSSMA

Responsible Office: 300/Office of Systems Safety and Mission Assurance (OSSMA)

Title: MISSION ASSURANCE GUIDELINES (MAG) FOR TAILORING TO THE NEEDS OF THE GODDARD SPACE FLIGHT CENTER (GSFC) PROJECTS

TABLE OF CONTENTS

PREFACE 7

CHAPTER 1. OVERALL REQUIREMENTS 13

 1.1 GENERAL 13

 1.2 DESCRIPTION OF OVERALL REQUIREMENTS 13

 1.3 USE OF MULTI-MISSION OR PREVIOUSLY DESIGNED, FABRICATED OR FLOWN
 HARDWARE 14

 1.4 SURVEILLANCE OF THE DEVELOPER 14

 1.5 ACRONYMS AND GLOSSARY 14

 1.6 CONTRACT DATA REQUIREMENTS LIST 14

CHAPTER 2. QUALITY MANAGEMENT SYSTEM 15

 2.1 GENERAL 15

 2.2 SUPPLEMENTAL QUALITY MANAGEMENT SYSTEM REQUIREMENTS 15

 2.2.1 Control of Nonconforming Product 15

 2.2.2 Material Review Board 15

 2.2.3 Reporting of Failures 16

 2.2.4 Control of Monitoring and Measuring Devices 16

 2.2.5 Modification of Flight Software and Ground Station Hardware and Software 16

 2.2.6 Flow-Down of Requirements 16

 2.3 GIDEP ALERTS AND PROBLEM ADVISORIES 16

CHAPTER 3. SYSTEM SAFETY REQUIREMENTS 17

 3.1 SYSTEM SAFETY REQUIREMENTS 17

 3.1.1 Mission-related Safety Requirements Documentation 17

 3.2 SYSTEM SAFETY DELIVERABLES 19

 3.2.1 System Safety Program Plan 19

 3.2.2 Safety Requirements Compliance Checklist 19

 3.2.3 Hazard Analyses 19

 3.3 SAFETY ASSESSMENT REPORT (SAR) 20

 3.4 SAFETY DATA PACKAGE / MISSILE SYSTEM PRELAUNCH SAFETY PACKAGE 20

 3.5 VERIFICATION TRACKING LOG 21

 3.6 MISCELLANEOUS SUBMITTALS FOR RANGE USE 21

 3.7 GROUND OPERATIONS PROCEDURES 21

 3.8 SAFETY VARIANCE 21

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

3.9	SUPPORT FOR SAFETY WORKING GROUP MEETINGS	22
3.10	ORBITAL DEBRIS ASSESSMENT.....	22
3.11	LAUNCH SITE SAFETY SUPPORT	22
3.12	MISHAP REPORTING AND INVESTIGATION.....	22
CHAPTER 4.	RELIABILITY AND PROBABILISTIC RISK ASSESSMENT.....	24
4.1	RELIABILITY AND PROBABILISTIC RISK ASSESSMENT PROGRAM	24
CHAPTER 5.	SOFTWARE ASSURANCE REQUIREMENTS.....	30
5.1	GENERAL.....	30
5.1.1	Software Assurance	30
5.1.2	Software Quality.....	30
5.1.3	Software Safety.....	31
5.1.4	Software Reliability	32
5.1.5	Verification and Validation.....	32
5.1.6	Independent Verification and Validation.....	32
5.1	REVIEWS	33
5.1.7	Software Reviews	33
5.1.8	Engineering Peer Reviews	33
5.2	SOFTWARE CONFIGURATION MANAGEMENT	33
5.3	GFE, EXISTING AND PURCHASED SOFTWARE	34
5.4	SOFTWARE ASSURANCE STATUS REPORTING.....	34
5.5	NASA SURVEILLANCE OF SOFTWARE DEVELOPMENT.....	34
CHAPTER 6.	GROUND DATA SYSTEMS ASSURANCE REQUIREMENTS.....	35
6.1	GENERAL.....	35
6.2	QUALITY MANAGEMENT SYSTEM	35
6.3	REQUIREMENTS.....	35
6.4	REVIEWS.....	36
6.5	ASSURANCE ACTIVITIES	36
6.5.1	Concept Phase.....	36
6.5.2	Requirements Phase.....	36
6.5.3	Design Phase.....	37
6.5.4	Implementation Phase.....	38
6.5.5	Testing Phase	38
6.5.6	Operations and Maintenance Phase	40
6.5.7	Activities Performed throughout the Lifecycle.....	41
6.6	GFE, COTS, EXISTING AND PURCHASED SOFTWARE.....	42
6.6.1	COTS Management	43
6.7	REUSE REQUIREMENTS	43
6.8	DEFECT PREVENTION REQUIREMENTS	43
6.9	DATABASES	43
6.10	SECURITY ASSURANCE	44
6.11	ELECTROMAGNETIC COMPATIBILITY CONTROL	44
6.12	RELIABILITY AND AVAILABILITY	44
6.12.1	Reliability Acceptance Testing	45
6.13	MAINTAINABILITY REQUIREMENTS	46
6.14	SYSTEM SAFETY	46
CHAPTER 7.	RISK MANAGEMENT REQUIREMENTS.....	48
7.1	GENERAL.....	48

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

7.2	APPLICABLE DOCUMENTS	48
7.3	RISK MANAGEMENT PLAN.....	48
7.4	PROBABILISTIC RISK ASSESSMENT	49
7.5	RISK LIST	49
7.6	RISK-BASED ACQUISITION MANAGEMENT	50
CHAPTER 8. INTEGRATED INDEPENDENT REVIEW REQUIREMENTS.....		51
8.1	GENERAL REQUIREMENTS	51
8.2	OVERVIEW OF REVIEW ACTIVITY	51
8.2.1	Mission Reviews:.....	51
8.2.2	Instrument Reviews	53
8.2.3	Spacecraft Reviews.....	53
8.2.4	Operations Reviews	53
CHAPTER 9. DESIGN VERIFICATION REQUIREMENTS.....		54
9.1	GENERAL.....	54
9.2	DOCUMENTATION REQUIREMENTS	54
9.2.1	System Performance Verification Plan	54
9.2.2	Environmental Verification Plan	54
9.2.3	System Performance Verification Matrix	55
9.2.4	Environmental Test Matrix	55
9.2.5	Environmental Verification Specification.....	55
9.2.6	Performance Verification Procedures	56
9.2.7	Verification Reports.....	56
9.2.8	System Performance Verification Report	56
CHAPTER 10. WORKMANSHIP STANDARDS		57
10.1	GENERAL.....	57
10.2	APPLICABLE DOCUMENTS	57
10.3	DESIGN	58
10.3.1	Printed Wiring Boards	58
10.3.2	Assemblies.....	58
10.3.3	Ground Data Systems that Interface with Space Flight Hardware.....	58
10.4	WORKMANSHIP REQUIREMENTS.....	58
10.4.1	Training and Certification.....	58
10.4.2	Flight and Harsh Environment Ground Systems Workmanship	58
10.4.3	Ground Systems (non-flight) Workmanship.....	59
10.4.4	Documentation.....	59
10.5	NEW OR ADVANCED MATERIALS AND PACKAGING TECHNOLOGIES.....	59
10.6	HARDWARE HANDLING	59
10.7	ELECTROSTATIC DISCHARGE CONTROL	59
10.7.1	Applicable Documents.....	59
10.7.2	Electrostatic Discharge Control Requirements	60
CHAPTER 11. PARTS REQUIREMENTS.....		61
11.1	GENERAL.....	61
11.2	PARTS CONTROL BOARD.....	62
11.2.1	Chairmanship.....	62
11.2.2	Membership	62
11.2.3	Delegation.....	62
11.2.4	Meetings.....	62

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

11.2.5	PCB Responsibilities	63
11.2.6	PCB Authority	63
11.3	MANAGEMENT OF PARTS SELECTION	63
11.3.1	EEE Parts	64
11.4	MANAGEMENT OF PARTS ENGINEERING REQUIREMENTS.....	65
11.4.1	System Design	65
11.4.2	Custom Devices	65
11.4.3	Reuse of Parts	65
11.4.4	Derating	66
11.4.5	Traceability and Lot Control.....	66
11.4.6	Incoming Inspection Requirements.....	66
11.4.7	Electronic Parts	66
11.4.8	Use of Alternate Quality Conformance Inspection and Small Lot Sampling Plans.....	67
11.5	MANAGEMENT OF PARTS PROCUREMENT	68
11.5.1	Supplier and Vendor Selection and Surveillance.....	68
11.5.2	Part Supplier and Manufacturer Surveillance (Monitoring).....	68
11.5.3	Coordinated Procurements.....	68
11.6	RADIATION HARDNESS ASSURANCE (RHA)	68
11.6.1	General.....	68
11.7	GOVERNMENT FURNISHED EQUIPMENT.....	69
11.8	COMMERCIAL OFF-THE-SHELF ITEM EQUIPMENT.....	69
11.9	PART QUALIFICATION.....	69
11.9.1	General.....	69
11.9.2	Manufacturing Baseline	70
11.9.3	Qualification by Extension.....	70
11.10	FAILURE ANALYSIS	70
11.11	PRESERVATION AND PACKAGING	70
11.12	HANDLING.....	70
11.13	DATA RETENTION.....	71
CHAPTER 12. MATERIALS, AND PROCESSES REQUIREMENTS.....		72
12.1	GENERAL.....	72
12.2	MATERIALS AND PROCESSES CONTROL BOARD	72
12.2.1	Chairmanship	73
12.2.2	Membership	73
12.2.3	Delegation.....	73
12.2.4	Meetings.....	73
12.2.5	MPCB Responsibilities.....	73
12.2.6	MPCB Authority.....	74
12.3	MANAGEMENT OF MP SELECTION	74
12.3.1	Materials Selection.....	74
12.3.2	Compliant Materials.....	75
12.3.3	Non-compliant Materials	75
12.3.4	Polymeric Materials	75
12.3.5	Flammability and Toxic Offgassing.....	75
12.3.6	Vacuum Outgassing.....	76
12.3.7	Shelf-Life-Controlled Materials.....	76
12.3.8	Inorganic Materials	76
12.3.9	Fasteners	76
12.3.10	Lubrication.....	77
12.3.11	Process Selection	77

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

12.4	MANAGEMENT OF MP ENGINEERING REQUIREMENTS	77
12.4.1	System Design	77
12.4.2	Reuse of Materials	77
12.4.3	Traceability and Lot Control.....	77
12.4.4	Incoming Inspection Requirements.....	78
12.5	MANAGEMENT OF MATERIALS AND PROCESSES PROCUREMENT	78
12.5.1	Supplier and Vendor Selection and Surveillance.....	78
12.5.2	MP Supplier and Manufacturer Surveillance (Monitoring).....	78
12.5.3	Coordinated Procurements.....	78
12.6	GOVERNMENT FURNISHED EQUIPMENT.....	79
12.7	COMMERCIAL OFF-THE-SHELF ITEM EQUIPMENT.....	79
12.8	MP QUALIFICATION.....	79
12.8.1	General.....	79
12.8.2	Manufacturing Baseline.....	79
12.8.3	Qualification by Extension.....	79
12.9	FAILURE ANALYSIS	80
12.10	HANDLING.....	80
12.11	DATA RETENTION.....	80
CHAPTER 13.	CONTAMINATION CONTROL REQUIREMENTS	87
13.1	GENERAL.....	87
13.2	CONTAMINATION CONTROL VERIFICATION PROCESS	87
13.3	CONTAMINATION CONTROL PLAN.....	87
13.4	MATERIAL OUTGASSING.....	87
13.5	THERMAL VACUUM BAKEOUT.....	87
13.6	HARDWARE HANDLING.....	87
CHAPTER 14.	APPLICABLE DOCUMENTS LIST.....	88
CHAPTER 15.	DATA ITEM DESCRIPTIONS.....	95
15.1	DID 2-1: QUALITY MANUAL	95
15.2	DID 2-2: PROBLEM FAILURE REPORT.....	96
15.3	DID 3-1: SYSTEM SAFETY PROGRAM PLAN.....	97
15.4	DID 3-2: SAFETY REQUIREMENT COMPLIANCE CHECKLIST.....	99
15.5	DID 3-3: PRELIMINARY HAZARD ANALYSIS	100
15.6	DID 3-4: OPERATIONS HAZARD ANALYSIS.....	102
15.7	DID 3-5 SAFETY ASSESSMENT REPORT (SAR).....	104
15.8	DID 3-6: SAFETY DATA PACKAGE / MISSILE SYSTEM PRELAUNCH SAFETY PACKAGE.....	106
15.9	DID 3-7: VERIFICATION TRACKING LOG	110
15.10	DID 3-8: GROUND OPERATIONS PROCEDURES	112
15.11	DID 3-9: SAFETY VARIANCE.....	113
15.12	DID 3-10: ORBITAL DEBRIS ASSESSMENT	115
15.13	DID 3-10A: ORBITAL DEBRIS ASSESSMENT REPORT	116
15.14	DID 4-1: RELIABILITY PROGRAM PLAN	117
15.15	DID 4-2: PROBABILISTIC RISK ASSESSMENT PLAN	118
15.16	DID 4-3: FAILURE MODE AND EFFECTS ANALYSIS	119
15.17	DID 4-4: FAULT TREE ANALYSIS	121
15.18	DID 4-5: PARTS STRESS ANALYSIS	122
15.19	DID 4-6: WORST CASE ANALYSIS.....	124
15.20	DID 4-7: RELIABILITY ASSESSMENTS AND PREDICTIONS	125
15.21	DID 4-9: LIMITED-LIFE ITEMS LIST.....	126

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

15.22	DID 5-1: SOFTWARE ASSURANCE PLAN.....	127
15.23	DID 5-2: SOFTWARE MANAGEMENT PLAN.....	128
15.24	DID 5-3: SOFTWARE CONFIGURATION MANAGEMENT PLAN	129
15.25	DID 5-5: SOFTWARE REQUIREMENTS SPECIFICATION	130
15.26	DID 7-1: RISK MANAGEMENT PLAN.....	131
15.27	DID 8-1: MISSION CONCEPT REVIEW	132
15.28	DID 8-2: MISSION DEFINITION REVIEW	133
15.29	DID 8-3: SYSTEM DEFINITION REVIEW.....	134
15.30	DID 8-4: PRELIMINARY DESIGN REVIEW	135
15.31	DID 8-5: CRITICAL DESIGN REVIEW	136
15.32	DID 8-6: PRE-ENVIRONMENTAL REVIEW	137
15.33	DID 8-7: PRE-SHIPMENT REVIEW.....	138
15.34	DID 8-8: MISSION OPERATIONS REVIEW.....	139
15.35	DID 8-9: FLIGHT OPERATIONS REVIEW.....	140
15.36	DID 9-1: SYSTEM PERFORMANCE VERIFICATION PLAN	141
15.37	DID 9-2: PERFORMANCE VERIFICATION PROCEDURE.....	143
15.38	DID 9-3: VERIFICATION REPORTS	144
15.39	DID 10-1: PRINTED WIRING BOARDS TEST COUPONS.....	145
15.40	DID 11-1: PARTS CONTROL PROGRAM PLAN	146
15.41	DID 11-2: AS DESIGNED PARTS, LIST.....	147
15.42	DID 12-1: MATERIALS AND PROCESSES CONTROL PROGRAM PLAN	149
15.43	DID 12-2: AS DESIGNED MATERIALS, AND PROCESSES LIST	150
15.44	DID 12-3: MATERIALS USAGE AGREEMENT	151
15.45	DID 12-4: STRESS CORROSION EVALUATION FORM.....	152
15.46	DID 12-5: POLYMERIC MATERIALS AND COMPOSITES USAGE LIST	153
15.47	DID 12-6: FLAMMABLE MATERIALS USAGE LIST	154
15.48	DID 12-7: ODOR AND TOXIC OFFGASSING MATERIALS USAGE LIST	155
15.49	DID 12-8: WAIVER.....	156
15.50	DID 12-9: INORGANIC MATERIALS AND COMPOSITES USAGE LIST.....	157
15.51	DID 12-10: FASTENER CONTROL PLAN.....	158
15.52	DID 12-11: LUBRICATION USAGE LIST	159
15.53	DID 12-12: LIFE TEST PLAN FOR LUBRICATED MECHANISMS.....	160
15.54	DID 12-13: MATERIAL PROCESS UTILIZATION LIST.....	161
15.55	DID 12-14: CERTIFICATE OF RAW MATERIAL COMPLIANCE.....	162
15.56	DID 13-1: CONTAMINATION CONTROL PLAN.....	163
APPENDIX A. ACRONYMS.....		164

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

PREFACE

P.1 PURPOSE

The purpose of this document is to serve as a resource to the Project Manager and OSSMA, in conjunction with 300-PG-7120.2.1, "Mission Assurance Guidelines (MAG) Implementation", in supporting the development of a realistic set of mission assurance requirements tailored to specific needs of an individual project. It is assumed that the project will select, tailor and then place the appropriate mission assurance requirements either directly into the contract SOW, and/or within a stand-alone Mission Assurance Requirements (MAR) document.

P.2 APPLICABILITY

The guidelines of this PG are intended for multiple missions and multiple instruments including Commercial Off-The-Shelf (COTS) items and apply to in-house, contracts, service level agreements and general support, all of which will be referred to as the developer.

To the extent referenced herein, applicable portions of the documents listed in Chapter 16 form a part of this document.

P.3 AUTHORITY

None.

P.4 REFERENCES

300-PG-7120.2.1, Mission Assurance Guidelines Implementation.

P.5 CANCELLATION

300-PG-7120.2.2D, MAG for Tailoring to the Needs of GSFC Projects.

P.6 SAFETY CONSIDERATIONS

None.

P.7 TRAINING

None.

P.8 RECORDS

None.

P.9 METRICS

None.

P.10 DEFINITIONS

The following definitions apply within the context of this document:

Acceptance Tests: The validation process that demonstrates that hardware is acceptable for flight. It also serves as a quality control screen to detect deficiencies and, normally, to provide the basis for delivery of an item under terms of a contract.

Assembly: See Level of Assembly.

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

Audit: A review of the developer's or sub-developer's documentation or hardware to verify that it complies with project requirements.

Collected Volatile Condensable Material (CVCM): The quantity of outgassed matter from a test specimen that condenses on a collector maintained at a specific constant temperature for a specified time.

Component: See Level of Assembly.

Configuration: The functional and physical characteristics of the payload and all its integral parts, assemblies and systems that are capable of fulfilling the fit, form and functional requirements defined by performance specifications and engineering drawings.

Configuration Control: The systematic evaluation, coordination, and formal approval/disapproval of proposed changes and implementation of all approved changes to the design and production of an item the configuration of which has been formally approved by the developer or by the purchaser, or both.

Configuration Management: The systematic control and evaluation of all changes to baseline documentation and subsequent changes to that documentation which define the original scope of effort to be accomplished (contract and reference documentation) and the systematic control, identification, status accounting and verification of all configuration items.

Contamination: The presence of materials of molecular or particulate nature, which degrade the performance of hardware.

Derating: The reduction of the applied load (or rating) of a device to improve reliability or to permit operation at high ambient temperatures.

Design Specification: Generic designation for a specification that describes functional and physical requirements for an article, usually at the component level or higher levels of assembly. In its initial form, the design specification is a statement of functional requirements with only general coverage of physical and test requirements. The design specification evolves through the project lifecycle to reflect progressive refinements in performance, design, configuration, and test requirements. In many projects the end-item specifications serve all the purposes of design specifications for the contract end-items. Design specifications provide the basis for technical and engineering management control.

Designated Representative: An individual (such as a NASA plant representative), firm (such as assessment developer), Department of Defense (DOD) plant representative, or other government representative designated and authorized by NASA to perform a specific function for NASA. As related to the developer's effort, this may include evaluation, assessment, design review, participation, and review/approval of certain documents or actions.

Destructive Physical Analysis (DPA): An internal destructive examination of a finished part or device to assess design, workmanship, assembly, and any other processing associated with fabrication of the part.

Design Qualification Tests: Tests intended to demonstrate that the test item will function within performance specifications under simulated conditions more severe than those expected from ground handling, launch, and orbital operations. Their purpose is to uncover deficiencies in design and method of manufacture. They are not intended to exceed design safety margins or to introduce unrealistic modes of failure. The design qualification tests may be to either "prototype" or "protoflight" test levels.

Discrepancy: See Nonconformance.

Electromagnetic Compatibility (EMC): The condition that prevails when various electronic devices are performing their functions according to design in a common electromagnetic environment.

Electromagnetic Interference (EMI): Electromagnetic energy, which interrupts, obstructs, or otherwise degrades or limits the effective performance of electrical equipment.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

Electromagnetic Susceptibility: Undesired response by a component, subsystem, or system to conducted or radiated electromagnetic emissions.

End-to-End Tests: Tests performed on the integrated ground and flight system, including all elements of the payload, its control, stimulation, communications, and data processing to demonstrate that the entire system is operating in a manner to fulfill all mission requirements and objectives.

Failure: A departure from specification that is discovered in the functioning or operation of the hardware or software. See nonconformance.

Failure Modes and Effects Analysis (FMEA): A procedure by which each credible failure mode of each item from a low indenture level to the highest is analyzed to determine the effects on the system and to classify each potential failure mode in accordance with the severity of its effect.

Flight Acceptance: See Acceptance Tests.

Fracture Control Program: A systematic project activity to ensure that a payload intended for flight has sufficient structural integrity as to present no critical or catastrophic hazard. Also to ensure quality of performance in the structural area for any payload (spacecraft) project. Central to the program is fracture control analysis, which includes the concepts of fail-safe and safe-life, defined as follows:

- a. **Fail-safe:** Ensures that a structural element, because of structural redundancy, will not cause collapse of the remaining structure or have any detrimental effects on mission performance.
- b. **Safe-life:** Ensures that the largest flaw that could remain undetected after non-destructive examination would not grow to failure during the mission.

Functional Tests: The operation of a unit in accordance with a defined operational procedure to determine whether performance is within the specified requirements.

Hardware: As used in this document, there are two major categories of hardware as follows:

- a. **Prototype Hardware:** Hardware of a new design; it is subject to a design qualification test program; it is not intended for flight.
- b. **Flight Hardware:** Hardware to be used operationally in space. It includes the following subsets:
 - (1) **Protoflight Hardware:** Flight hardware of a new design; it is subject to a qualification test program that combines elements of prototype and flight acceptance verification; that is, the application of design qualification test levels and duration of flight acceptance tests.
 - (2) **Follow-On Hardware:** Flight hardware built in accordance with a design that has been qualified either as prototype or as protoflight hardware; follow-on hardware is subject to a flight acceptance test program.
 - (3) **Spare Hardware:** Hardware the design of which has been proven in a design qualification test program; it is subject to a flight acceptance test program and is used to replace flight hardware that is no longer acceptable for flight.
 - (4) **Re-flight Hardware:** Flight hardware that has been used operationally in space and is to be reused in the same way; the validation program to which it is subject depends on its past performance, current status, and the upcoming mission.

Inspection: The process of measuring, examining, gauging, or otherwise comparing an article or service with specified requirements.

Instrument: See Level of Assembly.

Level of Assembly: The environmental test requirements of GEVS generally start at the component or unit-level assembly and continue hardware/software build through the system level (referred to in GEVS as the payload or spacecraft level). The assurance program includes the part level. Verification testing may also include testing at the assembly and subassembly levels of assembly; for test record keeping these levels are combined into a

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

“subassembly” level. The verification program continues through launch, and on-orbit performance. The following levels of assembly are used for describing test and analysis configurations:

- a. **Part:** A hardware element that is not normally subject to further subdivision or disassembly without destruction of design use. Examples include resistor, integrated circuit, relay, connector, bolt, and gaskets.
- b. **Subassembly:** A subdivision of an assembly. Examples are wire harness and loaded printed circuit boards.
- c. **Assembly:** A functional subdivision of a component consisting of parts or subassemblies that perform functions necessary for the operation of the component as a whole. Examples are a power amplifier and gyroscope.
- d. **Component or unit:** A functional subdivision of a subsystem and generally a self-contained combination of items performing a function necessary for the subsystem’s operation. Examples are electronic box, transmitter, gyro package, actuator, motor, battery. For the purposes of this document, “component” and “unit” are used interchangeably.
- e. **Section:** A structurally integrated set of components and integrating hardware that form a subdivision of a subsystem, module, etc. A section forms a testable level of assembly, such as components/units mounted into a structural mounting tray or panel-like assembly, or components that are stacked.
- f. **Subsystem:** A functional subdivision of a payload consisting of two or more components. Examples are structural, attitude control, electrical power, and communication subsystems. Also included as subsystems of the payload are the science instruments or experiments.
- g. **Instrument:** A spacecraft subsystem consisting of sensors and associated hardware for making measurements or observations in space. For the purposes of this document, an instrument is considered a subsystem (of the spacecraft).
- h. **Module:** A major subdivision of the payload that is viewed as a physical and functional entity for the purposes of analysis, manufacturing, testing, and record keeping. Examples include spacecraft bus, science payload, and upper stage vehicle.
- i. **Payload:** An integrated assemblage of modules, subsystems, etc., designed to perform a specified mission in space. For the purposes of this document, “payload” and “spacecraft” are used interchangeably. Other terms used to designate this level of assembly are Laboratory, Observatory, and satellite.
- j. **Spacecraft:** See Payload. Other terms used to designate this level of assembly are Laboratory, Observatory, and satellite.

Limit Level: The maximum expected flight.

Limited Life Items: Spaceflight hardware (1) that has an expected failure-free life that is less than the projected mission life, when considering cumulative ground operation, storage and on-orbit operation, (2) limited shelf life material used to fabricate flight hardware.

Maintainability: A measure of the ease and rapidity with which a system or equipment can be restored to operational status following a failure. It is characteristic of equipment design and installation, personnel availability in the required skill levels, adequacy of maintenance procedures and test equipment, and the physical environment under which maintenance is performed.

Margin: The amount by which hardware capability exceeds mission requirements.

Mission Assurance: the integrated use of the tasks of system safety, reliability assurance engineering, maintainability engineering, mission environmental engineering, materials and processes engineering, electronic parts engineering, quality assurance, software assurance, configuration management, and risk management to support NASA projects.

Module: See Level of Assembly.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

Monitor: To keep track of the progress of a performance assurance activity; the monitor need not be present at the scene during the entire course of the activity, but he will review resulting data or other associated documentation (see Witness).

Nonconformance: A condition of any hardware, software, material, or service in which one or more characteristics do not conform to requirements. As applied in quality assurance, nonconformances fall into two categories—discrepancies and failures. A discrepancy is a departure from specification that is detected during inspection or process control testing, etc., while the hardware or software is not functioning or operating. A failure is a departure from specification that is discovered in the functioning or operation of the hardware or software.

Offgassing: The emanation of volatile matter of any kind from materials into a manned pressurized volume.

Outgassing: The emanation of volatile materials under vacuum conditions resulting in a mass loss and/or material condensation on nearby surfaces.

Part: See Level of Assembly.

Payload: See Level of Assembly.

Performance Verification: Determination by test, analysis, or a combination of the two that the payload element can operate as intended in a particular mission; this includes being satisfied that the design of the payload or element has been qualified and that the particular item has been accepted as true to the design and ready for flight operations.

Protoflight Testing: See Hardware.

Prototype Testing: See Hardware.

Qualification: See Design Qualification Tests.

Red Tag/Green Tag: Physical tags affixed to flight hardware that mean: red (remove before flight) and green (enable before flight).

Redundancy (of design): The use of more than one independent means of accomplishing a given function.

Reliability: The probability that an item will perform its intended function for a specified interval under stated conditions.

Repair: A corrective maintenance action performed as a result of a failure so as to restore an item to op within specified limits.

Rework: Return for completion of operations (complete to drawing). The article is to be reprocessed to conform to the original specifications or drawings.

Section: See Level of Assembly.

Similarity, Verification by: A procedure of comparing an item to a similar one that has been verified. Configuration, test data, application and environment should be evaluated. It should be determined that design-differences are insignificant, environmental stress will not be greater in the new application, and that manufacturer and manufacturing methods are the same.

Single Point Failure: A single element of hardware the failure of which would result in loss of mission objectives, hardware, or crew, as defined for the specific application or project for which a single point failure analysis is performed.

Spacecraft: See Level of Assembly.

Subassembly: See Level of Assembly.

Subsystem: See Level of Assembly.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

Temperature Cycle: A transition from some initial temperature condition to temperature stabilization at one extreme and then to temperature stabilization at the opposite extreme and returning to the initial temperature condition.

Temperature Stabilization: The condition that exists when the rate of change of temperatures has decreased to the point where the test item may be expected to remain within the specified test tolerance for the necessary duration or where further change is considered acceptable.

Thermal Balance Test: A test conducted to verify the adequacy of the thermal model, the adequacy of the thermal design, and the capability of the thermal control system to maintain thermal conditions within established mission limits.

Thermal-Vacuum Test: A test conducted to demonstrate the capability of the test item to operate satisfactorily in vacuum at temperatures based on those expected for the mission. The test, including the gradient shifts induced by cycling between temperature extremes, can also uncover latent defects in design, parts, and workmanship.

Torque Margin: Torque margin is equal to the torque ratio minus one.

Torque Ratio: Torque ratio is a measure of the degree to which the torque available to accomplish a mechanical function exceeds the torque required.

Total Mass Loss (TML): Total mass of material outgassed from a specimen that is maintained at a specified constant temperature and operating pressure for a specified time.

Unit: See Level of Assembly.

Validation: the process of evaluating software during or at the end of the software development process to determine whether it satisfies specified requirements.

Verification: the process of evaluating software to determine whether the products of a given development phase (or activity) satisfy the conditions imposed at the start of that phase (or activity).

Vibroacoustics: An environment induced by high-intensity acoustic noise associated with various segments of the flight profile; it manifests itself throughout the payload in the form of directly transmitted acoustic excitation and as structure-borne random vibration.

Workmanship Tests: Tests performed during the environmental verification program to verify adequate workmanship in the construction of a test item. It is often necessary to impose stresses beyond those predicted for the mission in order to uncover defects. Thus random vibration tests are conducted specifically to detect bad solder joints, loose or missing fasteners, improperly mounted parts, etc. Cycling between temperature extremes during thermal-vacuum testing and the presence of electromagnetic interference during EMC testing can also reveal the lack of proper construction and adequate workmanship.

Witness: A personal, on-the-scene observation of a performance assurance activity with the purpose of verifying compliance with project requirements (see Monitor).

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

DIRECTIVE NO. 300-PG-7120.2.2E

Page 13 of 172

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

Chapter 1. Overall Requirements

1.1 GENERAL

GSFC is assigned a wide variety of missions that range in complexity from relatively simple to extremely complex; from short duration to many years; and from high National interest to narrow specialized interest. The guidelines presented in this document have been prepared to address this wide range of programs and projects and to reflect Agency adoption of commercial practices, such as International Organization for Standardization (ISO) 9001 quality management requirements, where suitable for spacecraft applications. Some assurance areas (reviews, validation, workmanship standards, parts, materials and processes, reliability, and contamination) are not covered by ISO requirements. Therefore, flight projects must tailor their requirements in these areas to satisfy mission needs. The General Environmental Verification Specification for Space Transportation System (STS) & Expendable Launch Vehicle (ELV) Payloads, Subsystems, and Components (GEVS-SE) should be used as a baseline guide for developing validation requirements tailored to a specific mission.

One area of Mission Assurance that is not negotiable is the System Safety Requirements. The Safety requirements (see Chapter 3 in this document) are levied by the launch range and the launch vehicle provider and are mandatory requirements for all space flight hardware developers. The GSFC OSSMA provides assistance to the Flight Projects in meeting those requirements. The GSFC Project Manager must ensure that the applicable safety requirements are included into the contract statement of work (SOW). The OSSMA Project Safety Manager assigned to each GSFC flight project will assist in providing the appropriate contract language.

In all cases the guidelines are targeted at the optimum set of principles that have been proven in previous low-risk GSFC missions to achieve success. When selecting any particular guideline, the Project Manager should assess whether that guideline needs to be given increased or decreased emphasis to suit the specific mission needs. The Project Manager should exercise flexibility in choosing those guidelines that will add value to the mission. The Project Manager may choose to accept a developer's proposed mission assurance program. These guidelines should be used as a reference for the Project Manager's assessment of the adequacy of the developer's mission assurance program.

The language of specific sections in this document has been prepared so that it can be inserted directly into a contract SOW or other appropriate contract documents with only minor changes. The language states the guidelines as requirements. This was done to assist the Project Manager's team in preparing the SOW document. Each specific guideline may be reworded to provide specific emphasis desirable for a particular application. Texts in italics are not requirements, but represent editorial comments.

1.2 DESCRIPTION OF OVERALL REQUIREMENTS

The developer shall plan and implement an organized Systems Safety and Mission Assurance Program (SSMAP) that encompasses:

1. All flight hardware, either designed/built/provided by the developer or furnished by GSFC, from project initiation through launch and mission operations.
2. The ground system that interfaces with flight equipment to the extent necessary to assure the integrity and safety of flight items.
3. The ground data system.
4. All software critical for mission success.

Managers of the assurance activities shall have direct access to developer management independent of project management, with the functional freedom and authority to interact with all other elements of the project. Issues

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

requiring project management attention shall be addressed with the developer(s) through the Project Manager(s) and/or Contracting Officer Technical Representative(s) (COTR).

The developer Systems Safety and Mission Assurance Program shall apply to the project and its associated developers. The developer shall provide documentation of their Systems Safety and Mission Assurance Program Plan in accordance with the SOW.

1.3 USE OF MULTI-MISSION OR PREVIOUSLY DESIGNED, FABRICATED OR FLOWN HARDWARE

When hardware that was designed, fabricated, or flown on a previous project is considered to have demonstrated compliance with some or all of the requirements of this document such that certain tasks need not be repeated, the developer shall demonstrate how the hardware complies with these requirements. The developer shall submit substantiating documentation in accordance with the SOW.

1.4 SURVEILLANCE OF THE DEVELOPER

The work activities, operations, and documentation performed by the developer and/or his suppliers are subject to evaluation, review, audit, and inspection by government-designated representatives from GSFC, the Government Inspection Agency (GIA), or an independent assurance contractor (IAC). GSFC will delegate in-plant responsibilities and authority via a letter of delegation, or the GSFC contract with the IAC.

The developer and suppliers shall grant access for National Aeronautics and Space Administration (NASA) and NASA representatives to conduct an assessment or survey upon notice. The developer shall provide resources to assist with the assessment or survey with minimal disruption to work activities. The developer, upon request, shall provide government assurance representatives with documents, records, and equipment required to perform their assurance and safety activities. The developer shall also provide the government assurance representative(s) with an acceptable work area within developer facilities.

Note: see Federal Acquisition Regulation (FAR) Parts 46.103, 46.104, 46.202-2, 46.4 and 46.5 for Government quality assurance requirements at contractors' facilities. See FAR Part 52.246 for inspection clauses for contract type.

1.5 ACRONYMS AND GLOSSARY

The definitions of words and terminology can be found in Appendix A Glossary.

Acronyms can be found in Appendix B Acronyms.

1.6 CONTRACT DATA REQUIREMENTS LIST

The Contract Data Requirements List (CDRL) identifies Data Item Descriptions (DIDs) describing data deliverable to the GSFC Project Office. When a DID is part of the SOW, it becomes a CDRL. Sample DIDs may be found in Appendix D Data Item Descriptions of this document. The following definitions apply with respect to assurance deliverables:

Deliver for Approval: *The GSFC Project approves within the period of time that has been negotiated and specified in the contract before the developer may proceed with associated work.*

Deliver for Review: *The GSFC Project reviews and may comment within 30 days. The developer may continue with associated work while preparing a response to GSFC comments unless directed to stop.*

Deliver for Information: *For GSFC Project information only. The developer's associated work schedule is not normally affected.*

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

Chapter 2. Quality Management System

This chapter establishes requirements for an effective Quality Management System (QMS). Augmentations to ISO requirements are included. The SAM may tailor requirements to meet the needs of the project.

2.1 GENERAL

The developer shall have a QMS that is compliant with the requirements of American National Standards Institute (ANSI)/ISO/American Society for Quality (ASQ) Q9001 or equivalent. The developer's Quality Manual shall be provided in accordance with the SOW (DID 2-1).

2.2 SUPPLEMENTAL QUALITY MANAGEMENT SYSTEM REQUIREMENTS

As mentioned previously, ISO requirements do not address some assurance related activities. These activities are identified in the following sections and should supplement the requirements of ANSI/ISO/ASQ Q9001.

2.2.1 Control of Nonconforming Product

The developer shall have a closed loop system for identifying and reporting nonconformance's, ensuring that positive corrective action is implemented to preclude recurrence and verification of the adequacy of implemented corrective action by audit and test as appropriate. The system shall include a nonconformance review process, which shall consist of a Material Review Board (MRB).

2.2.2 Material Review Board

MRB shall be used to process the nonconformance using the following disposition actions:

- a) Scrapped, because the product is not usable for the intended purposes and cannot be economically reworked or repaired.
- b) Re-worked, to result in a characteristic that completely conforms to the standards or drawing requirements.
- c) Returned to supplier, for rework, repair or replacement.
- d) Repaired using a standard repair process previously approved by the MRB and /or government Quality Assurance (QA) organization.
- e) Used as is upon concurrence with the government Quality Assurance (QA) organization.

MRB disposition actions shall also include request for major waiver. The MRB shall consist of a core team, supplemented with other disciplines brought in as necessary. A developer representative responsible for ensuring that MRB actions are performed and implemented per developer procedures shall chair it. The MRB shall consist of the appropriate functional and project representatives who are needed to ensure timely determination, implementation and close-out of recommended MRB disposition. At developer/supplier facilities, NASA/Government representatives may participate in MRB activities as deemed appropriate by Government management or contract, otherwise, the MRB chairperson shall advise the Government of the MRB actions and recommendations.

The MRB process shall investigate, in a timely manner, nonconforming item(s) in sufficient depth to determine proper disposition. For each reported nonconformance, there shall be an investigation and engineering analysis sufficient to determine cause and corrective actions for the nonconformance. Written authorization shall be provided to disposition the nonconformance's. The MRB close-out shall included documented objective evidence of the verification of effective corrective action.

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

2.2.3 Reporting of Failures

The developer shall report failures in accordance with the SOW (DID 2-2). The developer shall describe their processes for review, disposition, and approval of failure reports in applicable procedure(s) included, or referenced in the Quality Manual. The developer shall report instances of failure to the GSFC Project Office within 24 hours of occurrence.

The developer shall report failures beginning with the first power application at the start of end item acceptance testing of the major component, subsystem, or instrument level (as applicable to the hardware level for which the developer is responsible), or the first operation of a mechanical item. Software Problem reporting shall begin with first use of the flight build software. The developer shall continue reporting failures through formal acceptance by the GSFC project office and the post-launch operations, commensurate with developer presence and responsibility at GSFC and launch site operations. Developers may use their own form upon request and approval by the GSFC project office. All discrepancies including root cause determination, corrective action, verification, and close out shall be documented and available for review by NASA, even if it was not required to be reported.

2.2.4 Control of Monitoring and Measuring Devices

The developer shall comply with the requirements of Section 7.6 of ANSI/ISO/ASQ Q9001 "Quality Management Systems" regarding the control of monitoring and measuring devices. The developer's testing and calibration laboratories shall be compliant with the requirements of ISO/IEC 17025 "General Requirements for the Competence of Testing and Calibration Laboratories".

2.2.5 Modification of Flight Software and Ground Station Hardware and Software

The developer shall ensure modification of on-orbit flight software and ground station hardware and software is in accordance with original system design specifications and validation processes.

2.2.6 Flow-Down of Requirements

The developer's QA and safety programs shall flow requirements to all suppliers, and include a process to verify compliance. Specifically, the developer shall meet requirements by indicating, in the contract review and purchasing processes, the procedures for documenting, communicating, and reviewing requirements with sub-tier suppliers.

2.3 GIDEP ALERTS AND PROBLEM ADVISORIES

This section establishes requirements for GIDEP participation in order to detect problems that affect or potentially affect the suitability of electronic parts and materials for use in GSFC products or that affect or potentially affect personnel or system safety.

The developer shall participate in the GIDEP (Government-Industry Data Exchange Program) in accordance with the requirements of the GIDEP Operations Manual (S0300- BT-PRO-010) and the GIDEP Requirements Guide (S0300-BU-GYD-010), available from the GIDEP Operations Center, Post Office (PO) Box 8000, Corona, California 92878-8000. For information on GIDEP, refer to the following web site: <http://www.gidep.org>

The developer shall review all GIDEP ALERTs, GIDEP SAFE-ALERTs, GIDEP Problem Advisories, GIDEP Agency Action Notices, NASA Advisories and any informally documented component issues presented by Code 303, to determine if they affect the developer products produced for NASA. For GIDEP ALERTs, GIDEP SAFE-ALERTs, GIDEP Problem Advisories, GIDEP Agency Action Notices and NASA Advisories that are determined to affect the program, the developer shall take action to eliminate or mitigate any negative effect to an acceptable level. The developer shall generate the appropriate failure experience data report(s) (GIDEP ALERT, GIDEP SAFE-ALERT, GIDEP Problem Advisory) on a monthly basis, in accordance with the requirements of GIDEP SO300-BT-PRO-010 and S0300-BU-GYD-010 whenever failed or nonconforming items, available to other buyers, are discovered during the course of the contract.

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

DIRECTIVE NO. 300-PG-7120.2.2E

Page 17 of 172

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

Chapter 3. System Safety Requirements

3.1 SYSTEM SAFETY REQUIREMENTS

Spacecraft and instrument developers shall implement a system safety program in accordance with NPR 8715.3 "NASA Safety Manual" and the requirements imposed by GSFC OSSMA and the appropriate launch service provider/launch range safety representative.

The system safety program is a mandatory contract element and shall be placed directly into the contract SOW, technical specification and other direct contract requirements documents, including the Contract Data Requirements List (CDRL) for mandatory safety deliverables.

Prior to shipment of hardware to the launch range, Code 302 safety certification shall be obtained in accordance with 302-PG-7120.2.1 "Systems Safety Support to GSFC Missions and Other Organizations". A letter of safety compliance shall be initiated by the Project Safety Manager (PSM) and signed by the Code 302 Chief (OSSMA) stating all safety design requirements have been met and that the payload is safe to ship to the launch site and process for launch.

The system safety program begins in the concept phase of design and continues throughout all phases of the mission as defined by the applicable requirements documents listed below (see 3.2.1). The developer shall implement a program that provides for early identification and control of hazards during design, fabrication, test, transportation and ground activities. For STS launches the developer shall also include hazard identification and control for launch, orbital operations, landing and post-landing.

Specific safety requirements include the following:

- If a system failure may lead to a **catastrophic hazard**, the system shall have three inhibits (dual fault tolerant). A **Catastrophic hazard is defined as** a condition that may cause death or permanently disabling injury, major system or facility destruction on the ground, or vehicle during the mission.
- If a system failure may lead to a **critical hazard**, the system shall have two inhibits (single fault tolerant). A **Critical hazard is defined as** a condition that may cause severe injury or occupational illness, or major property damage to facilities, systems, or flight hardware.
- Hazards which cannot be controlled by failure tolerance (e.g., structures, pressure vessels, etc.) are called "Design for Minimum Risk" areas of design and have separate, detailed safety requirements that they must meet. Hazard controls related to these areas are extremely critical and warrant careful attention to the details of verification of compliance on the part of the developer.

3.1.1 Mission-related Safety Requirements Documentation

The following list mandatory compliance requirements relevant to the applicable launch vehicles/launch services. Satisfactory compliance with the requirements documents listed in the following paragraphs is required to gain payload access to the launch site and subsequent launch. The mission-related safety requirements in one of the following sub-paragraphs will normally apply; for STS Missions, 3.1.1.1 applies; for Eastern Test Range (ETR) or Western Test Range (WTR) Missions, 3.1.1.2 applies; for Wallops Flight Facility (WFF) Missions, 3.1.1.3 applies; for Japanese Missions, 3.1.1.4 applies; for European Missions, 3.1.1.5 applies; for Russian Missions, 3.1.1.6 applies. The most stringent safety requirements take precedence.

3.1.1.1 STS Missions (Flight and Ground)

a. NSTS 1700.7B, "Safety Policy and Requirements for Payloads Using the Space Transportation System".

b. NSTS/ISS 18798 -- Interpretations of NSTS/ISS Payload Safety Requirements.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

- c. NSTS/ISS 13830, Payload Safety Review and Data Submittal Requirements
- d. KHB 1700.7 – Space Shuttle Payload Ground Safety Handbook
- e. KNPR 1710.2, “Kennedy Space Center Safety Practices Procedural Requirements”.
- f. Facility-specific Safety Requirements as applicable.

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

- a. AFSPCMAN 91-710, “Range Safety User Requirements”.
- b. KNPR 1710.2, “Kennedy Space Center Safety Practices Procedural Requirements.”
- c. NPR 8715.3, “NASA Safety Manual”
- d. Facility-specific Safety Requirements, as applicable.

3.1.1.3 Wallops Flight Facility (WFF) Missions

- a. RSM-93, “Range Safety Manual for GSFC/WFF”
- b. 540-PG-8715.1.1 “Mechanical Systems Safety Manual” Volume I and II
- c. AFSPCMAN 91-710, “Range Safety User Requirements”

3.1.1.4 Japanese Missions

- a. JMR 002, “Launch Vehicle Payload Safety Requirements”.
- b. KDP-99105, “Safety Guide for H-II/H-IIA Payload Launch Campaign”.
- c. AFSPCMAN 91-710, “Range Safety User Requirements” as negotiated with JAXA and GSFC OSSMA.

3.1.1.5 European Missions

- a. ECSS-Q-40, “Space Product Assurance: Safety”
- b. CSG-RS-10A-CN, “Centre Spatial Guyanais (CSG) Safety Regulations Vol. 1: General Rules”
- c. CSG-RS-21A-CN, “CSG Safety Regulations Vol. 2 Pt. 1: Specific Rules: Ground Installations”
- d. CSG-RS-22A-CN, “CSG Safety Regulations Vol. 2 Pt. 2: Specific Rules: Spacecraft”
- d. AFSPCMAN 91-710, “Range Safety User Requirements” as negotiated with ESA and GSFC OSSMA.

3.1.1.6 Russian Missions

- a. P32928-103, “Requirements for International Partner Cargoes Transported on Russian Progress and Soyuz Vehicles”.

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

3.1.1.7 Payload Integration Facility Requirements

a. GSFC Payload Integration Facility Requirements. Developers doing I&T activities at GSFC shall comply with all facility requirements as provided in 540-PG-8715.1.1 "Mechanical Systems Safety Manual Volume I and II", as well as GPD 8715.1, "Goddard Space Flight Center Safety Policy". Developers shall complete a safety evaluation form in accordance with 540-PG-8715.1.1 "Mechanical Systems Safety Manual must be completed and submitted to Code 549 before any hardware or equipment will be accepted into the facility.

The specific safety requirements for the GSFC I&T facilities are provided in 540-PG-8715.1.1 "Mechanical Systems Safety Manual Volume I and II" and GPD 8715.1, "Goddard Space Flight Center Safety Policy".

b. Other Payload Integration Facility Requirements. Developers doing I&T activities at other installations shall comply with all applicable installation safety requirements.

NOTE: Range Facilities and commercial Integration Facilities typically have specific requirements that apply to Integration, Testing and Launch Preparation activities. The GSFC OSSMA will review and approve all procedures that apply to operations within facilities other than GSFC I&T facilities.

3.2 SYSTEM SAFETY DELIVERABLES

3.2.1 System Safety Program Plan

The developer shall prepare a System Safety Program Plan (SSPP) (DID 3-1). The developer shall submit the SSPP to GSFC for approval prior to submittal to the launch range.

The developer shall specify in the SSPP the hazard analyses required to be performed on flight hardware, GSE, integration & test and pre-launch operations.

3.2.2 Safety Requirements Compliance Checklist

The developer shall demonstrate that the payload is in compliance with all safety requirements and any non-compliant areas have been identified. The developer shall document this in a Compliance Checklist (DID 3-2).

Safety compliance will be granted via GSFC Code 302 Safety Certification letter to the Project Manager only after verification that all applicable safety requirements have been met.

3.2.3 Hazard Analyses

The GSFC Project Safety Manager will define which safety analyses are required based on the complexity of the payload. The Analysis Techniques listed in Appendix D of NPR 8715.3 will aid, and in certain areas, will be required by the developer for future CDRL deliverables (i.e., SDP, MSPSP, SAR). Space Shuttle payloads use NSTS 22254, Methodology of Space Shuttle Hazard Analysis, for guidance.

The developer shall document all the results of all Hazard Analyses in either the SDP, the MSPSP, or SAR.

3.2.3.1 Preliminary Hazard Analysis

The developer shall perform and document a Preliminary Hazard Analysis (PHA) to (1) identify safety critical areas; (2) provide an initial assessment of hazards; (3) identify recommended hazard controls; (4) follow-on actions (DID 3-3).

3.2.3.2 Operations Hazard Analysis (OHA)

The developer shall perform and document an Operations Hazard Analysis (OHA) on all projects prior to I&T activities (DID 3-4).

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

The OHA describes the hardware and test equipment operations to demonstrate that the planned I&T activities are compatible with the facility safety requirements and that any inherent hazards associated with those activities are mitigated to an acceptable level. At GSFC the OSSMA is responsible for reviewing and approving the OHA as well as the organization's test and handling procedures for I&T prior to receiving the hardware at GSFC.

The developer shall submit a Work Order Authorization (WOA) to the Project Safety Manager for approval before performing any hazardous operations. *At GSFC the Project Safety Manager will review all Work Order Authorizations (WOAs) and approve all Hazardous WOAs generated by the organization during I&T activities.*

3.2.3.3 Operating and Support Hazard Analysis

The developer shall perform and document an Operating and Support Hazard Analysis (O&SHA) to evaluate procedurally controlled activities for hazards or risks introduced into the system during pre-launch processing (i.e., launch site or processing facilities) and to evaluate adequacy of procedures used to eliminate, control, or abate identified hazards or risks. The developer shall document the results of the O&SHA in the SDP or MSPSP.

The O&SHA identifies and evaluates hazards resulting from the implementation of operations or tasks performed by persons, considering the following criteria: the planned system configuration and/or state at each phase of activity; the facility interfaces; the planned environments; the supporting tools or other equipment, including software controlled automatic test equipment, specified for use; operational and/or task sequence, concurrent task effects and limitations; biotechnological factors, regulatory or contractually specified personnel safety and health requirements; and the potential for unplanned events including hazards introduced by human errors. The human shall be considered an element of the total system, receiving both inputs and initiating outputs during the conduct of this analysis.

3.2.3.4 Software Safety Analysis

The developer shall identify hazards caused by software as a part of the nominal hazard analysis process, and their controls will be verified prior to acceptance.

Section 5.2.2 describes desired software safety activities to meet NASA HQ guidelines.

3.3 SAFETY ASSESSMENT REPORT (SAR)

This section is for developers that will produce an instrument or subsystem. They do not produce the document(s) referred to in section 3.5 but rather supply the SAR to the spacecraft or observatory developer. This document does not get delivered to Range Safety.

Each instrument or subsystem developer shall perform and document a comprehensive Safety Assessment Report (SAR) of their instrument or subsystem (DID 3-5).

This report is used to assist the spacecraft developer/integrator in preparing the Missile System Pre-launch Safety Package (MSPSP) for submittal to the launch range. This safety assessment shall identify all safety features of the hardware, software, and system design, as well as operational related hazards present in the system.

3.4 SAFETY DATA PACKAGE / MISSILE SYSTEM PRELAUNCH SAFETY PACKAGE

This section is for developers that will produce the spacecraft or observatory. They will need the document(s) called out in section 3.3 if an outside source will be producing an instrument or subsystem.

The spacecraft developer or integrator shall prepare and submit a Safety Data Package (SDP) for STS/ISS payloads, or a Missile System Pre-launch Safety Package (MSPSP) for ELV and Pegasus payloads, (DID 3-6) to GSFC for review and approval before submittal to the launch range. The developer shall take measures to control and/or minimize each significant identified hazard. The spacecraft developer /integrator shall use, as inputs to the SDP or MSPSP, the results of SAR(s) provided by the instrument and subsystem developers.

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

DIRECTIVE NO. 300-PG-7120.2.2E

Page 21 of 172

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

Early in the project lifecycle, the developer will work with GSFC OSSMA to tailor (as appropriate) safety requirements deemed not applicable to the payload, and then coordinate these with the launch range. Also early in the design phase and continuing throughout the development effort, the developer shall identify hazards associated with the flight system, ground support equipment, and their interfaces that affect personnel, launch vehicle hardware, or the spacecraft.

3.5 VERIFICATION TRACKING LOG

The developer shall establish a "closed loop" process for tracking all hazards to acceptable closure through the use of a Verification Tracking Log (VTL) (DID 3-7).

The VTL shall be delivered with the final SDP/MSPSP and updated regularly until all items are closed. Individual VTL items shall be closed with appropriate documentation verifying the stated hazard control has been implemented, and individual closures shall be complete prior to first operational use/restraint.

3.6 MISCELLANEOUS SUBMITTALS FOR RANGE USE

The following lists of forms are to be submitted to range safety:

- Material Selection List for Plastic Films, Foams, and Adhesive Tapes - (<http://rtreport.ksc.nasa.gov/techreports/95report/msf/ms10.html>) The list is published in GP-1098, KSC Ground Operations Safety Plan, Volume I, Safety Requirements, and is updated quarterly. Materials are evaluated for ESD, flammability, and compatibility with hypergols. (Ship-60 day to ETR/WTR/KSC)
- Radiation forms/analysis - KHB 1860.1 (KSC Ionizing Radiation Protection Program) and KHB 1860.2 (KSC Non-Ionizing Radiation Protection Program) includes forms for ionizing and non-ionizing radiation from RF, light, laser, and radioactive sources. Forms must be completed to provide information on the radiation source(s) and the source user(s). Procedures must also be submitted. (Ship-120 days to ETR/WTR/KSC)
- Process Waste Questionnaire (PWQ) (KSC/Eastern Range Only) - PWQ records all the hazardous materials that are brought to the range with the payload. Specific information on storage, containment, and spill control are required. (Ship- 60 days to KSC/ETR)
- Environmental Impact Statement (EIS) (KSC/Eastern Range Only) - An EIS is required to define the impact of an aborted/terminated launch. (Ship-60 days to KSC/ETR)

3.7 GROUND OPERATIONS PROCEDURES

The developer shall submit, in accordance with the contract schedule, all ground operations procedures (DID 3-8) to be used at GSFC facilities, or the launch site. The developer shall identify all hazardous ground operations, as well as the procedures to control them. Developers shall insure their launch site procedures comply with the launch site and NASA safety regulations. GSFC OSSMA will review and approve all hazardous procedures before submittal to the launch range.

Safety support of hazardous I&T operations performed at GSFC and at the launch site is required and needs to be planned and budgeted for by the project either through GSFC OSSMA or the GSFC building responsible organization in accordance with Mechanical Systems Safety Manual Volume I and II.

3.8 SAFETY VARIANCE

When a specific safety requirement cannot be met, the developer shall submit an associated safety variance, per NPR 8715.3; to GSFC OSSMA that identifies the hazard and shows the rationale for approval of a variance (DID 3-9.) The following definitions apply to the safety variance approval policy:

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

- a. Variance: Documented and approved permission to perform some act or operation contrary to established requirements.
- b. Deviation: A documented variance that authorizes departure from a particular safety requirement that does not strictly apply or where the intent of the requirement is being met through alternate means that provide an equivalent level of safety with no additional risk. The OSHA requirements (1910 29 CFR) term for deviation is alternate or supplemental standard only when it applies to OSHA requirements.
- c. Waiver: A variance that authorizes departure from a specific safety requirement where a special level of risk has been documented and accepted.

All requests for variance will be accompanied by documentation as to why the requirement can not be met, the risks involved, alternative means to reduce the hazard or risk, the duration of the variance, and comments from any affected employees or their representatives (if the variance affects personal safety).

3.9 SUPPORT FOR SAFETY WORKING GROUP MEETINGS

The developer shall provide technical support to the Project for Safety Working Group (SWG) meetings, Technical Interface Meetings (TIM), and technical reviews.

The SWG will meet as necessary to review procedures and analyses that contain or examine safety critical functions or as convened by the GSFC Project Safety Manager to discuss any situations that may arise with respect to overall project safety.

3.10 ORBITAL DEBRIS ASSESSMENT

- a. Each instrument or subsystem developer – shall aid the spacecraft contractor in completing an orbital debris assessment of the instrument. It is necessary to identify any stored energy sources in instruments (pressure vessel, dewar, etc.) as well as any energy sources that can be passivated at end of life.
- b. The spacecraft developer shall supply an Orbital Debris Assessment (DID 3-10) consistent with NPD 8710.3, Policy for Limiting Orbital Debris Generation and NSS 1740.14, Guidelines and Assessment Procedures for Limiting Orbital Debris in accordance with the CDRL. Design and safety activities shall take into account the spacecraft's ability to conform to debris generation requirements.

The developer can use Orbital Debris Assessment Software that is available for download from the NASA Orbital Debris Program Office at URL: <http://sn-callisto.jsc.nasa.gov>

3.11 LAUNCH SITE SAFETY SUPPORT

The developer shall provide safety support for hazardous operations at the launch site. NOTE: Range safety is not responsible for project safety support at the launch ranges.

Safety support of hazardous I&T operations performed at GSFC and at the launch site is required and needs to be planned and budgeted for by the project either through GSFC OSSMA or the GSFC building responsible organization in accordance with Mechanical Systems Safety Manual Volume I and II.

3.12 MISHAP REPORTING AND INVESTIGATION

The developer shall report any mishaps, incidents, hazards, and close calls on a NASA Form NF1627 or equivalent form, in accordance with NPR 8621.1 "NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Record keeping".

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

Mishaps at GSFC facilities shall be reported in accordance with GPG 8621.1, "Reporting of Mishaps, Incidents, Hazards, and Close Calls". The reporting of Mishaps, incidents, close calls, and hazardous conditions is the responsibility of all GSFC Managers, Supervisors and employees.

Additional requirements pertaining to the attachment of a Nonconformance Report (NCR) to the NF1627 and the initiation of a Hazard Abatement Plan are contained in GPG 8621.2, "Processing Mishap, Incident, Hazard, and Close Call Reports".

Procedures for the final phase of the process, involving the investigation mishaps, incidents, hazards, and close calls, are detailed in GPG 8621.3, "Mishap, Incident, Hazard, and Close Call Investigation." GPG 8621.3 also includes requirements for the establishment of investigation boards and the development, implementation, and evaluation of corrective actions and lessons learned. This directive is the GSFC implementation of the investigational aspects of NPR 8621.1 "NASA Procedures and Guidelines for Mishap Reporting, Investigating, and Recordkeeping".

Note: GPG 8621.3 does not apply to mission failures in the Balloon Program Office or Sounding Rocket Program Office in which there is no death, injury, or illness, or unanticipated property damage (see NPR 8621.1).

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

Chapter 4. Reliability and Probabilistic Risk Assessment

This chapter provides recommended Reliability and Probabilistic Risk Assessment requirements. The SAM, in conjunction with the SSRO, will tailor these requirements to conform with NPR 8705.4 Risk Classification for NASA Payloads. The tailored requirements will reflect project type (e.g. instrument versus observatory, and heritage design versus new development, etc.)

The tailored Reliability and Probabilistic Risk Assessment program has methods and techniques to:

- a. *Use Probabilistic Risk Assessment (PRA) to assess and manage program risk.*
- b. *Demonstrate that redundant elements, including alternative paths and workarounds, are functionally independent to the extent practicable.*
- c. *Demonstrate that the stresses applied to parts do not compromise part reliability.*
- d. *Identify single point failure items and how they affect mission objectives and degrade safety.*
- e. *Show that the design reliability is consistent with mission design life requirements.*
- f. *Identify limited-life items and ensure their useful lives are conserved for on-orbit operations.*
- g. *Perform trend analysis during fabrication and pre-launch I & T activities.*

4.1 RELIABILITY AND PROBABILISTIC RISK ASSESSMENT PROGRAM

Preparing a Reliability and Probabilistic Risk Assessment Program is recommended for every program and project, since it will form the baseline of what reliability and probabilistic risk assessment activities, analyses, and assessments are best suited to the project, provide details of the approach and methodologies used, and highlight the schedule for completion. The plan should be initiated during the early stages of formulation to ensure the required resources are properly identified, budgeted and planned. The Reliability Program and Risk Assessment Program and corresponding planning documents can be separate, or can be combined.

The developer shall have a Reliability and Probabilistic Risk Assessment Program. The developer shall ensure the Reliability Program is consistent with those portions of NASA-STD-8729.1 Planning, Developing and Managing an Effective Reliability (R&M) Program that refer to reliability under the SOW. The developer shall ensure the Probabilistic Risk Assessment Program is consistent with NPR 8705.4 Risk Classification for NASA Payloads.

4.2 Reliability Program Plan

The developer shall provide a Reliability Program Plan describing the planned approach for the project reliability activities (DID 4-1) with the proposal. The developer shall identify in the plan the reliability tasks to be performed and how those tasks will be implemented and controlled. The developer shall discuss the scheduling of the reliability tasks relative to project milestones. The developer shall ensure reliability functions are an integral part of the design and development process and the reliability functions interact effectively with other project disciplines, including systems engineering, hardware design, and product assurance. The developer shall describe how reliability assessments are integrated with the design process and other assurance practices. The developer shall describe how failure definitions and alternate and degraded modes of operations that include credible failure conditions could be mitigated by implementing workarounds. The developer shall describe the integration of reliability activities with the probabilistic risk assessment process.

4.3 Probabilistic Risk Assessment Plan

The Probabilistic Risk Assessment (PRA) and the PRA Plan provide a comprehensive, systematic and integrated approach to identifying undesirable events, the scenarios leading to those events beginning with the initiating event

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

or events, the frequency or likelihood of those events and the event consequences. The assessment will be used to assist in identifying pivotal events that may protect against, aggravate or mitigate the resulting consequences.

The developer shall provide a Probabilistic Risk Assessment (PRA) Plan describing the developer approach for the project probabilistic risk assessment activities under the SOW (DID 4-2). The developer shall describe scenarios that call for the use of probabilistic risk assessment tools. The developer shall identify the types of analyses to be performed for each scenario, and the modeling tools and techniques to be used (e.g., Master Logic Diagrams (MLD), Failure Mode and Effects Analysis (FMEA), Fault Tree Analyses (FTA), Event Tree Analyses (ETA), Event Sequence Diagrams).

The developer shall provide PRA with a comprehensive, systematic, and integrated approach to identifying undesirable events, the scenarios leading to those events beginning with the initiating event or events, the frequency or likelihood of those events and the event consequences. The developer shall use the PRA to assist in identifying pivotal events that may protect against, aggravate, or mitigate the resulting consequences.

The developer shall provide a comprehensive and balanced PRA that considers all relevant critical factors, including safety of the public, astronauts and pilots, NASA workforce, adverse impacts on the environment, high value equipment and property, national interests, security, etc. The developer shall implement the PRA procedures to reflect and incorporate the results of project risk analysis, including the identification of hazards, risks, and recommended controls to manage risk.

The developer shall perform, maintain, and submit the Probabilistic Risk Assessment under the SOW.

4.4 Reliability Analyses

The developer shall perform reliability analyses concurrently with design activities to optimize system configurations, and identify and promptly correct potential problems.

4.4.1 Failure Modes and Effects Analysis and Critical Items List

The developer shall perform a Failure Modes and Effects Analysis (FMEA) early in the design phase, under NPR 8705.4 Risk Classification for NASA Payloads (DID 4-3), to identify potential failure modes and the effect of those failures on related systems, or the mission. The developer shall revise the FMEA to reflect current configuration. The developer shall assess failure modes at the component interface level. The developer shall assess each failure mode for the effect at that level of analysis, the next higher level, and upward. The developer shall assign the failure mode a severity category based on the most severe effect caused by a failure. The developer shall address mission phases (e.g., launch, deployment, on-orbit operation, and retrieval) in the analysis.

The developer shall determine severity categories under Table 4-1:

TABLE 4-1. SEVERITY CATEGORIES

Category	Severity	Description
1	Catastrophic	Failure modes that could result in serious injury, loss of life (flight or ground personnel), or loss of launch vehicle.
1R		Failure modes of identical or equivalent redundant hardware items that could result in Category 1 effects if all failed.
1S		Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Category 1 consequences.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

2	Critical	Failure modes that could result in loss of one or more mission objectives as defined by the GSFC project office.
2R		Failure modes of identical or equivalent redundant hardware items that could result in Category 2 effects if all failed.
3	Significant	Failure modes that could cause degradation to mission objectives.
4	Minor	Failure modes that could result in insignificant or no loss to mission objectives

The developer shall use the results of the FMEA to evaluate the design against requirements. The developer shall ensure identified discrepancies are evaluated by management and design groups to determine the need for corrective action. The developer shall use the FMEA to ensure that redundant paths are isolated or protected so that any single failure causing loss of a functional path will not affect other functional paths, or the capability to switch to a redundant path. The developer shall perform FMEA analysis procedures and documentation under documented procedures. The developer shall analyze failure modes resulting in severity categories 1, 1R, 1S or 2 down to a level to determine the root failure cause.

The developer shall itemize failure modes assigned to Severity Categories 1, 1R, 1S, and 2 on a Critical Items List (CIL), and maintain the CIL with the FMEA. The developer shall include rationale for retaining the items on the CIL. The developer shall submit the FMEA and CIL to Project Office under the SOW. FMEA and CIL results shall be presented at all design reviews, beginning with PDR. Presentations shall include design trade-study results and FMEA results impacting design or risk decisions.

4.4.2 Fault Tree Analysis

The fault tree in itself is not a quantitative model, but becomes a quantitative assessment when combined with quantitative data as part of the PRA. The SSRO and the Project will determine whether a qualitative or quantitative fault tree analysis is appropriate.

The developer shall perform fault tree analyses that address both mission failures and degraded modes of operation under the NUREG-0492, Fault Tree Handbook (DID 4-4.) Beginning with each undesired state (mission failure or degraded mission), the developer shall expand the fault tree to include all credible combinations of events, faults, and environments that could lead to the undesired state. The developer shall consider component hardware and software failures, external hardware and software failures, and human factors in the analysis.

The developer shall provide the results of the Fault Tree Analysis to the Project Office for review. FTA results shall be presented at all design reviews, beginning with PDR. Presentations shall include design trade-study results and FTA results impacting design or risk decisions.

4.4.3 Parts Stress Analysis

The developer shall subject each application of electrical, electronic, and electromechanical (EEE) parts to stress analyses for conformance with the applicable derating guidelines.

The developer shall perform the analyses at the most stressful values that result from specified performance and environmental requirements (e.g., temperature and voltage) on the assembly or component.

The developer shall provide the analyses, summary sheets, and revisions as required to the Project Office for review (DID 4-5). Analyses results shall be presented at all design reviews beginning with PDR. Presentations shall include design trade study results and Parts Stress Analyses results impacting design or risk decisions.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

4.4.4 Worst Case Analysis

The developer shall perform Worst Case Analyses (*DID 4-6*) on circuits with common cause failures (such as replicated circuitry) or where failures result in a FMEA severity category of 2 or higher. The developer shall analyze the most sensitive design parameters, including those that are subject to variations that could degrade performance. The developer shall demonstrate the design margins in electronic circuits, optics, electromechanical and mechanical items by analyses, test or both to ensure they meet design requirements.

The developer shall consider all parameters set at worst case limits and worst case environmental stresses for the parameter and operation being evaluated in the analyses. Part parameter values for the analyses typically include:

- a. Manufacturing variability.
- b. Variability due to temperature.
- c. Environmental aging effects.
- d. Cumulative space radiation parameter changes.

The developer shall revise the analyses with design changes. The developer shall provide the results of the analyses at all design reviews starting with the PDR. Presentations shall include design trade study results and Worst Case Analyses results impacting design or risk decisions.

4.4.5 Reliability Assessments and Predictions

The developer shall perform comparative numerical reliability assessments and reliability predictions in accordance with *DID 4-7* to:

- a. Evaluate alternative design concepts, redundancy, and part selections.
- b. Identify design elements that impact system reliability.
- c. Identify potential mission limiting elements and components that will require special attention in part selection, testing, environmental isolation and special operations.
- d. Evaluate designs in terms of mission success requirements.
- e. Evaluate reliability impacts of proposed engineering change and waivers.

The developer shall describe the level of detail of a model suitable for performing the intended functions enumerated above. The developer shall provide assessments and updates to GSFC for information under the SOW or Reliability Program Plan. The developer shall report results of reliability assessments at design reviews, beginning with PDR. The developer shall address in the report and design review presentations the design trade studies and reliability prediction results impacting design or risk decisions.

4.4.6 Software Reliability

Refer to Section 5.2 for Software Reliability requirements.

4.5 Reliability Analysis of Test Data

The developer shall fully utilize test information during the normal test program to assess reliability performance and identify potential or existing problem areas.

4.5.1 Trend Analyses

The developer shall assess all subsystems and components to determine measurable parameters that relate to performance stability. The developer shall monitor selected parameters for trends starting at component acceptance testing and continuing during the system integration and test phases. The developer shall ensure monitoring is accomplished within the normal test framework; i.e., during functional tests and environmental tests. The developer shall establish a system for recording and analyzing the parameters as well as any changes from the nominal (even if

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

the levels are within specified limits). The developer shall maintain and submit a list of subsystem and components to be assessed, parameters to be monitored, and trend analysis reports under the SOW or the Reliability Plan (DID 4-8.) The developer shall provide a list of parameters to be monitored at the CDR. The developer shall provide trend analysis reports at the Pre-Environmental Review (PER) and Flight Readiness Review (FRR).

4.5.2 Analysis of Test Results

The developer shall analyze test information, trend data and failure investigations to evaluate reliability implications. The developer shall document identified problem areas, and ensure developer management takes corrective action. The developer shall include this information in progress reports to the Project, or in a separate monthly report. The developer shall report results of analyses at design reviews. The developer shall address in the report design trade studies and reliability prediction results impacting design or risk decisions.

4.6 Limited-Life Items

The developer shall provide a plan to identify and manage limited-life items (DID 4-9). The developer shall submit the Limited-Life Items Plan for approval under the SOW. In the plan, the developer shall define limited-life items, the impact on mission parameters, responsibilities for mitigating limited-life items, and provide a list of limited-life items, including data elements as follows:

Expected life.

Required life.

Duty cycle.

Rationale for selection.

The useful life period starts with fabrication and ends with the completion of the final orbital mission.

The developer shall list limited-life items including selected structures, thermal control surfaces, solar arrays and electromechanical mechanisms. The developer shall consider atomic oxygen, solar radiation, shelf-life, extreme temperatures, thermal cycling, wear and fatigue to identify limited-life thermal control surfaces and structure items; the developer shall include mechanisms such as batteries, compressors, seals, bearings, valves, tape recorders, momentum wheels, gyros, actuators and scan devices when aging, wear, fatigue and lubricant degradation limit their life.

The developer shall maintain records allowing for evaluation of cumulative stress (time and cycles) for limited-life items, starting when useful life is initiated, and indicating the project activity that stresses the items.

The developer shall obtain a program waiver approval by GSFC when the use of an item whose expected life is less than its mission design life.

4.7 Control of Sub-Developers and Suppliers

The developer shall ensure that system elements obtained from sub-developers and suppliers meet project reliability requirements. All subcontracts shall include provisions for review and evaluation of the sub-developers' and suppliers' reliability efforts by the prime developer at the prime developer's discretion, and by GSFC at its discretion. The developer shall tailor the reliability requirements of this document in hardware and software subcontracts for the project. The developer shall exercise necessary surveillance to ensure that sub-developer and supplier reliability efforts meet overall system requirements.

The developer shall ensure the tailored requirements:

- Incorporate quantitative reliability requirements in subcontracted equipment specifications.
- Assure that sub-developers have reliability programs that are compatible with the overall program
- Review sub-developer assessments and analyses for accuracy and correctness of approach.

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

DIRECTIVE NO. 300-PG-7120.2.2E

Page 29 of 172

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

- Review sub-developer test plans, procedures and reports for correctness of approach and test details.
- Attend and participate in sub-developer design reviews.
- Ensure that sub-developers, during the project operational phase, comply with the applicable system reliability requirements.

4.8 Reliability of Government Furnished Equipment

When the overall system includes components or other elements furnished by the Government, the developer shall be responsible for identifying and requesting from the Project Office adequate reliability data on the items. The developer shall use the reliability data provided by the Project Office to perform the reliability analyses. The developer shall formally notify the Project Office promptly when examination of the data or testing by the developer indicates that the reliability or maintainability of Government Furnished Equipment is inconsistent with the reliability requirements of the overall system.

4.9 Maintainability

Maintainability requirements have been removed from this handbook. Projects needing specific maintainability requirements will contact OSSMA Code 302 for assistance in developing maintainability requirement. The degree of maintainability analysis and assessment performed for a program or project should be relative to the anticipated need and ability, to perform maintenance. The ability to perform maintenance on-orbit is either a well-planned activity (as in the case of a Hubble Space Telescope (HST) servicing mission), or does not exist (as in the case of an ELV launched spacecraft). However, maintainability needs to be considered for ground systems, and for flight hardware maintenance activities that may arise during Integration & Test (I&T) (as in the case of replacing a flight battery, or repairing a solar array).

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

Chapter 5. Software Assurance Requirements

The Systems Assurance Manager (SAM) shall ensure that software assurance processes and products are addressed in applicable mission assurance requirements. Software assurance shall be addressed in the developer's QMS, system safety, reliability, maintainability, and risk management programs. These software assurance requirements may be specified in the SOW or reference documents such as a Mission Assurance Requirements document. All disciplines of Software Assurance shall be addressed; however, tailoring is acceptable commensurate with the size of the development team, size and complexity of the software, the amount of software reuse, and the criticality of the software.

5.1 GENERAL

[Note: If subcontractors are part of the development process, state the following up front.] For the purposes of Section 5, all references to the developer shall include the prime software developer, as well as any subcontractors tasked in the development process.

5.1.1 Software Assurance

The developer's Software Assurance program shall address software assurance disciplines (i.e., Software Quality, Software Safety, Software Reliability, Verification and Validation, and Independent Verification and Validation) and functions for all flight and ground system software. The software assurance program shall apply to software and firmware developed under this contract, including Government off-the-shelf (GOTS) software, modified off-the-shelf (MOTS) software, and commercial off-the-shelf (COTS) software when included in a NASA system.

The developer shall identify a person responsible for directing and managing the Software Assurance Program (e.g., a software assurance manager). The developer shall prepare and maintain a Software Assurance Plan that meets the intent of DID 5-1 and the Institute of Electrical and Electronics Engineers (IEEE) Standard 730, "Software Quality Assurance Plans". For smaller projects, this plan may be incorporated in another planning document (e.g., the Software Management Plan).

The developer shall also plan and document software roles and responsibilities, software development processes and procedures, software reviews, software tools, resources, schedules, and deliverables throughout the development life cycle in a Software Management Plan, see DID 5-2. The developer shall document and maintain under configuration control all software requirements in a Software Requirements Specification, see DID 5.5.

5.1.2 Software Quality

The developer shall implement a Software Quality program to assure the quality of the software products and software processes. The software quality discipline shall plan and conduct process and product assurance activities throughout the development life cycle.

Product assurance activities shall be performed to assure: *(choose activities)*

1. Standards and procedures for management, software engineering and software assurance activities are defined.
2. All plans (e.g., Configuration Management, Risk Management, Software Management Plan) required by the contract are documented and comply with contractual requirements.
3. Standards, design, and code are evaluated for quality and issues.
4. All software requirements are documented and traceable from system requirements to design, code and test (i.e., a software requirements traceability matrix).

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

5. Software requirement verification status is updated and maintained via a software requirements verification matrix.
6. Formal and acceptance-level software tests are witnessed to assure satisfactory completion and maintenance of test artifacts.
7. Software products and related documentation (e.g., Version Description Documents and User Guides) have the required content and satisfy their contractual requirements.
8. Project documentation, including plans, procedures, reports, schedules and records are reviewed for impact to the quality of the product.
9. Software quality metrics are captured, analyzed, and trended to ensure the quality and safety of the software products.

Process assurance activities shall be performed to assure: *(choose activities)*

1. Management, software engineering, and assurance personnel adhere to specified standards and procedures and comply with contractual requirements.
2. All plans (e.g., Configuration Management, Risk Management, Software Management Plan) and procedures are implemented according to specified standards and procedures.
3. Contract requirements are passed down to any subcontractors, and that the subcontractor's software products satisfy the prime developer's contractual requirements.
4. Engineering peer reviews (e.g., design walkthroughs and code inspections) and software milestone reviews are conducted and action items are tracked to closure.
5. A software problem reporting system and corrective action process is in place and provides the capability to document, search, and track software problems and anomalies.
6. The software is tested to verify compliance with functional and performance requirements.
7. Software safety processes and procedures are followed.

5.1.3 Software Safety

NOTES to SAM on what's safety critical: *Software safety is a systematic approach to identifying, analyzing, tracking, mitigating and controlling software hazards and hazardous functions (data and commands) to ensure safer software operation within a system. It ensures that safety issues related to software are addressed in reviews and that specific safety analyses and tests are performed that consider specific software safety issues and potential hazards. While much of software safety depends on a good software development process and the overall software assurance activities, software safety is specifically concerned with those features of the software whose failure could impact safety.*

Any software that has the potential to cause a hazard or is required to support control of a hazard, as identified by safety analyses, is safety critical software. Software in a system that monitors, controls, interfaces with directly, or is resident in a processor handling critical or hazardous system functions is deemed software safety critical. Non-safety-critical software may become safety critical if it can impact safety-critical software resident with it (i.e., on the same machine or network). Other safety-critical software performs analyses or "crunches numbers" that will be used with, or for, safety-critical equipment or by an operator to make safety critical decisions. If the software does not meet any of the above criteria, then it is probably not safety critical.

The developer shall conduct a Software Safety program that is integrated with the overall software assurance and systems safety program and is compliant with the software safety requirements of NASA-STD-8719.13. The developer shall document their approach to the Software Safety program in the System Safety Program Plan (see [DID 3-1](#)) or the Software Management Plan (see [DID 5-2](#)), as appropriate. The developer shall ensure that software

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

safety requirements are clearly identified, documented, traced and controlled throughout the lifecycle. In cases, where the developer cannot meet a software safety requirement and/or feels that it is not in the best interest of the project to implement, the developer shall document these items in a deviation/waiver package. The developer shall furnish this deviation/waiver package to the customer for review/disposition.

For software deemed software safety critical, the developer shall identify and document the software safety critical classification of each item in terms of criticality, severity, associated risks, and likelihood of occurrence. Software safety requirements shall also be clearly identified and distinguishable in the software requirements traceability matrix. The developer shall test all software safety critical components on actual hardware to ensure that the safety requirements were sufficiently implemented and that applicable controls are in place to verify all safety conditions.

The developer shall continually monitor, assess, and review the software development efforts for changes that may affect the safety critical classification of the software and as necessary update engineering analyses to reflect these changes.

5.1.4 Software Reliability

The developer shall conduct a Software Reliability program for incorporating and measuring reliability in the products produced by each process of the life cycle. The developer shall document their Software Reliability program in the Software Management Plan (see DID 5-2). The software reliability program shall be tailored to the appropriate level based upon criticality of the software to the mission, software safety criticality, software complexity, size, cost, consequence of failure, and other attributes. Items to be specifically addressed in the plan shall include the activities to be undertaken to achieve the software reliability requirements, as well as the activities to be undertaken to demonstrate that the software reliability requirements have been verified.

As part of the software reliability program, the developer shall collect, analyze, and track measures that are consistent with IEEE Standard 982.1-1988, IEEE Standard Dictionary of Measures to Produce Reliable Software. Measurements for evaluating reliability (e.g., defect density, mean-time-to-failure, and code complexity) shall be documented.

5.1.5 Verification and Validation

The developer shall plan and implement a Verification and Validation (V&V) program to ensure that software being developed or maintained satisfies functional, performance, and other requirements at each stage of the development process and that each phase of the development process yields the right product. To assist in the verification and validation of software requirements, the developer shall develop and maintain under configuration control a Software Requirements Verification Matrix. This matrix shall document the flow-down of each requirement to the test case and test method used to verify compliance and the test results. The matrix shall be made available to NASA upon request.

V&V activities shall be performed during each phase of the development process and shall include the following:

1. Analysis of system and software requirements allocation, verifiability, testability, completeness and consistency.
2. Design and code walkthroughs and/or inspections (i.e., engineering peer reviews).
3. Formal reviews.
4. Documented Test Plans and Procedures.
5. Test planning, execution, and reporting.

5.1.6 Independent Verification and Validation

When the IV&V discipline is required, the developer shall provide all information required for the NASA Independent Verification and Validation (IV&V) effort to NASA IV&V Facility personnel. This shall include, but

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

is not limited to, access to all software reviews and reports, contractor plans and procedures, software code, software design documentation, and software problem reporting data. Wherever possible, the developer shall permit electronic access to the required information or furnish soft copies of requested information to NASA IV&V personnel.

The developer shall review and assess all NASA IV&V findings and recommendations. The developer shall forward their assessment of these findings and recommendations to NASA IV&V personnel accordingly. The developer shall take necessary corrective action based upon their assessment and notify NASA IV&V personnel of this corrective action. The developer shall also notify NASA IV&V personnel of those instances where they chose not to take corrective action. A developer Point of Contact shall be assigned and available to NASA IV&V personnel, as required, for questions, clarification, and status meetings.

5.1 REVIEWS

5.1.7 Software Reviews

The developer shall conduct the following formal software reviews with GSFC personnel in attendance and/or on the review team:

1. Software Requirements Review (SWRR).
2. Preliminary Design Review (PDR).
3. Critical Design Review (CDR).
4. Test Readiness Review (TRR).
5. Acceptance Review (AR).

If software is addressed as part of the formal system-level reviews (e.g., SRR, PDR, or CDR), the developer shall adhere to the review criteria provided by the GSFC Systems Review Office (see Chapter 8).

The developer shall record and maintain minutes and action items from each review. The developer shall respond to Request for Actions (RFAs) and any action items assigned by the review panel and/or the project as a result of each review and provide a status of all action items and RFAs at subsequent software or system-level reviews.

5.1.8 Engineering Peer Reviews

The developer shall implement a program of engineering peer reviews (e.g., design walkthroughs or code inspections) throughout the software development lifecycle to identify and resolve concerns prior to formal system/subsystem level reviews. Peer review teams shall be comprised of technical experts with significant practical experience relevant to the technology and requirements of the software to be reviewed. These reviews shall be commensurate with the scope, complexity, and acceptable risk of the software system/product.

Action items or Requests for Action (RFAs) from engineering peer reviews shall be recorded, maintained, and tracked throughout the development lifecycle.

5.2 SOFTWARE CONFIGURATION MANAGEMENT

The developer shall develop and implement a Software Configuration Management (SCM) system that provides baseline management and control of software requirements, design, source code, data, and documentation. The developer shall document the SCM system, and associated tools, in a Software Configuration Management Plan, see DID 5-3 or the Software Management Plan (see DID 5-2). The plan shall address configuration identification, configuration control, configuration status accounting, and configuration audits and reviews.

As part of the SCM, the developer shall employ a source code version control tool (e.g., ClearCase, Starbase) that allows developers to check in/check out current or previous versions of a source file. The developer shall also use a

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

requirements management tool (e.g., DOORS) to manage the software requirements baseline. The developer shall document and implement a process for Software Problem Reporting and Corrective Action that addresses reporting, analyzing, and tracking software non-conformances throughout the development lifecycle.

5.3 GFE, EXISTING AND PURCHASED SOFTWARE

If the developer will be provided software or firmware as GFE, or will use existing or purchased software or COTS, the developer shall ensure that the software meets the functional, performance and interface requirements placed upon it. The developer shall ensure that the software meets applicable standards, including those for design, code and documentation, or shall secure a GSFC project waiver to those standards.

5.4 SOFTWARE ASSURANCE STATUS REPORTING

As part of the Project Monthly Status Reports, the developer shall include the following software assurance highlights (*choose status items*):

1. Organization and key personnel changes.
2. Assurance accomplishments and resulting software assurance metrics for activities such as, but not limited to, inspection and test, reviews, contractor/subcontractor surveys, and audits.
3. Subcontractor assurance accomplishments, including items listed above.
4. Trends in software quality metric data (e.g., total number of software problem reports, including the number of problem reports that were opened and closed in that reporting period).
5. Significant problems or issues that could affect cost, schedule and/or performance.
6. Plans for upcoming software assurance activities.
7. Lessons Learned.

5.5 NASA SURVEILLANCE OF SOFTWARE DEVELOPMENT

The developer shall allow NASA representatives and/or their designate/assignee to perform surveillance activities throughout the entire software development lifecycle. Insight/oversight activities shall include, but are not limited to the following:

1. The developer shall allow NASA representatives electronic access to their software problem reporting system remotely from GSFC.
2. The developer shall provide NASA representatives the necessary software documentation to perform their job (e.g., software management plans, software assurance plans, configuration management plans, design documentation)
3. The developer shall allow NASA representatives to review results and corrective action from process and product audits.
4. The developer shall allow NASA representatives to be present at any engineering peer reviews (e.g., code inspections) that NASA representatives deem appropriate. The NASA representative shall be allowed to submit RFAs or action items for developer consideration.
5. The developer shall allow NASA representatives to review the status of all RFAs and action items, as well as their resolution.

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

Chapter 6. Ground Data Systems Assurance Requirements

This chapter provides recommended Ground Data System (GDS) Assurance Requirements. GDS Assurance requirements for certain areas, such as, reliability and maintainability are specified in the Assurance Requirements for the specific area. These requirements should be tailored to meet the needs of the project.

Note: there exist various interpretations and sources of requirements for the development of GDS components. For some efforts, the GDS requirements will represent the entire set of requirements that the GDS must fulfill and will serve as the guiding force behind the entire development efforts (for example, a system requirements document for a level zero processing system/facility). However, in some cases, the GDS requirements may represent a subset of requirements, typically mission critical requirements, that are part of an overall set of requirements for a particular system (for example, only those mission critical requirements from a system requirements document for a level zero processing system/facility). This chapter attempts to provide assurance-requirements that cover both instances.

6.1 GENERAL

GDS components may include but are not limited to GDS software, firmware and hardware, ground support elements (simulators, etc), COTS, databases, key parameter and test checkout software, and any software developed under the project that is related to flight mission operations. These components may be developed in-house entirely by the developer, provided by a sub-developer/subcontractor to the developer, purchased by the government, purchased by the developer, or furnished by other parties including the government.

6.2 QUALITY MANAGEMENT SYSTEM

QMS related requirements are discussed in Chapter 2 of this document. It should be noted that the QMS shall be applied to the development and assurance functions for GDS components as well. In all cases the development effort shall provide evidence (quality records for GSFC review) as insight to the quality of the developing software, hardware and other GDS components as evidence of application of QMS processes, and as status of assurance problems, safety issues and organizational/personnel changes. Quality records shall include any corrective actions, relating to GDS development, recommended by QMS audits. The developer will allow NASA audits, when deemed necessary by the Project Manager, to assure compliance of the developer's QMS with ANSI/ISO/ASQ Q9001 and to assure that the QMS is applied to the contracted activities.

6.3 REQUIREMENTS

The developer shall identify, document and maintain GDS requirements that will serve as the basis of the development, implementation, operation and maintenance of the GDS and its components. These requirements may include but are not limited to functional, performance, reliability, maintainability, safety and test/verification requirements.

The developer shall review and analyze the GDS requirements to assure that they are consistent, clear, valid, feasible, compatible, complete, testable and do not include inappropriate level of design information. The developer shall work with GSFC and/or other entities as necessary to resolve any problems/issues associated with the GDS requirements.

The developer shall baseline the GDS requirements early in the development effort, specifically in conjunction with a formal requirement review. The developer shall maintain the GDS requirements under configuration control throughout the lifecycle. All changes to the GDS requirements, including those generated both internally and externally, shall be managed by the developer's Configuration Control Board (CCB) process and reviewed/approved as applicable by GSFC.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

6.4 REVIEWS

Formal reviews are discussed in Chapter 8 of this document.

The developer shall implement a program of engineering reviews (peer reviews) throughout the development lifecycle to identify and resolve concerns prior to formal, system level reviews. The developer shall plan for such engineering working-level reviews such that they are represented on the project's development schedule. For each engineering review, the developer shall identify and document the following:

- Review process.
- Required participants in the reviews.
- Specific criteria/requirements for successful completion.
- Artifact(s)/documentation required for the review.
- Review results.
- Describe how follow-up actions are documented, tracked and controlled.

6.5 ASSURANCE ACTIVITIES

Note: the assurance related activities mentioned throughout this section should be tailored to reflect the GDS and its associated components criticality, mission objectives and accepted level of risk. Tailoring should take into account the size, complexity, reusability, flexibility, portability, interoperability, safety-criticality, reliability, maturity, system compatibility, etc. of the GDS and its components.

The developer shall perform various assurance-related activities throughout the development lifecycle to ensure that the GDS and its components meet GDS requirements. The developer shall initiate these activities as early in the development lifecycle as possible, specifically in the concept phase, and continue these activities into the operations and maintenance phase where applicable. Some of these assurance-related activities are applicable to all phases of the lifecycle and the developer shall conduct these activities throughout the entire lifecycle. These activities include but are not limited to the following:

- Planning, Tracking and Oversight.

6.5.1 Concept Phase

Specific assurance-related activities that the developer shall perform during the concept phase include but are not limited to the following:

- Tradeoff and evaluation studies and/or prototyping efforts to provide insight into the feasibility of GDS components meeting the operational concept, constraints and preliminary requirements.
- Define and document criteria used to perform tradeoff and evaluation studies and maintain all results from these studies for GSFC review.
- Participation in a system requirements reviews.

6.5.2 Requirements Phase

In addition to the activities mentioned above, specific assurance-related activities that the developer shall perform during the requirements phase include but are not limited to the following (note: some of these activities may be performed prior to this phase or subsequent to this phase where applicable):

- Analyze and refine the requirements to assure they are consistent, clear, valid, feasible, compatible, complete, testable and do not include inappropriate level of design information.

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

DIRECTIVE NO. 300-PG-7120.2.2E

Page 37 of 172

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

- Ensure requirements are generated, analyzed, refined, decomposed and allocated to appropriate GDS components through the use of a systems analysis and allocation process. This process shall be used to verify requirements are correct and complete at each level prior to further allocation and decomposition, and to verify them for feasibility and top-level design concept prior to further allocation.
- Document trade studies and analyses performed to aid in deciding which requirements to allocate to hardware, software and other components. When a system-level requirement is allocated to more than one configuration item (CI), a process is used to assure that the lower-level requirements taken together satisfy the system-level requirement.
- Establish functional, performance, safety, reliability, maintainability and test/verification requirements for each incremental system (delivery/build) as applicable. This process should assure all requirements are allocated to planned increments prior to the design and development of the increment.
- Ensure that the systems analysis and allocation methodology is compatible with other methodologies adopted on the project.
- Manage allocation of new and additional requirements between hardware, software and other components by a change review and control process; and manage the reallocation of existing requirements between hardware, software and other components by a change review and control process.
- Use a defined process to generate, review and allocate interface requirements.
- Maintain a process to provide, ensure and maintain two-way requirements traceability from system specifications to hardware, software and other components that serve as configuration items. This requirement traceability shall be established and documented as early in the lifecycle as possible.
- Generate, document and maintain a requirements verification matrix.
- Conduct a requirement review and at the end of each phase of the development process to ensure requirements are complete and testable.

6.5.3 Design Phase

Specific assurance-related activities that the developer shall perform during the design phase include but are not limited to the following (note: some of these activities may be performed prior to this phase as applicable):

- Select and document an engineering development lifecycle model consistent with the program requirements and needs. The rationale for selecting the lifecycle development models and methods shall be recorded and maintained.
- Establish and maintain the computer system architecture (hardware, software and other components), for determining the nature and number of the configuration items, and for maintaining traceability of the architecture to requirements. This process shall define the relationships between GDS architecture components (hardware, software, etc) including the system-level component hierarchy and control structure and the operational (human) interface as applicable.
- Maintain a process to define, maintain, and document interfaces (both internal and external) within the architecture.
- Evaluate how suitable the GDS architecture is for implementing all of the requirements, as well as how the design constraints are satisfied. The developer shall identify, document and maintain criteria used to perform any architecture evaluations. Suitable development/project personnel shall participate and support these evaluation efforts.
- Evaluate the design based on the use of risk reduction techniques, such as the creation of models and prototypes (proofs, benchmarks) as necessary.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

- Periodically reassess the adequacy of the GDS architecture over the development cycle. The developer shall identify, document and maintain criteria that are used to provide data to determine whether to stay with the original design or change.
- As requirements change, perform a review of the GDS architecture design for flexibility to adapt to new requirements, and (as necessary) updates, the ground data system architecture design.
- Review all architectural changes and their impact on design margins (such as memory, throughput, bus loading and data latency) as well as cost and schedule baselines prior to implementation. Any proposed change to the GDS architecture design shall be subject to GSFC review/approval.
- Document and maintain the rationale of all major systems engineering decisions and where applicable implement a process to arbitrate contention across trade-off studies for utilization of system-level resources and reserves.
- Conduct reviews and appropriate tests at the end of each phase of the development process to ensure that the requirements have been correctly implemented into design, code, documentation and data.
- Allocate and maintain traceability between the GDS architecture/components and the GDS requirements.
- Conduct design walkthroughs and reviews.

6.5.4 Implementation Phase

Specific assurance-related activities that the developer shall perform during the implementation phase include but are not limited to the following (note: some of these activities may be performed prior to this phase as applicable):

- Define and document the components of each build, delivery and/or release.
- Conduct peer reviews/walkthroughs for code.
- Conduct unit testing.
- Conduct reviews and appropriate tests at the end of this phase of the development process to ensure that the requirements have been correctly implemented into design, code, documentation and data.
- Allocate and maintain traceability between the GDS architecture/components and the GDS requirements.
- Conduct configuration reviews, Functional Configuration Audits (FCAs) and Physical Configuration Audits (PCAs) to define, document and ensure the configuration of the GDS and its components.

6.5.5 Testing Phase

Note: the testing phase may be comprised of various types of testing including but not limited to unit testing, integration & test, system level, acceptance test, interface, end-to-end, compatibility testing, data flow testing, regression testing and operational readiness testing. Unit testing, integration & test, and system level testing are typically performed solely by the developer with some level of oversight by an independent entity. Acceptance test, interface, end-to-end, compatibility testing, data flow and operational readiness testing are typically performed with support by other entities including other ground data system elements (Mission Operations Center (MOC), data processing facilities, end-user facilities and the appropriate network elements) in order to fully demonstrate operational compatibility and the ability of the entire system to perform as required during the mission.

Specific assurance-related activities that the developer shall perform during the test phase include but are not limited to the following (note: some of these activities may be performed prior to this phase as applicable):

- Plan for and document test related activities early in the development stages of the project in a test plan(s). As necessary, a separate test plan may be required for each of the various types of testing mentioned above. The plan shall be maintained under configuration control and updated as requirements are changed. All test plans

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

DIRECTIVE NO. 300-PG-7120.2.2E

Page 39 of 172

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

shall be made subject to GSFC review and approval as applicable. The developer's test plans shall include but is not limited to the following:

- Number of system builds planned and when they will occur.
- Description of the tests to be performed including the different levels of testing (from units to Computer Software Configuration Items (CSCIs) to subsystem to system-level test), expected test results, personnel responsible for testing, any required support from other organizations and data required for the test(s).
- GDS components to be tested
- Test environment under which the test(s) will be conducted including test facility requirements, special test support tools (i.e., simulators, emulators, etc.) and any special operating conditions required.
- Requirements Verification Matrix (RVM) documenting traceability of requirements to test cases.
- Generate test procedures that implement the test plans and facilitate the verification and validation of GDS requirements. All test procedures shall be made subject to GSFC review and approval as applicable.
- Maintain a process to ensure that any test tools and test data are qualified prior to use during testing activities.
- Ensure that test personnel attend and participate as necessary in various reviews throughout the lifecycle, to include but not limited to requirements, architecture and design reviews.
- Identify and document test readiness criteria for both formal and informal testing activities. Test criteria shall be made subject to GSFC review and approval as applicable.
- Maintain and update the RVM generated earlier in the lifecycle to include the status (pass, fail, deferred, etc) of each requirement throughout the testing phases and various testing activities.
- Document all test results in a test report. Test reports should document the validation of requirements, specific tests completed, conformance of the test results to the expected results, the number, type and criticality of any identified discrepancies/nonconformances, identification of the hardware, software and other GDS components tested including version number, etc.
- Define and document a transition process/plan to progress from the test environment to the operations and maintenance environment.
- Document all defects/nonconformances encountered during the testing activities. These defects/nonconformances shall be assessed for criticality, severity, impact, etc to determine appropriate action and resolution. The developer shall track and report on the status of all defects/nonconformances.
- Identify all nonconformances that impact the developer's ability to meet GDS requirements and document these items in a waiver, which must be reviewed/approved by GSFC as applicable.
- Ensure an independent entity, either internal or external QA representatives/personnel, witness all testing activities as appropriate.
- Ensure and maintain configuration control of the test environment including hardware, software, simulators, test data, databases and other components throughout the test program.
- Assess all changes made to the system architecture and its components to determine the necessity for regression testing. The developer shall conduct regression testing based upon assessed and approved/implemented changes as appropriate.
- Conduct abnormal/erroneous condition testing as appropriate.
- Maintain a process for determining the level of test for safety critical GDS components. The developer shall develop test procedures to ensure that all safety critical GDS components are tested at and beyond the systems

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

limits, with abnormal/erroneous conditions, as well as all transition points (e.g., mode to mode). The developer shall execute these test procedures for all safety critical GDS components.

- Conduct reviews and appropriate tests at the end of each phase of the development process to ensure that the requirements have been correctly implemented into design, code, documentation and data.
- Conduct pre-test briefings and generate briefing messages where appropriate to facilitate the coordination of various test related activities. Briefing message contents may include but are not limited to:
 - Test Case/Procedure Name/Number
 - Purpose of the Test
 - Testing Dates/Times
 - Test Participants and required resources (scheduling of lab and station support, data sources (e.g. s/c, s/c data tape, engineering test unit or s/c simulator), software, hardware and support system configurations (to include release/version numbers where appropriate).
 - GDS requirements to be verified.
 - Contact list to include names and numbers of test participants
- Conduct post-pass and post-test debriefings. During these debriefs, the developer shall summarize test results, disposition the test (pass/fail, etc), deviations from test procedures, requirements verified and discrepancy reports generated, etc.
- Conduct mission simulations to validate nominal and contingency mission operating procedures and to provide for operator familiarization training. In order to provide ample time for checkout of operational configurations, it is considered essential that users participate in mission simulations.
- Conduct reviews and appropriate tests at the end of each phase of the development process to ensure that the requirements have been correctly implemented into design, code, documentation and data.

6.5.6 Operations and Maintenance Phase

Specific assurance-related that the developer shall perform during the operations and maintenance phase include but are not limited to the following (note: some of these activities may be performed prior to this phase as applicable):

- Generate and deliver to GSFC formal acceptance data delivery packages identifying the contents of the delivery and any associated metadata/artifacts describing the delivery and its contents.

For those GDS instances where hardware is delivered, contents of the data delivery package shall include but is not limited to the following information:

- a. As-Built configuration list.
- b. List of parts used.
- c. List of materials and processes used.
- d. Test logbook including total operating time and cycle records.
- e. List of open items (i.e., nonconformances, etc) with reasons for items being open and appropriate authorization/approvals/waivers.
- f. Listing and status of all identified Limited-Life items.
- g. Trend data.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

- h. Test results and verification success criteria.
- i. Known problems and workarounds.
- *For those GDS instances where software is delivered, contents of the data delivery package shall include but is not limited to the following information:*
 - a. Software Delivery Letter.
 - Description of delivery contents
 - Build instructions.
 - Special operating instructions.
 - List of resolved anomaly reports and change requests.
 - List of unresolved anomaly reports and change requests.
 - Copy of resolved anomaly reports and change requests.
 - Copy of unresolved anomaly reports and change requests.
 - Matrix of requirements addressed by this release, including waivers for those requirements not met as appropriate.
 - Release history summary matrix.
 - Inventory of the delivered media.
 - List of changes to documentation associated with this release.
 - Verification success criteria
 - Known problems and workarounds.
 - b. Software Delivery Media.
 - c. Accompanying Documentation

6.5.7 Activities Performed throughout the Lifecycle

6.5.7.1 Planning, Tracking and Oversight

- The developer shall define and document a Management Program to include planning, tracking and oversight activities for the project/program in a development plan, see DID 5-1 for guidance.
- The developer shall ensure that periodic and appropriate coordination among developers, acquisition organizations, users, maintainers, testers, QA and customers, regarding user needs, acquisition organization resources, technology status, and GDS requirements occurs throughout the development lifecycle.
- The developer shall ensure and maintain a system engineering process (as appropriate) that emphasizes an integrated product development approach. This approach shall define systems engineering interfaces with other engineering interfaces and disciplines with the development activities, as well as the interfaces between the system and subsystem developers and/or subcontractors/COTS vendors. The developer shall ensure and maintain a process to manage, provide an escalation path for, and resolve conflicts regarding intergroup issues, including system-level issues that arise internally or with subcontractors/COTS vendors. The developer shall identify and track critical dependencies between development groups participating in development activities.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

- The developer shall utilize support tools that are compatible with other tools used by other project members to facilitate the communication, exchange and sharing of data.
- The developer shall identify and select metrics to be collected and analyzed on a routine basis to ensure development and management activities are proceeding per customer requirements. Metrics shall be based upon the program's defined system engineering process.
- The developer shall define the specific measurement data to be collected, their precise definitions, the intended use and analysis of each measurement and the process control points at which they will be collected and reported.
- The developer shall identify and maintain requirements for metrics, define variance thresholds, which when exceeded require corrective actions.
- The developer shall ensure that the measurement program is integrated with the program's development process across the lifecycle and any teaming/subcontracting arrangements.
- The developer shall maintain a quality plan that serves as the basis for the project's activities for quality management. The quality goals for the GDS and its associated components shall be defined, monitored, and revised throughout the lifecycle. Quality goals shall be allocated appropriately to the subcontractors delivering products and/or GDS components to the project whenever applicable.
- The project's quality plan shall contain provisions to ensure that quality is built into the GDS and its associated components. The plan shall identify points in the lifecycle process where quality is measured. The plan shall identify methods for analyzing quality measurements, for evaluating whether they meet customer's needs, and for determining the necessary corrective actions.
- The developer shall maintain/possess a QA organization/entity that is assigned the responsibility to monitor the development process, and the associated components/products. QA shall interface with all relevant disciplines participating in the lifecycle activities including engineering, configuration management and testing. The QA group is empowered to effect changes to the program when quality goals are not being met.
- The developer shall follow a written QA plan for measuring and monitoring the performance of the program's defined management and development processes. The developer shall verify adherence to the defined development and management processes. The developer shall perform audits on designated work products to verify compliance with quality goals, and adherence to the applicable standards and requirements.

6.6 GFE, COTS, EXISTING AND PURCHASED SOFTWARE

- If the developer will be provided software as GFE, or will use existing or purchased software and/or COTS products, the developer is responsible for these components meeting all functional, performance and interface requirements.
- The developer shall be responsible for ensuring that these components meet all applicable standards, including those for design, code and documentation, or for securing a GSFC project waiver to those standards.
- The developer shall be required to submit documentation providing indication of suitability for use and compliance to all applicable requirements and standards.
- Any significant modification to these components shall be subject to all of the provisions of the developer's QMS and the provisions of this document. Significant modification will be defined by the project and its CCB procedures and will be subject to GSFC review.

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

DIRECTIVE NO. 300-PG-7120.2.2E

Page 43 of 172

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

6.6.1 COTS Management

- The developer shall identify and maintain traceability of GDS requirements satisfied by COTS products/components.
- The developer shall conduct trade studies to identify potential COTS products that may meet GDS requirements.
- The developer shall identify and maintain criteria for COTS selection.
- The developer shall document the rationale/justification for the selection of all COTS components contained within the GDS.
- The developer shall maintain a CM program for all COTS products/components of the GDS.
- The developer shall maintain a COTS management plan for all COTS products/components of the GDS.
- The COTS management plan shall include and address the adequacy of existing COTS products/components in meeting or exceeding GDS requirements, processes utilized to ensure COTS updates/upgrades are routinely assessed and implemented based upon a documented criteria, etc.
- The developer shall demonstrate and document the fulfillment of GDS requirements by COTS products/components via the RVM.

6.7 REUSE REQUIREMENTS

Note: for some GDS development efforts, the use of reusable components may be desired to contain/save costs, leverage existing technologies/components/products, etc.

- The developer shall maximize future reuse potential of new developed system and software components within the constraints of the system cost, schedule and performance baselines.
- The developer shall identify, assess and document lifecycle impact of reuse-related decisions, including the choice of computer languages, processors, architectures, environments, the development of reusable assets and the maintenance of re-use repositories.

6.8 DEFECT PREVENTION REQUIREMENTS

- The developer shall develop and maintain a program/plan for defect prevention activities.
- The developer's program/plan shall at a minimum, include identification of defect causes and assessments for potential process improvement opportunities. The developer shall conduct causal analysis meetings as appropriate. Data on defects as identified in peer reviews, document reviews and testing shall be collected and analyzed by the developer. The developer shall identify, prioritize and systematically eliminate common causes of defects based upon their defect prevention program/plan.
- The developer shall revise development and management processes as a result of defect prevention actions as applicable.
- The developer shall document and track defect prevention data across entities coordinating defect prevention activities. The developer shall provide feedback on the status and results of the organization and program's defect prevention activities to project personnel on a periodic basis.

6.9 DATABASES

- The developer shall maintain a process and procedures for database development. The process shall include activities such as internal reviews, walkthroughs, statusing, test and discrepancy resolution.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

- The developer shall ensure that the database development processes and procedures are compatible with the selected database methodology.
- The developer shall utilize a process for the verification and validation of the database system.
- The developer shall ensure that system/software releases and database releases are configured with one another.
- The developer shall test the interface between the software and Database Management System (DBMS) tested.
- The developer shall implement CM on the database system to ensure that the database release version is defined and documented, controlled and that the integrity of the data contained within is controlled.
- The developer shall ensure that appropriate security measures are implemented on the database system and on the data contained within the database system.

6.10 SECURITY ASSURANCE

- The developer shall conduct a security program to identify and mitigate security risks associated with the GDS and its components. All security risks shall be assessed/analyzed for impact and likelihood of occurrence.
- The security program shall ensure that security requirements are established, documented and implemented during all phases of the software lifecycle. Security tasks and activities shall include the addressing of security concerns during reviews, analyses, inspections, testing and audits.
- The developer shall identify and characterize system security vulnerabilities to include analyzing GDS assets/components, defining specific vulnerabilities, and providing an assessment of the overall system vulnerability.
- The developer shall identify and report upon all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security.
- The developer shall ensure that solutions are verified and validated with respect to security.
- The developer shall be compliant with all NASA security related policies, procedures, standards and guidelines as appropriate.

6.11 ELECTROMAGNETIC COMPATIBILITY CONTROL

For GDS components subject to electromagnetic compatibility problems, the developer shall submit an Electromagnetic Compatibility Control (EMC) test plan in accordance with the contract schedule that identifies an overall implementation of an effective EMC test program. The test plan shall include test requirements that will assure compatibility within each element, within the project as a whole, and within the project's facilities. It shall describe any special testing requirements and the content of EMC sections of applicable Interface Control Documents (ICDs). The EMC test plan and the activities described within it shall comply with the requirements found in MIL-STD-461, "Electromagnetic Emission and Susceptibility Requirement for Control of Electromagnetic Interference", as applicable.

6.12 RELIABILITY AND AVAILABILITY

Note: the requirements below, along with those in Chapter 4, should be used as inputs to develop estimated spare parts requirements and related parameters, including maintenance manpower requirements, preventive maintenance policy, facility requirements and level or repair analysis.

Reliability and availability assurance requirements for the GDS and associated components shall include the following:

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

- The developer shall define, measure, control and report on reliability in all lifecycle phases as appropriate. The developer shall implement corrective actions whenever reliability related requirements are not being satisfied.
- The developer shall allocate basic reliability and mission reliability requirements to the GDS architecture component level (at which failures are postulated), necessary to identify redundancy. The developer shall ensure that reliability requirements are used to establish baseline requirements against which the design alternatives are evaluated. Requirements consistent with the allocations shall be imposed on any subcontractors, suppliers and/or COTS vendors whenever appropriate.
- The developer shall assure that equipment and components obtained from subcontractors, suppliers and/or COTS vendors meet allocated requirements and if not, such deficiencies shall be report to GSFC.
- The developer shall develop reliability predictions for the GDS and its components. These models and predications shall reflect applicable experience from previous projects and/or similar GDS components and shall be revised/maintained throughout the lifecycle as pertinent data becomes available. These models shall be documented, accessible for GSFC review and used continually throughout the design process. These reliability models shall be used to augment system engineering tradeoff studies. Appropriate prediction techniques are described in Chapter 4.
- The developer shall develop and document analyses to determine possible modes of failure and their effects on the GDS and its components. Appropriate analysis techniques are described in Chapter 4.
- The developer shall perform reliability evaluation on the GDS and its components via the collection of failure and time data throughout the lifecycle. Appropriate evaluation techniques are described in Chapter 4.

6.12.1 Reliability Acceptance Testing

The GDS and/or its components shall be subjected to a failure free acceptance test by government personnel and its representatives, as required. The length of the test will be as specified in the contract; for example, in the range from 300 to 1,000 hours. The developer shall provide the resources to create the test software, hardware and test data; as well as support testing operations, analyze results and make corrections as required.

The general guidelines to be followed include the following:

- a. The developer shall certify in writing that the system is installed and ready to use, and shall provide documentation of a successful system checkout performed which demonstrates that the system, including hardware and software components, is in an acceptable operating condition. The system will then be turned over for testing by an Acceptance Test team.
- b. If the equipment operates failure free in accordance with the specification during the specified performance period the equipment shall be deemed to have met the standard of performance.
- c. If a failure occurs, the test shall be terminated and the developer shall be responsible for determining the cause of the failure. The equipment shall then be returned to working condition and resubmitted for test.
- d. If the equipment fails to meet the standard of performance after the specified number of attempts, because of recurring failures, the Technical Officer may, at his option, notify the Contracting Officer to require a replacement of said equipment or to terminate the contract in accordance with the provisions of the default clause of this contract.
- e. Operational use time for equipment is defined as the accumulated time during which the unit(s) is (are) in actual operation, including any interval of time between the start and stop of the central processing unit(s).
- f. In addition to any diagnostic programs provided by the developer, the government may use additional test programs developed by the team with technical assistance from the developer, as required.

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

The developer shall provide test procedures and test reports in accordance with the contract schedule. The test procedures shall make full use of benchmark and standard system diagnostics to verify compliance to performance requirements including interfaces. Documentation on how to run the test(s) and interpret the results will be specified in the procedures.

6.13 MAINTAINABILITY REQUIREMENTS

Note: maintainability engineering includes a process for establishing design requirements and a number of engineering tasks that rate a part of the systems engineering process. These tasks focus primarily on the form, fit and function of the design that will allow for practical and economical maintenance within established project constraints. The requirements below, along with those in Chapter 4, should be used as inputs to develop estimated spare parts requirements and related parameters, including maintenance manpower requirements, preventive maintenance policy, facility requirements and level of repair analysis.

Maintainability assurance requirements for the GDS and associated components shall include the following:

- The developer shall define and evaluate the effort, cost and equipment required to support/maintain the GDS and its components.
- The developer shall define, measure, control and report on maintainability in all lifecycle phases as appropriate. The developer shall implement corrective actions whenever maintainability related requirements are not being satisfied.
- The developer shall allocate maintainability requirements to the GDS architecture component level as appropriate. The developer shall ensure that maintainability requirements are used to establish baseline requirements against which the design alternatives are evaluated. Requirements consistent with the allocations shall be imposed on any subcontractors, suppliers and/or COTS vendors whenever appropriate.
- The developer shall assure that equipment and components obtained from subcontractors, suppliers and/or COTS vendors meet allocated requirements and if not, such deficiencies shall be report to GSFC.
- The developer shall develop maintainability predictions for the GDS and its components. These models and predications shall reflect applicable experience from previous projects and/or similar GDS components and shall be revised/maintained throughout the lifecycle as pertinent data becomes available. These models shall be documented, accessible for GSFC review, and used continually throughout the design process. These maintainability models shall be used to augment system engineering tradeoff studies. Appropriate prediction techniques are described in Chapter 4.
- The developer shall perform maintainability evaluation/demonstration tests on the GDS and its components to verify that all preventive and corrective maintenance activities, such as system and data level backups, can be successfully executed. Maintainability demonstration shall be conducted in the operational environment as available, or an environment that duplicates the operational environment as closely as possible. To the maximum extent possible, operators, technicians, system and/or database administrators of the system shall perform the maintenance actions during the maintainability demonstration.

6.14 SYSTEM SAFETY

Note: the objective of the safety program is to verify that the operation of the GDS and its components will not endanger life, property and/or adversely affect the operation of other GDSs or supported flight platforms. System safety is defined as the application of engineering and management principles, criteria and techniques to optimize safety within the constraints of operational effectiveness, time and cost throughout all phases of the system lifecycle. Refer to Chapter 3 for additional information pertaining to system safety.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

- The developer shall initiate a safety program to identify and mitigate safety critical GDS components. If any GDS component(s) are identified as safety critical, the developer shall conduct a safety program on those components in compliance with NPG 8715.3, "NASA Safety Manual".
- For GDS components that are software and deemed as safety critical, the safety program shall be implemented in accordance with NASA-STD-8719.13 "NASA Software Safety Standard". *See section 5.2.2 of this document for software safety related items.*
- The developer shall establish and identify procedures and instructions, which will be used to execute all system safety analyses. The developer shall perform system safety analyses assuring that:
 - a. Safety is designed into the product; known hazardous conditions that cannot be eliminated through equipment design or operational procedures are controlled or reduced to an acceptable level. Residual hazards shall be tracked with their severity status and provided to NASA on a periodic basis.
 - b. Results of previous trade studies and analyses are considered.
 - c. Other related analyses, such as Failure Modes and Effects and Criticality Analysis (FMECA), are considered to preclude duplication of analytical work.
- All safety-related analyses, studies and assessments shall be accessible for GSFC review.

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

Chapter 7. Risk Management Requirements

This chapter provides procedures and requirements for applying effective risk management to GSFC projects as required by NPR 7120.5, "Program and Project Management Processes and Requirements" and Goddard Procedures and Requirements document 7120.4 "Risk Management". CRM training, tools, techniques, and case studies as applied to NASA projects are available at <http://crm.nasa.gov>.

7.1 GENERAL

The developer shall implement an organized, systematic decision-making process for Continuous Risk Management (CRM) process to increase the likelihood of achieving program/project goals. The CRM process shall apply to all aspects of the program/project. This process shall identify, analyze, plan (for the handling of risks), track, control, communicate and document all project risks. The developer shall:

- a. Search for, identify, and document all project risks (before they become problems)
- b. Evaluate, classify, and prioritize all identified risks
- c. Plan and implement risk mitigation strategies, actions, and tasks (and assign appropriate resources)
- d. Track risks being mitigated, collect data to capture risk attributes and mitigation information, establish performance metrics, examine trends, and analyze deviations and anomalies
- e. Control risks by closeout, re-planning, contingency planning, or continued tracking and execution of the current plan
- f. Document risk information and communicate to all levels of the project
- g. Report on outstanding risk items at all management and design reviews

The developer shall implement a systems management approach that formalizes and integrates the CRM process throughout the system life cycle. All elements of the system shall be addressed (e.g., flight, ground and launch vehicle segments, hardware and software, critical ground support equipment). All phases of the life cycle shall be considered (e.g., fabrication, assembly, integration and test, environmental testing, transportation, launch site processing, launch deployment, in-orbit check out, operations decommissioning).

7.2 APPLICABLE DOCUMENTS

- a. GPR 1060.2 Management Review and Reporting for Programs and Projects
- b. GPR 8700.4 Integrated Independent Reviews
- c. GPR 7120.4 Risk Management
- d. NPR 8705.4 Risk Classification for NASA Payloads
- e. NPR 8705.5 Probabilistic Risk Assessment for NASA Programs and Projects
- f. NPR 7120.5 Program and Project Management Processes and Requirements
- g. NPR 8000.4 Risk Management Procedures and Guidelines
- h. NPR 8715.3 NASA Safety Manual

7.3 RISK MANAGEMENT PLAN

The project-specific implementation of the CRM process for each project shall be documented in a Risk Management Plan (RMP). The RMP shall be reviewed by the SAM, approved by the PM and concurred by the Office of Mission Success (Code-170). The RMP shall be developed, approved and implemented early in project

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

formulation, no later than the mid-point of the planned formulation period and prior to any mid-formulation review gates imposed by the funding Enterprise (i.e., Office of Space Science Interim Confirmation Review). The RPM is a controlled document and shall be maintained by the PM throughout the project life cycle.

The developer shall document the project-specific implementation of the CRM process in a Risk Management Plan (RMP) in accordance with DID 7-1. Preparation of the RMP is a requirement established by the NPR 7120.5 and includes the content shown in NPR 8000.4, "Risk Management Procedures and Guidelines". The plan shall include risks associated with hardware and software (e.g., technical challenges, new technology qualification, etc), COTS, system safety, performance, cost and schedule (i.e., programmatic risks). The plan shall identify which tools and techniques will be used to manage the risks.

All identified risks shall be documented and reported in accordance with the project's RMP. Identified risk areas shall be addressed at project status reviews and at Integrated Independent Reviews (GPR 8700.4). Risk status shall be available to all members of the project team for review. Although not all risks will be fully mitigated, all risks shall be addressed with mitigation and acceptance strategies agreed upon at appropriate mission reviews.

7.4 PROBABILISTIC RISK ASSESSMENT

The implementation of the CRM process shall include the use of tools and methodologies to support the qualitative and quantitative assessment of risk inherent in the system design and associated development and operations activities. Risk assessments are conducted as part of the system design, analysis and trade study activities. The results of these risk assessments shall be used to support project management decisions with respect to safety and mission success, and programmatic commitments.

Comparative numerical reliability assessments and/or reliability predictions, such as Probabilistic Risk Assessment (PRA) (see Chapter 4), should be employed to:

- a. Evaluate alternative design concepts, redundancy or cross- and other reliability goals and requirements as applicable strapping approaches, and part substitutions
- b. Identify the elements of the design that are the greatest detractors of system reliability
- c. Identify those potential mission limiting elements and components that will require special attention in part selection, testing, environmental isolation, and/or special operations
- d. Assist in evaluating the ability of the design to achieve the mission life requirement
- e. Evaluate the impact of proposed engineering change and waiver requests on reliability

The developer shall perform Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) described in Chapter 4 of this document. The methods of analysis may be tailored to meet the needs of the project. The results of FMEA, FTA and any numerical reliability assessments or predictions shall be reported at system-level critical milestone reviews. The presentations shall include descriptions of how the analysis was used to perform design trade-offs and how the results were taken into consideration when making design or risk management decisions.

7.5 RISK LIST

The developer shall maintain a Risk List throughout the project life cycle, along with programmatic impacts. The list should indicate which risks have the highest probability, which have the highest consequences, and which risks represent the greatest risk to mission success. The list should also identify actions being taken to address each specific risk. The Risk List shall be configuration controlled.

Risk status shall be communicated on a regular basis to the entire project team and customers. Risk status shall be communicated to the Governing Program Management Council (PMC) through the Monthly Status Reviews. For each primary risk (those having both high probability and high impact/severity), the developer shall prepare and maintain the following in the risk sections of the Program/Project Plans:

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

- a. Description of the risk, including primary causes and contributors, actions embedded in the program or project to date to reduce or control it, and information collected for tracking purposes.
- b. Primary consequences should the undesired event occur.
- c. Estimate of the probability of occurrence (qualitative or quantitative) together with the uncertainty of the estimate and the effectiveness of any implemented risk mitigation measures.
- d. Potential additional risk mitigation measures, which shall include a comparison of the cost of risk mitigation versus the cost of occurrence multiplied by the probability of occurrence.
- e. Characterization of a primary risk as "acceptable" shall be supported by a rationale (with the concurrence of the Governing PMC) that all reasonable mitigation options (within cost, schedule, and technical constraints) have been instituted.

7.6 RISK-BASED ACQUISITION MANAGEMENT

GSFC projects shall incorporate the requirements of the Risk-Based Acquisition Management (RBAM) initiative as part of the CRM process. The purpose of RBAM is to convey NASA's focus on safety and mission success to NASA contractors.

- a. Acquisition planning shall incorporate input from GSFC personnel responsible for safety and mission assurance, health, environmental protection, information technology, export control, and security.
- b. When technical proposals are required as part of requests for proposals for supplies or services, offerors shall be instructed to identify and discuss risk factors and their approach for managing those risk factors (see NFS 1815.201 and NSF 1815.203-72). Where the solicitation requires submission of a Safety and Health Plan (see NFS 1823.7001(c)), safety and health shall be considered in the evaluation process (also see NFS 1815.305).
- c. Quality assurance surveillance plans are required and prepared with the statement of work for all performance-based contracts and, as necessary, for other contracts. Those plans shall reflect a specific surveillance approach that is commensurate with the perceived risk. The plans are general at the outset, but after contract award, contracting officers shall ensure that the plans are revised to reflect the risks associated with the successful proposal (see NFS 1846.401).

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

DIRECTIVE NO. 300-PG-7120.2.2E

Page 51 of 172

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

Chapter 8. Integrated Independent Review Requirements

The developer shall support a comprehensive set of independent reviews that are conducted by the GSFC Systems Review Office (SRO). The reviews cover all aspects of the mission system development and operations. In addition, each developer shall conduct a program of planned, scheduled and documented engineering peer reviews covering all aspects of his or her area of responsibility.

8.1 GENERAL REQUIREMENTS

For each specified review conducted by the GSFC SRO, the developer shall:

- a. Develop and organize material for oral presentation to the GSFC review team. Copies of the presentation material will be made available as required by the DID description below for the various reviews.
- b. Support splinter meetings resulting from the review.
- c. Produce timely written responses to recommendations and action items resulting from the review.
- d. Summarize, as appropriate, the results of the engineering peer reviews conducted by the developer.

8.2 OVERVIEW OF REVIEW ACTIVITY

8.2.1 Mission Reviews:

The primary purpose of mission-level Integrated Independent Reviews (IIRs), is to provide expert technical review of the end-to-end mission system in accordance with GPG 8700.4. Through the planned series of IIRs, the IIRT shall evaluate the adequacy of the planning, design, implementation, and associated processes to safely and successfully accomplish the mission requirements. The IIRs shall be supported by a comprehensive set of engineering peer reviews conducted in accordance with GPG 8700.6.

The Integrated Independent Review Team (IIRT) shall also assess programmatic performance and ability to deliver on commitments as documented in the approved Project Plan, Program Plan or Program Commitment Agreement. In addition, the IIRT shall note any observed deficiencies with respect to compliance with NPG 7120.5 and GSFC-STD-1000.

The IIRT shall:

- Assess the compatibility of the mission success criteria, and the acceptability of the risk associated with their accomplishment
- Assess the technical content, schedule, staffing and cost of the project over the entire life cycle
- Assess progress/milestone achievement against approved baselines
- Assess system resource management and margins (e.g. mass, power, propellant)
- Assess technical progress, risks remaining and mitigation plans
- Assess the safety hazards, and hazard mitigation and control strategies
- Assess the utilization of past lessons learned and the capture of new knowledge
- Identify deficiencies from the above assessments and recommend corrective measures

The Project Manager and IIRT shall utilize the criteria defined in GSFC-STD-1001 for the content of a particular review. The IIRT shall also utilize the evaluation criteria associated with Key System Management Practices referenced in GPR 8700.4. At the conclusion of each review, the IIRT shall use these criteria as key metrics to trend over the life cycle of the project as a benchmark for comparison with other projects.

The specific mission-level reviews consist of the following:

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

- a. **Mission Concept Review (MCR)** – The MCR affirms the mission need and examines proposed mission objectives and the concept for satisfying them. The MCR is normally held at the end of mission feasibility assessment after concept studies are complete. (see DID 8-1 for guidance).
- b. **Mission Definition Review (MDR)** – The MDR establishes that the baseline mission requirements are clearly understood, that the requirements for each independent system element have been determined, and that the currently envisioned system design will fully satisfy those requirements in order to justify that it is ready to complete system definition and to flow down requirements to lower levels of the system. It also confirms that planning for remaining project activities is adequate and that there are reasonable expectations that the project will accommodate any imposed constraints and meet its success criteria within the allocated resources. The MDR is normally held very early in the definition phase upon completion of a feasible mission definition and while system concept changes can be accommodated with minimal impact. Because of shortened development cycles or other considerations, the MDR may be combined with the SDR (see DID 8-2 for guidance).
- c. **System Definition Review (SDR)** – The SDR establishes that the baseline mission requirements are clearly understood, that system definition is complete, that the allocation of requirements to each independent system element and their respective subsystems is complete and verifiable, and that those lower level requirements are traceable to the mission level. In so doing, the project justifies readiness to proceed with preliminary design. In addition, the MDR establishes that planning for remaining project activities is adequate and that there are reasonable expectations that the project will accommodate any imposed constraints and meet its success criteria within the allocated resources. The SDR occurs at the end of system definition upon completion of a feasible design that will satisfy all system requirements. When appropriate, because of shortened development cycles or other considerations, the SDR can be combined with the MDR. (see DID 8-3 for guidance).
- d. **Preliminary Design Review (PDR)** – By illustrating a credible and tractable design solution that meets all mission requirements, the PDR establishes that the project has completed a credible and acceptable mission formulation, is prepared to proceed with the detailed design, and is on track to complete the flight and ground system development and mission operations within the identified cost and schedule constraints. The PDR is conducted at the end of formulation (end of the definition phase) (see DID 8-4 for guidance).
- e. **Critical Design Review (CDR)** – The CDR establishes that the maturity of the design and development effort is appropriate to support proceeding with full scale fabrication activities, and that the project is on track to complete the flight and ground system development and mission operations in order to meet mission performance requirements within the identified cost and schedule constraints. The CDR is conducted near the completion of final design and after completion of engineering model evaluations and breadboard development and test.. (see DID 8-5 for guidance).
- f. **Pre-Environmental Review (PER)** – Through the complete and comprehensive evaluation of project status, the PER establishes readiness to proceed with environmental testing of the integrated flight system and to demonstrate that the project is on track to complete the flight and ground system development and mission operations in order to fully meet mission performance requirements within allocated cost and schedule resources. The PER is held after completion of the initial successful comprehensive systems test of the fully-integrated flight system and prior to initiation of the system level environmental test sequence. (see DID 8-6 for guidance).
- g. **Pre-Ship Reviews (PSR)** – The PSR establishes that all flight and ground system verification activities have been successfully completed and that the system is ready for final processing prior to launch and mission operations. The PSR is conducted prior to shipment of flight system elements to the launch site and after successful completion of all verification activities, including environmental and functional performance testing as well as ground system and network compatibility testing. (see DID 8-7 for guidance).

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

8.2.2 Instrument Reviews

The set of reviews for each instrument shall generally consist of SDR, PDR, CDR, PER and PSR. Where applicable, the reviews for identical follow-on instruments shall generally consist of a PER and PSR. Success criteria for the mission-level reviews may be tailored by the IIRT in order to define criteria for these reviews.

8.2.3 Spacecraft Reviews

The set of reviews for each spacecraft shall generally consist of SDR, PDR, CDR, PER, and PSR. Success criteria for the mission-level reviews may be tailored by the IIRT in order to define criteria for these reviews.

8.2.4 Operations Reviews

The reviews specifically focused on mission operations consist of the MOR and the FOR. In addition, ground system development and mission operations is a major subject to be addressed in each of the aforementioned mission reviews.

- a. **Mission Operations Review (MOR)** – the MOR establishes the adequacy of plans and schedules for ground systems and flight operations preparation in order to justify readiness to proceed to implement the remaining required activities. The MOR is the first of two IIRT reviews held to examine mission operations status. It is typically held subsequent to completion of detail design and fabrication activity, but prior to initiation of major integration activities of flight or ground-system elements (see DID 8-8 for guidance)
- b. **Flight Operations Review (FOR)** – The FOR reviews the progress of ground system development and mission operations planning activities and establishes readiness to proceed with final preparations of ground system elements to support successful launch and mission operations. The FOR is held late in the test flow of the flight system, but prior to the last major interactive test between the flight and ground system elements. The review is conducted before shipment of flight system elements to the launch site. (see DID 8-9 for guidance)

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

Chapter 9. Design Verification Requirements

The design verification program, including environmental test, may be tailored to reflect system criticality, mission objectives, system characteristics, such as physical size and complexity, and the level of risk accepted by the project.

9.1 GENERAL

The developer shall conduct a verification program to ensure that the flight system meets the specified mission requirements. The program shall consist of functional demonstrations, analytical investigations, physical measurements and tests that simulate all expected environments. The developer shall provide adequate verification documentation including a verification plan and matrix, environmental test matrix and verification procedures.

The Verification Program begins with functional testing of assemblies. It continues through functional and environmental testing supported by appropriate analysis, at the unit/component, subsystem/instrument and spacecraft/payload levels of assembly. The program concludes with end-to-end testing of the entire operational system including the payload, the Payload Operations Control Center (POCC), and the appropriate GDS elements.

The GEVS-SE for STS & ELV Payloads, Subsystems, and Components shall be used as a baseline guide for developing the verification program. The GEVS-SE document is available at:

<http://arioch.gsfc.nasa.gov/302/gevs-se/toc.htm>. Alternative methods are acceptable provided that the net result demonstrates compliance with the intent of the requirements.

9.2 DOCUMENTATION REQUIREMENTS

The following documentation requirements shall be tailored to meet project needs, and shall be delivered and approved in accordance with the SOW.

9.2.1 System Performance Verification Plan

A System Performance Verification Plan, see DID 9-1, shall be prepared and define the tasks and methods required to determine the ability of the system to meet each project-level performance requirement (structural, thermal, optical, electrical, guidance/control, Radio Frequency (RF)/telemetry, science, mission operational, etc.) and to measure specification compliance. Limitations in the ability to verify any performance requirement shall be addressed, including the addition of supplemental tests and/or analyses that will be performed and a risk assessment of the inability to verify the requirement.

The plan shall address how compliance with each specification requirement will be verified. If verification relies on the results of measurements and/or analyses performed at lower (or other) levels of assembly, this dependence shall be described.

For each analysis activity, the plan shall include objectives, a description of the mathematical model, assumptions on which the models will be based, required output, criteria for assessing the acceptability of the results, the interaction with related test activity, if any, and requirements for reports. Analysis results shall take into account tolerance build-ups in the parameters being used.

The following documents may be included as part of the System Performance Verification Plan or as separate documents to meet project needs.

9.2.2 Environmental Verification Plan

An Environmental Verification Plan shall be prepared, as part of the System Performance Verification Plan or as a separate document, that prescribes the tests and analyses that will collectively demonstrate that the hardware and software comply with the environmental verification requirements.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

The Environmental Verification Plan shall provide the overall approach to accomplishing the environmental verification program. For each test, it shall include the level of assembly, the configuration of the item, objectives, facilities, instrumentation, safety considerations, contamination control, test phases and profiles, necessary functional operations, personnel responsibilities and requirement for procedures and reports. It shall also define a rationale for retest determination that does not invalidate previous verification activities. When appropriate, the interaction of the test and analysis activity shall be described.

Limitations in the environmental verification program that preclude the verification by test of any system requirement shall be documented. Alternative tests and analyses shall be evaluated and implemented as appropriate, and an assessment of project risk shall be included in the System Performance Verification Plan.

Because of the intended tailoring of the verification program, the preliminary plan shall provide sufficient verification philosophy and detail to allow assessment of the program. For example, for the environmental test portion of the verification, it is not sufficient to state that the GSFC GEVS requirements will be met. A program philosophy must be included. Examples of program philosophy are:

All components shall be subjected to random vibration.

Random vibration shall be performed at the subsystem or section level of assembly rather than at the component level.

All instruments shall be subjected to acoustics tests and 3-axis sine and random vibration.

All components shall be subjected to EMC tests.

All flight hardware shall see 8-thermal-vacuum cycles prior to integration on the spacecraft.

9.2.3 System Performance Verification Matrix

A System Performance Verification Matrix shall be prepared and maintained, to show each specification requirement, the reference source (to the specific paragraph or line item), the method of compliance, applicable procedure references, results, report reference numbers, etc. This matrix shall be included in the system review data packages showing the current verification status as applicable.

9.2.4 Environmental Test Matrix

As an adjunct to the system/environmental verification plan, an environmental test matrix (ETM) shall be prepared that summarizes all tests that will be performed on each component, each subsystem or instrument, and the payload. The purpose is to provide a ready reference to the contents of the test program in order to prevent the deletion of a portion thereof without an alternative means of accomplishing the objectives. All flight hardware, spares and prototypes (when appropriate) shall be included in the ETM. The matrix shall be prepared in conjunction with the initial environmental verification plan and shall be updated as changes occur.

A complementary matrix shall be kept showing the tests that have been performed on each component, subsystem, instrument or payload (or other applicable level of assembly). This shall include tests performed on prototypes or engineering units used in the qualification program and shall indicate test results (pass/fail or malfunctions).

9.2.5 Environmental Verification Specification

As part of the System Performance Verification Plan, or as a separate document, an environmental verification specification shall be prepared that defines the specific environmental parameters that each system element is subjected to either by test or analysis in order to demonstrate its ability to meet the mission performance requirements. Such things as payload peculiarities and interaction with the launch vehicle shall be taken into account.

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

9.2.6 Performance Verification Procedures

For each verification test activity conducted at the component, subsystem, and payload levels (or other appropriate levels) of assembly, a verification procedure shall be prepared that describes the configuration of the test article, how each test activity contained in the verification plan and specification will be implemented, see DID 9-2 for guidance.

Test procedures shall contain details such as instrumentation monitoring, facility control sequences, test article functions, test parameters, pass/fail criteria, quality control checkpoints, data collection, and reporting requirements. The procedures also shall address safety and contamination control provisions.

9.2.7 Verification Reports

After each component, subsystem, payload, etc. verification activity has been completed, a report shall be submitted in accordance with contract schedule, see DID 9-3 for guidance. For each analysis activity, the report shall describe the degree to which the objectives were accomplished, how well the mathematical model was validated by related test data, and other such significant results. In addition, as-run verification procedures and all test and analysis data shall be retained for review.

9.2.8 System Performance Verification Report

At the conclusion of the verification program, a final system Performance Verification Report shall be delivered comparing the hardware/software specifications with the final verified values (whether measured or computed). It is recommended that this report be subdivided by subsystem/instrument.

The System Performance Verification Report shall be developed and maintained "real-time" throughout the program summarizing the successful completion of verification activities, and showing that the applicable system performance specifications have been acceptably complied with prior to integration of hardware/software into the next higher level of assembly, see DID 9-3 for guidance

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

CHAPTER 10. Workmanship Standards

This chapter recommends workmanship standards that provide process and acceptance requirements for the manufacture of reliable flight and ground support hardware. These standards may be tailored to meet the needs of the project.

10.1 GENERAL

The developer shall plan and implement a Workmanship Program to assure that all electronic packaging technologies, processes and workmanship activities selected and applied meet mission objectives for quality and reliability. See Chapter 13 for additional information on electrostatic discharge (ESD) control.

10.2 APPLICABLE DOCUMENTS

The current status and/or any application notes for these standards can be obtained at Uniform Resource Locator (URL): <http://workmanship.nasa.gov/>. The most current version of these standards shall be used for new procurements. However, if a specific revision is listed for a referenced standard, it is that revision only that is approved for use unless otherwise approved by project management.

- Conformal Coating and Staking: NASA-STD-8739.1, "Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies".
- Soldering – Flight, Surface Mount Technology: NASA-STD-8739.2, "Surface Mount Technology".
- Soldering – Flight, Manual (hand): NASA-STD-8739.3, "Soldered Electrical Connections".
- Soldering – Ground Systems: Association Connecting Electronics Industries (IPC)/Electronics Industry Alliance (EIA) J-STD-001C, "Requirements for Soldered Electrical and Electronic Assemblies".
- Electronic Assemblies – Ground Systems: IPC-A-610, "Acceptability of Electronic Assemblies".
- Crimping, Wiring, and Harnessing: NASA-STD-8739.4, "Crimping, Interconnecting Cables, Harnesses, and Wiring".
- Fiber Optics: NASA-STD-8739.5, "Fiber Optic Terminations, Cable Assemblies, and Installation".
- ESD Control: ANSI/ESD S20.20, "Protection of Electrical and Electronic Parts, Assemblies and Equipment" (excluding electrically initiated explosive devices).
- Printed Wiring Board (PWB) Design:
 - 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 D-275 "Design Standard for Rigid Printed Boards and Rigid Printed Board Assemblies".
- PWB Manufacture:
 - IPC A-600, "Acceptability of Printed Boards".
 - IPC-6011, "Generic Performance Specification for Printed Boards".
 - IPC-6012, "Qualification and Performance Specification for Rigid Printed Boards"
 - Flight Applications – Supplemented with: IPC 6012B Performance Specification Sheet for Space and Military Avionics
 - IPC-6013 "Qualification and Performance Specification for Flexible Printed Boards".
 - IPC-6018 "Microwave End Product Board Inspection and Test."

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

10.3 DESIGN

10.3.1 Printed Wiring Boards

The PWB manufacturing and acceptance requirements identified in this chapter are based on using PWBs designed in accordance with the PWB design standards referenced above. Space flight PWB designs shall comply with the Class 3 requirements of the appropriate manufacturing standard (e.g., specified plating thickness, internal annular ring dimensions, etc.). For rigid PWBs, the finished boards shall comply with IPC-6012B Class 3/A requirements per the IPC-6012B Performance Specification Sheet for Space and Military Avionics.

10.3.2 Assemblies

The design considerations listed in the NASA workmanship and IPC standards listed above should be incorporated to the extent practical.

10.3.3 Ground Data Systems that Interface with Space Flight Hardware

GDS assemblies (this includes ground support equipment) that interface directly with space flight hardware shall be designed and fabricated using space flight parts, materials and processes for any portion of the assemblies that mate with the flight hardware; or that will reside with the space flight hardware in environmental chambers or other test facilities that simulate a space flight environment (e.g., connectors, test cables, etc.). Printed wiring boards meeting these criteria shall be procured to IPC-6012B Class 3/A requirements or Class 3 requirements of the other IPC PWB specifications.

10.4 WORKMANSHIP REQUIREMENTS

10.4.1 Training and Certification

All personnel working on flight hardware shall be certified as having completed the required training, appropriate to their involvement, as defined in the above standards or, when approved by project management, in the developer's quality manual. This includes, but is not limited to, the aforementioned workmanship and ESD standards. At a minimum, certification shall include successful completion of formal training in the appropriate discipline. Re-certification shall be in accordance with the requirements defined in the above workmanship standards.

10.4.2 Flight and Harsh Environment Ground Systems Workmanship

10.4.2.1 Printed Wiring Boards

PWBs shall be manufactured in accordance with the Class 3 requirements in the above referenced IPC PWB manufacturing standards; rigid PWBs shall conform to IPC-6012B Class 3/A requirements as specified by the Performance Specification Sheet for Space and Military Avionics. . The developer shall provide PWB test coupons to the GSFC Materials Engineering Branch (MEB) or a GSFC/MEB approved laboratory for evaluation, see DDI 10-1. Coupon acceptance shall be obtained prior to population of flight PWBs. Test coupons and test reports are not required for delivery to GSFC/MEB if the developer has the test coupons evaluated by a laboratory that has been approved by the GSFC/MEB, however, they shall be retained and included as part of the Project's documentation/data deliverables package.

10.4.2.2 Assemblies

Assemblies shall be fabricated using the appropriate workmanship standards listed above (i.e., NASA-STD-8739.3 for hand soldering; NASA-STD-8739.4 for crimping/cabaling; NASA-STD-8739.5 for fiber optic termination and installation; NASA-STD-8739.2 for Surface Mount Soldering, etc.) and ANSI/ESD S20.20.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

10.4.3 Ground Systems (non-flight) Workmanship

10.4.3.1 Printed Wiring Boards

PWBs shall be manufactured in accordance with the Class 3 requirements in the above referenced IPC PWB manufacturing standards.

10.4.3.2 Assemblies

Assemblies shall be fabricated using the Class 3 requirements of J-STD-001, IPC-A-610, and ANSI/ESD S20.20. If any conflicts between J-STD-001 and IPC-A-610 are encountered, the requirements in J-STD-001 shall take precedence.

10.4.4 Documentation

The developer shall document the procedures and processes that will be used to implement the above referenced workmanship, design, and ESD control standards; including any procedures or process requirements referenced in by those standards.

Alternate standards may be proposed by the developer. Proposals shall be accompanied by objective data documenting that mission safety or reliability will not be compromised. Their use is limited to the specific project and allowed only after they have been reviewed and approved by program management.

10.5 NEW OR ADVANCED MATERIALS AND PACKAGING TECHNOLOGIES

New and/or existing advanced materials and packaging technologies (e.g., multi-chip modules (MCMs), stacked memories, chip on board (COB), ball grid array (BGA), etc.) shall be reviewed and approved by the Parts Control Board (PCB).

10.6 HARDWARE HANDLING

The developer shall use proper safety, ESD control and, where appropriate, clean room practices when handling flight hardware. The electrostatic charge generation and contamination potential of materials, processes, and equipment (e.g., cleaning equipment, packaging materials, purging, tent enclosures, etc.) shall be addressed. Materials used in the handling of flight hardware (i.e. finger cots, gloves, wipes, swabs, etc.) shall be screened to verify that contact with the hardware does not result in violation of the appropriate project contamination control requirements.

10.7 ELECTROSTATIC DISCHARGE CONTROL

This section establishes requirements for an effective ESD Control Program in order to prevent damage to electronic hardware from ESD events. These requirements may be tailored to meet the needs of the project.

The developer shall document and implement an ESD Control Program to assure that all manufacturing, inspection, testing, and other processes will not compromise mission objectives for quality and reliability due to ESD events.

10.7.1 Applicable Documents

The current status and/or any application notes for these standards can be obtained at the following URL:

<http://workmanship.nasa.gov>

The most current version of these standards should be used for new procurements. Included shall be ANSI/ESD S20.20 ESD Association Standard for the Development of an Electrostatic Discharge Control Program for

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

DIRECTIVE NO. 300-PG-7120.2.2E**EFFECTIVE DATE:** May 3, 2005**EXPIRATION DATE:** May 3, 2010

protection of electrical and electronic parts, assemblies, and equipment (excluding electrically initiated explosive devices). However, if a specific revision is listed for a referenced standard, it is that revision only that is approved for use unless otherwise approved by project management.

10.7.2 Electrostatic Discharge Control Requirements

- The developer shall document and implement an ESD Control Program in accordance with ANSI/ESD S20.20, Protection of Electrical and Electronic Parts, Assemblies and Equipment (excluding electrically initiated explosive devices) suitable to protect the most sensitive component involved in the project. At a minimum, the ESD Control Program shall address training, protected work area procedures and verification schedules, packaging, facility maintenance, storage, and shipping.
- All personnel who manufacture, inspect, test, otherwise process electronic hardware, or require unescorted access into ESD protected areas shall be certified as having completed the required training, appropriate to their involvement, as defined in ANSI/ESD S20.20 or in the developer's quality manual prior to handling any electronic hardware.
- Electronic hardware shall be manufactured, inspected, tested, or otherwise processed only at designated ESD protective work areas. These work areas shall be verified on a regular schedule as identified in the developer's ESD Control Program; an ESD Control Program that has been approved by the procuring organization
- Electronic hardware shall be properly packaged in ESD protective packaging at all times when not actively being manufactured, inspected, tested, or otherwise processed.
- Alternate standards may be proposed by the developer. Their use is limited to the specific project and are allowed only after they have been reviewed and approved by the GSFC Project Office.
- Materials selected for packaging or protecting ESD sensitive devices shall not leach chemicals, leave residues, or otherwise contaminate parts or assemblies (e.g., "pink poly" is well known for its outgassing of contaminants and should only be used for storing documentation or other non-hardware uses).

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

Chapter 11. Parts Requirements

This chapter provides recommended Parts requirements. These requirements may be tailored to meet the needs of the project.

11.1 GENERAL

The developer/sub-developer shall plan and implement a Parts Control Program (PCP) to assure that all selected items for use in flight hardware meet mission objectives for quality and reliability. The developer shall prepare a PCP plan describing the approach and methodology for implementing a PCP, see DID 11-1.

Existing developer in-house documentation equivalent with DID 11-1 may be used and referenced in the plan as applicable to address how these requirements are to be met and shall be submitted to GSFC for approval. All appropriate sub-developers shall also participate in the parts control program to the extent required by the prime developer and GSFC in order to meet these requirements. The plan shall address how the developer ensures the flow down of the applicable parts control program requirements to the sub-developers. The PCP plan may be incorporated in the developer's Performance Assurance Implementation Plan.

The plan shall include:

- a. Parts Control Board (PCB) operating procedures, membership, responsibilities, authority, meeting schedules, Parts review procedures, Parts approval/disapproval procedures, GSFC involvement, and plans for updating the operating procedures; the definition of the role and authority of each PCB member; and relationships with various groups within the prime, associate, and sub-developer organizations (see section 11.2 for further information).
- b. Shelf life control plan (see section 11.4.7.2 for further information).
- c. Parts application derating (see section 11.4.4 for further information).
- d. Part vendor surveillance and audit plan (see section 11.5.2 for further information).
- e. Part qualification plan that describes how parts should be qualified for the intended end item application (see section 11.9 for further information).
- f. Incoming inspection and test plan (see section 11.4.6 for further information).
- g. Destructive Physical Analysis (DPA) plan (see section 11.4.7.1 for further information).
- h. Defective parts controls program.
- i. PCB coordination and interactions with other program control boards; i.e., CCB, and failure review board (FRB).
- j. Radiation hardness assurance program plan as required (see section 11.6 for further information).
- k. ESD control plan.
- l. Corrosion prevention and control plan.
- m. Contamination Prevention and Control Plan, as required.
- n. Standardization of parts program .
- o. Alternate Quality Conformance Inspection (QCI) and small lot sample plans, as required (see section 11.4.8 for further information).
- p. Traceability control plan.
- q. PCB shall develop, update and maintain a Project Approved Parts List (PAPL).

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

11.2 PARTS CONTROL BOARD

A PCB shall be responsible for the planning, management, and coordination of the selection, application, and procurement requirements of all parts intended for use in the deliverable end item(s). PCB findings, decisions, and directions shall be within the contractual requirements, and shall be binding on all applicable developers and sub-developers. The GSFC Project Parts Engineer (PPE) shall be a permanent member of the PCB to ensure real-time approval/disapproval of PCB decisions and actions. If there are any parts issues, which the developer and GSFC cannot resolve at the PCB level, then the GSFC PE shall inform the SAM and the Project Manager of the issue and the associated risk. After this discussion, the GSFC Project Manager will decide whether to accept the risk and ask the developer to submit a waiver to document the issue, or to elevate the issue to the developer's management for resolution.

11.2.1 Chairmanship

The PCB Chairman shall be responsible for preparation and distribution of PCB meeting agenda and minutes, conducting PCB meetings and managing the PCB.

11.2.2 Membership

The PCB membership shall include at least one member from each appropriate developer and sub-developer. The GSFC PPE will appoint a representative to be a voting member of the developer/sub-developer PCB. Other members may be designated by GSFC or the PCB chairman. Each member shall be supported in technical matters as required. Each member shall have the authority to commit his activity, organization, or company to PCB decisions within the scope of the applicable contract. Representation at individual meetings shall be required, consistent with the scheduled subject matter on the agenda.

11.2.3 Delegation.

The authority to conduct PCB may be delegated by the prime developer PCB chairman to major developers/sub-developers. Each organization so delegated shall supply the responsible activity PCB with meeting minutes documenting decisions in a timely manner. All information shall be made available to each higher acquisition activity. Each higher acquisition activity retains the right of disapproval of delegated PCB decisions. However, the GSFC PPE shall be a voting member at all developer/sub-developer PCB activities.

11.2.4 Meetings

The PCB shall conduct meetings as follows:

- a. A post-award organizational PCB meeting shall be convened by the developer/sub-developer within 60 days after contract is awarded. The chairman shall coordinate the date and location of the meeting with GSFC, and inform proposed member activities of the schedule and meeting agenda. The purpose of this initial meeting is to establish responsibilities, procedures, and working relationships to allow the rapid transition to an operational PCB.
- b. Regularly scheduled meetings shall be held as determined necessary by the PCB chairman. These meetings shall address, as a minimum, predefined agenda items for discussion.
- c. Special PCB meetings may be called by the PCB chairman to discuss special items that may require expeditious resolution. Adequate notification shall be provided to all PCB members.
- d. PCB meetings may be accomplished either in person, via telephone, or other media such as tele/video conference.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

11.2.5 PCB Responsibilities

- a. The PCB shall establish and document formal operating procedures.
- b. The PCB shall develop and maintain a Project Approved Parts, List (PAPL). The PCB shall review and approve all parts.
- c. The PCB shall define parts selection and approval criteria and shall prepare and maintain supporting documents for part approval.
- d. Through interface with design activity, the PCB shall ensure the design selection and use of parts that meets the technical program requirements.
- e. The PCB shall ensure derating of all electronic parts and adequate design margins for mechanical parts used in deliverable end items. The PCB shall review and approve any proposed deviations from the technical program requirements.
- f. The PCB shall ensure the establishment of DPA policies, procedures and reporting formats. DPA problems and anomalies of concern shall be reviewed by the PCB.
- g. The PCB shall ensure the review of the results of DPA, failure analyses, and any other details pertaining to part selection. All parts problems shall require disposition by the PCB.
- h. The PCB shall ensure the timely identification of long lead parts items and other problem procurements.
- i. The PCB shall ensure the identification and configuration control of any changes to PCB approved documentation.
- j. The PCB shall ensure that laboratories and analysis facilities used for evaluation of all parts are reviewed for capabilities of equipment and personnel before performing analyses in compliance with these requirements.
- k. The PCB shall ensure that all screening and testing of parts is conducted by acceptable laboratories with capable personnel, equipment and software.
- l. The PCB shall prepare and distribute the meeting minutes within 5 working days after the meeting. The minutes shall document all action items, significant areas of disagreement and the basis for all decisions from the meeting.

11.2.6 PCB Authority

The PCB shall ensure that all part items approved for use meet mission reliability and performance requirements. All PCB decisions shall be documented in the meeting minutes. All supporting technical analysis shall be provided and any additional analysis and tests in accordance with PCB direction attached to the meeting minutes. The PCB shall have the authority to approve technical changes to the detail part requirements when baseline changes fall into one or more of the categories specified below without impact to the item performance in the intended application:

- a. Variation from design and construction requirements of the detail specification.
- b. Screening and lot acceptance tests and acceptance criteria deviations from the detail specifications.

11.3 MANAGEMENT OF PARTS SELECTION

The developer/sub-developer shall manage the parts selection in accordance with criteria specified herein. All parts shall be selected to assure that mission reliability and performance requirements are met. The developer/sub-developer shall develop a Parts Identification List and/or an As-designed Parts List (ADPL), see DID 11-2, to start the PCB activity. The list shall be submitted to the PCB, ten days prior to the meeting. All approved parts by PCB

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

shall be added to the Project Approved Parts list within 10 days of approval, and shall be the only source for procurement.

11.3.1 EEE Parts

11.3.1.1 EEE Parts Selection

Parts selection shall be guided by the GSFC EEE-INST-002, "Instructions for EEE Parts Selection, Screening, Qualification and Derating," and the NASA Parts Selection List (NPSL) both of which provide for 3 part levels as described below. The EEE-INST-002 and the NPSL is available at the following URLs: http://www.nepp.nasa.gov/index_nasa.cfm/725/ and <http://nepp.nasa.gov/npsl> respectively.

- Level 1 parts are inherently low risk and are suitable for use in all applications including life support, mission critical, single-string and single-point failure. Level 1 active parts should be reviewed for radiation hardness.
- Level 2 parts have inherently higher risk than level 1 and are considered moderate risk. Level 2 parts are suitable for most general purpose space flight applications but are not recommended for life support, mission critical, single-string or single-point failure applications unless there is on-orbit reparability. Level 2 active parts need to be evaluated for radiation hardness.
- Level 3 parts are inherently high risk because there is little dependable data or history available for them and changes in their materials, designs and processes may occur continuously without notification. Level 3 parts are intended for mission applications where the use of high-risk parts is acceptable. Level 3 parts should not be used in single-point failure or single-string applications unless a very high risk for failure or malfunction is acceptable. Level 3 parts shall be evaluated for radiation hardness, radiation testing is recommended.

The inherent risk of the parts selected shall be mitigated to meet application needs by qualification and upscreening, in accordance with GSFC EEE-INST-002, "Instructions for EEE Parts Selection, Screening, Qualification and Derating". Further mitigation strategies may be recommended by the PCB. The project manager shall approve the quality level selected for the application.

A procurement document may be required for parts based on PCB recommendation. The procurement document shall fully identify the item being procured and shall include physical, mechanical, electrical, and environments and quality assurance provisions necessary to control manufacture and acceptance in accordance GSFC EEE-INST-002, "Instructions for EEE Parts Selection, Screening, Qualification, and Derating". When parts are procured to acceptable manufacturer's in-house specifications, the attribute screening data package for the lot shall also be procured. The manufacturer shall notify GSFC of any changes to a procured part's specification or design.

The use of Plastic Encapsulated Microcircuits (PEMs) is not recommended on NASA GSFC spaceflight applications. only if their use is necessary to achieve unique requirements that cannot be found in hermetic high reliability parts. Each use of PEMS shall be thoroughly evaluated for thermal, mechanical, and radiation implications of the specific application and found to meet mission requirements. PEMs shall be selected for their functional advantage and availability, not for cost saving; the steps necessary to ensure reliability usually negate any initial apparent cost advantage. A PEM shall not be substituted for a form, fit and functional equivalent, high reliability, hermetic device in spaceflight applications. All PEMs shall be approved by PCB and shall be processed in accordance with GSFC EEE-INST-002.

11.3.1.2 Parts Identification List (PIL)

The PIL shall list all parts proposed for use in flight hardware. The PIL is prepared from design team inputs or subcontractor inputs, to be used for presenting candidate parts to the PCB. The PIL shall be ready for review prior to the Preliminary Design Review (PDR). The PIL shall include as a minimum the following information: part number, part name or description, manufacturer, manufacturer's generic part number, drawing number,

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

specifications, comments as necessary to indicate problems, long lead times, additional testing imposed, application unique notes, etc. (Refer to DID 11.2)

11.3.1.3 Project Approved Parts List (PAPL)

PCB chair is responsible to develop, maintain, and update the PAPL and will distribute to the members within 15 working days to the PCB members for review. PCB chair shall assure that only approved parts are procured and any additional testing requirements are properly implemented. Developer/sub-developer shall coordinate all sub-contractor PAPL and submit to GSFC within 15 days after PCB meetings. (Refer to DID 11.2)

11.3.1.4 As-Designed Parts List (ADPL)

The PCB chair is responsible to establish an As-Designed Parts List (ADPL) as soon as the preliminary release of designs for CDR. (Refer to DID 11.2)

11.3.1.5 As-Built Parts List (ABPL)

The ABPL is generally a final compilation of all parts as installed in flight equipment, with additional "as-installed" part information such as manufacturer name, CAGE code, Lot-Date Code, part serial number (if applicable), quantity used and box or board location. The manufacturer's plant specific CAGE code is preferred, but if unknown, the supplier's general cage code is sufficient. (Refer to DID 11.2)

11.4 MANAGEMENT OF PARTS ENGINEERING REQUIREMENTS

11.4.1 System Design.

The PCB is responsible for ensuring that parts used throughout the system meets the application, reliability, quality, and survivability requirements, as derived from the system level requirements. Parts engineering shall review and approve all drawings and specifications (A level, B level, device detail specifications, etc.) to ensure that part requirements are met. All parts shall be selected to meet their intended application in the predicted mission radiation environment.

11.4.2 Custom Devices

Custom microcircuits, such as Application Specific Integrated Circuits (ASICs), hybrid microcircuits, MCMs etc., planned for use by the developer shall be subjected to a design review. The review shall be conducted as part of the PCB activity. The design review shall address, at a minimum, derating of elements, method used to assure each element reliability, assembly process and materials, and method for assuring adequate thermal analysis to meet application requirements.

11.4.3 Reuse of Parts

Parts which have been installed in an assembly, and are then removed from the assembly for any reason, shall not be used again in any item of flight or spare hardware without prior approval of the PCB based on the submission of evidence that this practice does not degrade the system performance.

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

DIRECTIVE NO.	<u>300-PG-7120.2.2E</u>
EFFECTIVE DATE:	<u>May 3, 2005</u>
EXPIRATION DATE:	<u>May 3, 2010</u>

11.4.4 Derating

A uniform derating policy to meet the system requirements shall be established by the PCB in accordance with the derating guidelines of GSFC EEE-INST-002 and used by all developers in the program

Exceptions to this derating policy shall require the approval of the PCB. The derating policy shall address degradation sensitive parameters and maximum rated variations expected over the program mission life including storage environments and radiation effects.

The developer's derating guidelines may be used when approved by the PCB. The developer/sub-developer shall maintain documentation on parts derating analysis and shall be available for PCB review.

11.4.5 Traceability and Lot Control.

The developer/sub-developer shall develop and maintain a traceability and lot control plan in accordance with the requirements specified below and approved by the PCB. When given a lot date code or batch number, the developer/sub-developer shall be capable of determining the unique piece of equipment (black box level) by serial number in which the part or material is installed or used. Traceability to the serial number of an individual device or to a lower level of assembly shall be as determined and specified by the PCB. Traceability shall be maintained for all flight printed circuit boards (PCBs) so that part number, serial number, and lot date code information is known for all PCBs; in addition, any vendor identification necessary to trace the PCBs to their representative coupons shall be maintained and provided as needed.

All EEE parts and cable assemblies shall have one hundred percent (100%) lot traceability to the production lot. Any other parts not included in the above that require traceability shall be identified in the traceability lot control plan. Identification and serialization data for EEE parts shall be maintained in the manufacturing and processing records and shall contain lot date code, lot and purchase order numbers, and manufacturer of the part. The developer/sub-developer shall ensure that markings for small chip devices (usually printed on the parts' packaging) are recorded in the manufacturing and processing records prior to use.

11.4.6 Incoming Inspection Requirements

Each developer/sub-developer shall perform, or be responsible for the performance of applicable incoming tests and inspections including DPA of parts to ensure that they meet the requirements of the procurement specification. Unless previously accomplished and accepted by government or developer/sub-developer field personnel, incoming testing and inspections shall be accomplished upon receipt of the parts. The inspection and testing of parts shall be conducted in accordance with a plan approved by the PCB.

11.4.7 Electronic Parts

11.4.7.1 Destructive Physical Analysis

A sample of each lot date code of microcircuits, hybrids, semiconductors, capacitors, relays and filters shall be subjected to a DPA. All other parts may require a sample DPA if it is deemed necessary as indicated by failure history, GIDEP Alerts, or other reliability concerns. DPA tests, procedures, sample size and criteria shall be as specified in GSFC S-311-M-70, Destructive Physical Analysis. Developer/sub-developer's procedures for DPA may be used in place of GSFC S-311-M-70 and shall be submitted with the PCP for concurrence prior to use. The PCB on a case-by-case basis shall consider variation to the DPA sample size requirements, due to part complexity, availability or cost. Variations in sample sizes and the supporting justification shall be recorded in the PCB minutes.

It is recommended that exposure time be limited when using Real Time X-ray inspection for DPA or failure analysis of microcircuits and hybrids because in extreme cases, exposure levels may accumulate sufficiently to damage sensitive devices.

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

DIRECTIVE NO.	<u>300-PG-7120.2.2E</u>
EFFECTIVE DATE:	<u>May 3, 2005</u>
EXPIRATION DATE:	<u>May 3, 2010</u>

11.4.7.2 Shelf-Life Control

The developer/sub-developer shall develop a shelf life control program that identifies the shelf life limitations for all parts to be stored. This plan shall specify the length of time required and minimum requirements for re-inspection, retest, & any other action required to ensure maintenance of space flight quality and reliability. The plan shall be reviewed and approved by the PCB and controls shall be identified to ensure that the plan is followed before parts are issued to assembly.

11.4.7.3 Parts Shelf Life Control

The shelf life control program shall identify those part types considered to be potentially age sensitive. The plan shall identify specific actions necessary in association with the potentially age sensitive parts. In general, the plan shall consider a pedigree review and actions similar to that shown below for all parts older than 5 years. The plan shall define the specific limit for each part based upon logistical considerations of parts procurement schedules, program manufacturing schedules, and required program life. When parts exceed specified age limits in storage, actions shall be taken as specified in the control plan or the PCB shall provide direction based upon the following considerations:

- a. Assess original part quality (e.g. mil specification quality levels V, Q or M for microcircuits, class K and H for hybrids, source control drawings (SCDs), etc.)
- b. Assess lot history (suppliers percent defective, quantity used to date, number of failures, etc.).
- c. Review of original screening/test data.
- d. Review of problem/GIDEP Alerts.
- e. Review of original DPA.
- f. Review storage environment controls (temperature, ESD protection, handling, etc.).
- g. When possible, consider application criticality, redundancy, etc.
- h. Analyze construction details to identify age sensitive design characteristics
- i. When retest/ re-screen appears warranted, assess availability of retest equipment, outside re-screen facilities, potential for part damage during re-screening, etc.
- j. Program technical requirements for screening shall be used as guidance for any planned re-screening of product due to shelf life limitations.
- k. Solderability of parts

11.4.8 Use of Alternate Quality Conformance Inspection and Small Lot Sampling Plans

The developer/sub-developer may implement an alternate QCI plan and a small lot sample plan for small lot quantities in accordance with the program's technical requirements. The PCB shall review and approve these plans. These plans may be used under the following conditions:

- a. The product(s) being purchased is not listed in the program's space quality baseline.
- b. Implementation criteria as defined in the program's technical requirements are satisfied.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

11.5 MANAGEMENT OF PARTS PROCUREMENT

11.5.1 Supplier and Vendor Selection and Surveillance

The PCB is responsible for the selection and qualification of part suppliers, vendors, laboratories and manufacturers.

11.5.2 Part Supplier and Manufacturer Surveillance (Monitoring)

The PCB shall establish a policy and procedures for the periodic surveillance and auditing of suppliers, vendors, laboratories and manufacturers to ensure compliance to procurement, quality, reliability and survivability requirements. Developer/sub-developer surveillance of laboratories, suppliers, vendors, and manufacturers that have been approved as a part of Qualified Parts List (QPL) or Qualified Manufacturer's List (QML) program for products listed in the space quality baseline is not required. When surveillance/audit data is available from other sources (e.g. other developer/sub-developer programs, other developers/sub-developers, independent audits reports, etc.) the developer/sub-developer may utilize the results of the data contingent on the review and approval by the PCB. Acceptability of the data shall be based on technical considerations, as well as timeliness and confidence in the source of the data.

11.5.3 Coordinated Procurements

Implementation of a coordinated procurement program is highly encouraged. When appropriate, the PCB shall establish policies for the use of coordinated procurements for all developers and sub-developers use. This may include the use of common specifications, management responsibilities, purchase agreements, monitoring, and quality assurance. The PCB (and procurement organizations) may ensure that a master purchase agreement allows authorized sub-developers to initiate their own procurements within the scope and framework of the master purchase agreement.

11.6 RADIATION HARDNESS ASSURANCE (RHA)

11.6.1 General

An appropriate radiation hardness assurance program shall be developed and conducted, through the PCB, based on program requirements. The program plan shall address all phases of the flight hardware program including the design, test, and production.

11.6.1.1 Specification of the Radiation Environment

The radiation environment for the mission of interest shall be specified using established codes and algorithms. This includes the trapped particle environment, galactic cosmic ray environment and solar particle event environment, and induced environments such as that caused by a radioisotope thermal generator (RTG).

11.6.1.2 Radiation Transport Analysis

When deemed necessary, transport calculations for the incident radiations shall be performed for shielding appropriate for the mission of interest using established codes.

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

11.6.1.3 Evaluation of Radiation Effects in Microelectronic Devices and Integrated Circuits

The following potential failure modes of microelectronic components caused by radiation exposure during the mission shall be evaluated:

- a. total ionizing dose effects, including enhanced low dose rate effects
- b. single event effects, including single event upset, single event latch up and single event transients
- c. displacement damage effects
- d. other radiation effects determined to be relevant for the mission of interest

11.6.1.4 Qualification of Parts for Use

Parts shall be considered qualified for use in the mission if they have the same wafer diffusion lot date code that has been used previously for similar applications in a radiation environment at least as severe as that of the mission under consideration. Alternatively, they shall be considered qualified if radiation testing shows that the effects specified in section 11.6.1.3 shall not compromise the mission.

11.7 GOVERNMENT FURNISHED EQUIPMENT

Parts contained in unmodified government furnished equipment used in the end item of the contract shall not be subject to parts control.

11.8 COMMERCIAL OFF-THE-SHELF ITEM EQUIPMENT

The requesting user shall demonstrate to the PCB that the COTS items meet the quality, reliability, environmental and survivability (if required) requirements of the contract end item for the intended application.

11.9 PART QUALIFICATION.

11.9.1 General

All parts, including any processes developed to accomplish rework or retrofit, shall be qualified for program use. Only qualified parts shall be used on flight hardware. For each non-qualified part, the developer(s) shall prepare a qualification plan and procedure. For electronic parts, the qualification plans and procedures shall be based on the application or program technical requirements. The qualification plan shall identify all conditions and testing necessary to meet the program and mission reliability and qualification requirements. These plans and procedures shall be reviewed and approved by the PCB. A summary report of qualification test results shall be submitted to the PCB. The PCB shall maintain an up-to-date listing of the qualification status of all program parts. Test methods used for qualification of parts shall be in accordance with applicable specifications and shall include test methods for any additional tests necessary to fully qualify the part for its intended use in the system.

Qualification of parts shall be expedited by the following:

- a. Initial selection of parts using applicable military specified parts previously qualified for use on space programs.
- b. Proof testing of all parts to the program requirement levels.
- c. Vendor audits and certification.

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

11.9.2 Manufacturing Baseline

As part of the qualification plan for each non-qualified part item, the developer(s) shall insure that the non-qualified part item supplier has an established manufacturing baseline and review the manufacturing baseline for compliance to the program's technical requirements. The manufacturing baseline for all other parts shall be reviewed and controlled.

11.9.3 Qualification by Extension

Parts may be qualified by extension, when supporting data is available and shows that either of the following criteria are met:

- a. The part was successfully used in a prior but recent space application in which the application environment conditions of use and test were, at least, as severe as those required of the candidate part for qualification.
- b. The part design and construction is the same as the previously qualified part. The part is manufactured by the same manufacturing facility to the same manufacturing baseline as the previously qualified part, and the utilization of the part does not result in critical stresses or mechanical strain (such as due to thermal mismatch) greater than the previously qualified part.

11.10 FAILURE ANALYSIS

Failure analysis shall be performed on part failures experienced during assembly and testing. Failures shall be analyzed to the extent necessary to understand the failure mode and cause, to detect and correct out-of-control processes, to determine the necessary corrective actions, and to determine lot disposition. When required, a failure analysis report shall be prepared and documented. The PCB shall determine and implement appropriate corrective action for each part failure. All failures, and the results of final failure analysis, shall be documented. Failure analysis reports shall be retrievable for the duration of the contract, and shall be available to GSFC.

11.11 PRESERVATION AND PACKAGING

Preservation, packaging, and packing shall be in accordance with the item and the system requirements. All parts that are subject to degradation by electrostatic discharge shall be packaged in accordance with ANSI/ESD-S20.20, Protection of Electrical and Electronic Parts, Assemblies, and Equipment (Excluding Electrically Initiated Explosive Devices) and approved ESD procedures.

11.12 HANDLING

Handling (including storage) procedures shall be instituted to prevent part and material degradation. The handling procedures shall be retained through inspection, kitting, and assembly and shall be identified on "build to" documentation. The following criteria shall be used as a minimum for establishing handling and storage procedures for parts:

- a. Control of environment, such as temperature, humidity, contamination, and pressure.
- b. Measures and facilities to segregate and protect parts routed to different locations such as, to the a laboratory for inspection, or returned to the manufacturer from unaccepted shipments.
- c. Easily identifiable containers to identify space quality parts shall be used.
- d. Control measures to limit personnel access to parts during receiving inspection and storage.
- e. Facilities for interim storage of parts.
- f. Provisions for protective cushioning, as required, on storage area shelves, and in storage and transportation containers.
- g. Protective features of transportation equipment design to prevent packages from being dropped or dislodged in transit

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

- h. Protective bench surfaces on which parts are handled during operations such as test, assembly, inspection, and organizing kits.
- i. Required use of gloves, finger cots, tweezers, or other means when handling parts to protect the parts from contact by bare hands.
- j. Provisions for protection of parts susceptible to damage by electrostatic discharge.
- k. Unique parts criteria.

11.13 DATA RETENTION

The program shall maintain records of incoming inspection tests, lot qualification and acceptance test data, radiation hardness assurance test data, traceability data and other data as determined by the PCB for a period of time specified by the GSFC.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

Chapter 12. Materials, and Processes Requirements

This chapter provides recommended Materials and Processes requirements. These requirements may be tailored to meet the needs of the project.

12.1 GENERAL

The developer shall plan and implement a Materials, and Processes Control Program (MPCP) to assure that all selected items for use in flight hardware meet mission objectives for quality and reliability. The developer shall prepare a MPCP plan describing the approach and methodology for implementing a MPCP, see DID 12-1.

Existing developer in-house documentation equivalent with DID 12-1 may be used and referenced in the plan as applicable to address how these requirements are to be met and shall be submitted to GSFC for approval. All appropriate sub-developers shall also participate in the materials, and processes control program to the extent required by the prime developer and GSFC in order to meet these requirements. The plan shall address how the developer ensures the flow down of the applicable materials, and processes control program requirements to the sub-developers. The MPCP plan may be incorporated in the developer's Performance Assurance Implementation Plan.

The plan shall include:

- r. Materials, & Processes Control Board (MPCB) operating procedures, membership, responsibilities, authority, meeting schedules, MP review procedures, MP approval/disapproval procedures, GSFC involvement, and plans for updating the operating procedures; the definition of the role and authority of each MPCB member; and relationships with various groups within the prime, associate, and sub-developer organizations (see section 12.2 for further information). In programs where the developer deems that a MPCB is impractical, a Materials Assurance Engineering shall serve in its place.
- s. Shelf life control plan (see section 12.3.8 for further information).
- t. MP vendor surveillance and audit plan (see section 12.5.2 for further information).
- u. MP qualification plan that describes how new MP should be qualified for the intended end item application (see section 12.9 for further information).
- v. Incoming inspection and test plan (see section 12.4.6 for further information).
- w. Destructive Physical Analysis (DPA) plan (see section 12.4.7.1 for further information).
- x. Defective materials controls program.
- y. MPCB coordination and interactions with other program control boards; i.e., CCB, failure review board (FRB), mass properties control board (MPCB) and MRB.
- z. Corrosion prevention and control plan.
- aa. Contamination Prevention and Control Plan, as required.
- bb. Standardization of program MP.
- cc. Traceability control plan.

12.2 MATERIALS AND PROCESSES CONTROL BOARD

A MPCB shall be responsible for the planning, management, and coordination of the selection, application, and procurement requirements of all materials and processes intended for use in the deliverable end item(s). MPCB findings, decisions, and directions shall be within the contractual requirements, and shall be binding on all applicable developers and sub-developers. The GSFC Materials Assurance Engineer (MAE) shall be a permanent member of the MPCB to ensure real-time approval/disapproval of MPCB decisions and actions. If there are any

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

materials issues, which the developer and GSFC cannot resolve at the MPCB level, then the GSFC MAE shall inform the SAM and the Project Manager of the issue and the associated risk. After this discussion, the GSFC Project Manager will decide whether to accept the risk and ask the developer to submit a waiver to document the issue, or to elevate the issue to the developer's management for resolution.

12.2.1 Chairmanship

The MPCB Chairman shall be responsible for preparation and distribution of MPCB meeting agenda and minutes, conducting MPCB meetings and managing the MPCB.

12.2.2 Membership

The MPCB membership shall include at least one member from each appropriate developer and sub-developer. GSFC will appoint a representative to be a voting member of the developer/sub-developer MPCB. Other members may be designated by GSFC or the MPCB chairman. Each member shall be supported in technical matters as required. Each member shall have the authority to commit his activity, organization, or company to assist as needed to support MPCB decisions within the scope of the applicable contract. Representation at individual meetings shall be required, consistent with the scheduled subject matter on the agenda.

12.2.3 Delegation.

The authority to conduct MPCB may be delegated by the prime developer MPCB chairman to major developers/sub-developers. Each organization so delegated shall supply the responsible activity MPCB with meeting minutes documenting decisions in a timely manner. All information shall be made available to each higher acquisition activity. Each higher acquisition activity retains the right of disapproval of delegated MPCB decisions.

12.2.4 Meetings

The MPCB shall conduct meetings as follows:

- e. A post-award organizational MPCB meeting shall be convened by the developer. The chairman shall coordinate the date and location of the meeting with GSFC, and inform proposed member activities members of the schedule and meeting agenda. The purpose of this initial meeting is to establish responsibilities, procedures, and working relationships to allow the rapid transition to an operational MPCB.
- f. Regularly scheduled meetings shall be held as determined necessary by the MPCB chairman. These meetings shall address, as a minimum, predefined agenda items for discussion.
- g. Special MPCB meetings may be called by the MPCB chairman to discuss special items that may require expeditious resolution. Adequate notification shall be provided to all MPCB members.
- h. MPCB meetings may be accomplished either in person, via telephone, or other media such as tele/video conference.

12.2.5 MPCB Responsibilities

- l. The MPCB shall establish and document formal operating procedures.
- m. The MPCB shall develop and maintain a Materials and Processes List (MPL). The MPCB shall review and approve all MPs.
- n. The MPCB shall define MP selection and approval criteria and shall prepare and maintain supporting documents for MP approval.
- o. Through interface with design activity, the MPCB shall ensure the design selection and use of MP that meets the technical program requirements.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

- p. The MPCB shall ensure adequate design margins for mechanical parts used in deliverable end items. The MPCB shall review and approve any proposed deviations from the technical program requirements.
- q. The MPCB shall ensure the review of the results of MRB actions and any other details pertaining to MP. All MP problems shall require disposition by the MPCB.
- r. The MPCB shall ensure the timely identification of long lead MP items and other problem procurements.
- s. The MPCB shall ensure the identification and configuration control of any changes to MPCB approved documentation.
- t. The MPCB shall ensure that laboratories and analysis facilities used for evaluation of MP are reviewed for capabilities of equipment and personnel before performing analyses in compliance with these requirements.
- iii. The MPCB shall prepare and distribute the meeting minutes within 5 working days after the meeting. The minutes shall document all action items, significant areas of disagreement and the basis for all decisions from the meeting.

12.2.6 MPCB Authority

The MPCB shall ensure that all MP items approved for use meet mission reliability and performance requirements. All MPCB decisions shall be documented in the meeting minutes. All supporting technical analysis shall be provided and any additional analysis and tests in accordance with MPCB direction attached to the meeting minutes. The MPCB shall have the authority to approve technical changes to the detail MP requirements when baseline changes fall into one or more of the categories specified below without impact to the item performance in the intended application:

- c. Variation from design and construction requirements of the detail specification.
- d. Screening and lot acceptance tests and acceptance criteria deviations from the detail specifications.

12.3 MANAGEMENT OF MP SELECTION

The developer shall manage the MP in accordance with criteria specified herein. MP shall be selected to assure that mission reliability and performance requirements are met. The developer shall develop a Materials, and Process List and/or an As-designed Materials, and Processes List (ADMPL), see DID 12-2, to start the MPCB activity. The list shall be submitted to the MPCB, ten days prior to the meeting. All non-compliant materials and processes shall be documented on a Material Usage Agreement (MUA), see DID 12-3. All approved MP by MPCB shall be added to the Project Approved MP list within 10 days of approval, and shall be the only source for procurement.

12.3.1 Materials Selection

In order to anticipate and minimize materials problems during space hardware development and operation, when selecting materials and lubricants, the developer shall consider potential problem areas such as radiation effects, thermal cycling, stress corrosion cracking, galvanic corrosion, hydrogen embrittlement, lubrication, contamination of cooled surfaces, composite materials, atomic oxygen, useful life, vacuum outgassing, toxic offgassing, flammability, spacecraft charging effects, and fracture toughness, as well as the properties required by each material usage or application. In cases where it is determine that a MPCB is not required, the GSFC MAE shall assume the role of the MPCB.

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

12.3.2 Compliant Materials

The developer shall use compliant materials in the fabrication hardware to the extent practicable. In order to be compliant, a material must be used in a conventional application and meet the applicable selection criteria identified in Table 12-1. A compliant material does not require an MUA.

Table 12-1: MATERIAL SELECTION CRITERIA

Type Launch	Payload Location	Flammability and Toxic Offgassing	Vacuum Outgassing	Stress Corrosion Cracking (SCC)
STS	Orbiter Crew Compartment	Note 1	No Requirement	Note 5
STS	Cargo Bay	Note 2	Note 4	Note 5
ELV	All	Note 3	Note 4	Note 5

NOTES:

1. Flammability and toxic offgassing requirements as defined in NASA-STD-6001.
2. Flammability and toxic offgassing requirements specified in NSTS 1700.7, Paragraph 209.
3. Hazardous materials requirements, including flammability, toxicity and compatibility as specified in AFSPCMAN91-710V3 "Range Safety User Requirements Manual, section 10.1.
4. Vacuum Outgassing requirements as defined in paragraph 12.3.7.
5. Stress corrosion cracking requirements as defined in Marshall Space Flight Center (MSFC)-STD-3029.

12.3.3 Non-compliant Materials

A material that does not meet the requirements of the applicable selection criteria of Table 12-1, or meet the requirements of Table 12-1, but is used in an unconventional application, will be considered to be a non-compliant material. The proposed use of a non-compliant material requires that a MUA and/or a Stress Corrosion Evaluation Form (see DID 12-4) or developer's equivalent forms (Figures 12-1 and 12-2) be submitted to the MPCB for approval in accordance with the SOW.

12.3.4 Polymeric Materials

The developer shall prepare and submit a polymeric materials list, see DID 12-5, or the developer's equivalent (Figure 12-3). The list shall be submitted to the MPCB for review and approval.

12.3.5 Flammability and Toxic Offgassing

Material flammability and toxic offgassing shall be determined in accordance with the test methods described in NASA-STD-6001, see DID 12-6 and DID 12-7. STS payload materials which will be located in the orbiter crew cabin shall meet the requirements of NASA-STD-6001, see DID 12-6. Materials for payload elements located in the orbiter cargo bay shall meet the requirements of NHB 1700.7, Paragraph 209. ELV payload materials shall meet the requirements of AFSPCMAN91-710V3 "Range Safety User Requirements Manual.

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

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

DIRECTIVE NO. 300-PG-7120.2.2E**EFFECTIVE DATE:** May 3, 2005**EXPIRATION DATE:** May 3, 2010

12.3.6 Vacuum Outgassing

Material vacuum outgassing shall be determined in accordance with American Society for Testing of Materials (ASTM) E-595. In general, a material is qualified on a product-by-product basis. However, GSFC may require lot testing of any material for which lot variation is suspected. Materials provided for outgas testing shall be in cure state or condition which is representative of the flight configuration. In such cases, material approval is contingent upon lot testing. Only materials for use in a vacuum environment, that have a total mass loss (TML) less than 1.00% and a collected volatile condensable mass (CVCMM) less than 0.10% shall be considered compliant. All others are classified as non-compliant and requires an MUA (see 12.3.3).

12.3.7 Shelf-Life-Controlled Materials

Polymeric materials that have a limited shelf-life shall be controlled by a process that identifies the start date (manufacturer's processing, shipment date, or date of receipt, etc.), the storage conditions associated with a specified shelf-life, and expiration date. Materials such as o-rings, rubber seals, tape, uncured polymers, lubricated bearings, lubricants, solder flux, and paints shall be included. The use of materials whose date code has expired requires that the developer demonstrate, by means of appropriate tests, that the properties of the materials have not been compromised for their intended use. Such materials shall be approved by the MPCB. This shall be accomplished by means of a waiver, see DID 12-8. When a limited-life piece part is installed in a subassembly, its usage shall be approved by the MPCB. This shall be accomplished by including the subassembly item in the Limited-Life Plan.

12.3.8 Inorganic Materials

The developer shall prepare and document an inorganic materials list (Figure 12-4) or the developer's equivalent (DID 12-9). The list shall be submitted to the MPCB for review and approval. In addition, the developer may be requested to submit supporting applications data. The criteria specified in MSFC-STD-3029 shall be used to determine that metallic materials meet the stress corrosion cracking criteria. An MUA shall be submitted for each material usage that does not comply with the MSFC-STD-3029 requirements. Additionally, for the MPCB to approve usage of individual materials, a stress corrosion evaluation form or an equivalent developer form or any/all of the information contained in the stress corrosion evaluation form may be required from the developer. Nondestructive evaluation requirements are contained in the STS fracture control requirements.

The use of tin, zinc, and cadmium platings in any flight application requires an MUA prior to use of that material. Bright tin, cadmium, and zinc platings have the potential for developing whisker growths. For tin, these have been measured up to 12.5 microns in diameter and up to 10 mm in length. These whiskers can result in short circuits, plasma arcing, and debris generation within the spacecraft. Zinc and cadmium platings also evaporate in vacuum environments and may redeposit on optics or electronics, posing potential risks to flight hardware.

12.3.9 Fasteners

As part of the materials list approval process, the MPCB will approve all flight fasteners. Towards this end, the developer shall provide all information required by the MPCB to ensure its ability to concur with the flightworthiness of flight fasteners. The developer shall comply with the procurement documentation and test requirements for flight hardware and critical ground support equipment fasteners contained in 541-PG-8072.1.2, GSFC Fastener Integrity Requirements. The developer shall prepare a Fastener Control Plan, see DID 12-10, for submission to the MPCB. Material test reports for fastener lots shall be submitted to the MPCB for information. Fasteners made of plain carbon or low alloy steel shall be protected from corrosion. When plating is specified, it shall be compatible with the space environment. On steels harder than RC 33, plating shall be applied by a process that is not embrittling to the steel.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

12.3.10 Lubrication

The developer shall prepare and document a lubrication usage list (Figure 12-5) or the developer's equivalent (DID 12-11). The list shall be submitted to the MPCB for review and approval. The developer may be requested to submit supporting applications data. Lubricants shall be selected for use with materials on the basis of valid test results that confirm the suitability of the composition and the performance characteristics for each specific application, including compatibility with the anticipated environment and contamination effects. All lubricated mechanisms shall be qualified by life testing in accordance with the life test plan or heritage of an identical mechanism used in identical applications, see DID 12-12 Life Test Plan for Lubricated Mechanisms.

12.3.11 Process Selection

The developer shall prepare and document a materials processes utilization list (DID 12-13) or the developer's equivalent (Figure 12-6). The list shall be submitted to the MPCB for review and approval. A copy of any process shall be submitted for review upon request. Manufacturing processes (e.g., lubrication, heat treatment, welding and chemical or metallic coatings) shall be carefully selected to prevent any unacceptable material property changes that could cause adverse effects of materials applications.

12.4 MANAGEMENT OF MP ENGINEERING REQUIREMENTS

12.4.1 System Design.

The MPCB is responsible for ensuring that MP used throughout the system meets the application, reliability, quality, and survivability requirements, as derived from the system level requirements. MP engineering shall review and approve all drawings and specifications (A level, B level, device detail specifications, etc.) to ensure that MP requirements are met. All MP shall be selected to meet their intended application in the predicted mission environment (radiation, thermal, AO, UV, etc.).

12.4.2 Reuse of Materials

Materials which have been installed in an assembly, and are then removed from the assembly for any reason, shall not be used again in any item of flight or spare hardware without prior approval of the MPCB based on the submission of evidence that this practice does not degrade the system performance.

12.4.3 Traceability and Lot Control.

The developer shall develop and maintain a traceability and lot control plan in accordance with the requirements specified below and approved by the MPCB. When given a lot date code or batch number, the developer shall be capable of determining the unique piece of equipment (black box level) by serial number in which the part or material is installed or used. Traceability to the serial number of an individual device or to a lower level of assembly shall be as determined and specified by the MPCB. Traceability shall be maintained for all flight printed circuit boards (PCBs) so that part number, serial number, and lot date code information is known for all PCBs; in addition, any vendor identification necessary to trace the PCBs to their representative coupons shall be maintained and provided as needed.

NOTE: Numbering is incorrect for following sections of 12.4

12.4.3.1 Mechanical Materials

One hundred percent (100%) lot traceability is required for materials used in applications where a failure could jeopardize component or mission success. Traceability and production or batch lot control for materials used in other applications shall be maintained where risk and cost so dictate.

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

12.4.3.2 Raw Materials

Raw materials purchased by the developer shall be accompanied by the results of non-destructive, chemical and physical tests, or Certificate of Compliance, see DID 12-14. These requirements also apply to any supplier used by the developer.

12.4.4 Incoming Inspection Requirements

Each developer shall perform, or be responsible for the performance of applicable incoming tests and inspections of materials to ensure that they meet the requirements of the procurement specification. Unless previously accomplished and accepted by government or developer field personnel, incoming testing and inspections shall be accomplished upon receipt of the materials. The inspection and testing of materials shall be conducted in accordance with a plan approved by the MPCB.

12.4.4.1 Shelf-Life Control

The developer shall develop a shelf life control program that identifies the shelf life limitations for all materials to be stored. This plan shall specify the length of time required and minimum requirements for re-inspection, retest, & any other action required to ensure maintenance of space flight quality and reliability. The plan shall be reviewed and approved by the MPCB and controls shall be identified to ensure that the plan is followed before materials are issued to assembly.

12.4.4.1.1 Material Shelf Life Control

In addition to general age limitation considerations, the plan shall identify any specific temperature and humidity requirements for storage and any associated limitations on life. Any special environmental requirements (e.g., storage in dry nitrogen) shall be identified.

12.5 MANAGEMENT OF MATERIALS AND PROCESSES PROCUREMENT

12.5.1 Supplier and Vendor Selection and Surveillance

The MPCB is responsible for the selection and qualification of MP suppliers, vendors, laboratories and manufacturers.

12.5.2 MP Supplier and Manufacturer Surveillance (Monitoring)

The MPCB shall establish a policy and procedures for the periodic surveillance and auditing of suppliers, vendors, laboratories and manufacturers to ensure compliance to procurement, quality, reliability and survivability requirements. Developer surveillance of laboratories, suppliers, vendors, and manufacturers that have been approved as a Qualified Manufacturer's List (QML) program for products listed in the space quality baseline is not required. When surveillance/audit data is available from other sources (e.g. other developer programs, other developers/s sub-developers, independent audits reports, etc.) the developer may utilize the results of the data contingent on the review and approval by the MPCB. Acceptability of the data shall be based on technical considerations, as well as timeliness and confidence in the source of the data.

12.5.3 Coordinated Procurements

Implementation of a coordinated procurement program is highly encouraged. When appropriate, the MPCB shall establish policies for the use of coordinated procurements for all developers and sub-developers use. This may include the use of common specifications, management responsibilities, purchase agreements, monitoring, and

CHECK THE GSFC DIRECTIVES MANAGEMENT SYSTEM AT

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

quality assurance. The MPCB (and procurement organizations) may ensure that a master purchase agreement allows authorized sub-developers to initiate their own procurements within the scope and framework of the master purchase agreement.

12.6 GOVERNMENT FURNISHED EQUIPMENT

MP contained in unmodified government furnished equipment used in the end item of the contract shall not be subject to MP control.

12.7 COMMERCIAL OFF-THE-SHELF ITEM EQUIPMENT

The requesting user shall demonstrate to the MPCB that the COTS items meet the quality, reliability, environmental and survivability (if required) requirements of the contract end item for the intended application.

12.8 MP QUALIFICATION.

12.8.1 General

All MP, including any processes developed to accomplish rework or retrofit, shall be qualified for program use. Only qualified MP shall be used on flight hardware. For each non-qualified MP, the developer(s) shall prepare a qualification plan and procedure. The qualification plan shall identify all conditions and testing necessary to meet the program and mission reliability and qualification requirements. These plans and procedures shall be reviewed and approved by the MPCB. A summary report of qualification test results shall be submitted to the MPCB. The MPCB shall maintain an up-to-date listing of the qualification status of all program MP. Test methods used for qualification of MP shall be in accordance with applicable specifications and shall include test methods for any additional tests necessary to fully qualify the material for its intended use in the system.

Qualification of MP shall be expedited by the following:

- d. Initial selection of MP using applicable military specified MP previously qualified for use on space programs.
- e. Proof testing of all materials to the program requirement levels.
- f. Vendor audits and certification.

12.8.2 Manufacturing Baseline

As part of the qualification plan for each non-qualified MP item, the developer(s) shall insure that the non-qualified MP item supplier has an established manufacturing baseline and review the manufacturing baseline for compliance to the program's technical requirements. The manufacturing baseline for all other MP shall be reviewed and controlled.

12.8.3 Qualification by Extension

Materials, or processes may be qualified by extension, when supporting data is available and shows that either of the following criteria are met:

- c. The material, or process was successfully used in a prior but recent space application in which the application environment conditions of use and test were, at least, as severe as those required of the candidate MP for qualification.
- d. The material design and construction is the same as the previously qualified material. The material is manufactured by the same manufacturing facility to the same manufacturing baseline as the previously

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

qualified material, and the utilization of the material does not result in critical stresses or mechanical strain (such as due to thermal mismatch) greater than the previously qualified material.

12.9 FAILURE ANALYSIS

Failure analysis shall be performed on material failures experienced during assembly and testing. Failures shall be analyzed to the extent necessary to understand the failure mode and cause, to detect and correct out-of-control processes, to determine the necessary corrective actions, and to determine lot disposition. When required, a failure analysis report shall be prepared and documented. The MPCB shall determine and implement appropriate corrective action for each MP failure. All failures, and the results of final failure analysis, shall be documented. Failure analysis reports shall be retrievable for the duration of the contract, and shall be available to GSFC.

12.10 HANDLING

Handling (including storage) procedures shall be instituted to prevent material degradation. The handling procedures shall be retained through inspection, kitting, and assembly and shall be identified on "build to" documentation. The following criteria shall be used as a minimum for establishing handling and storage procedures for materials:

- a. Control of environment, such as temperature, humidity, contamination, and pressure.
- b. Measures and facilities to segregate and protect materials routed to different locations such as, to the materials review crib, or to a laboratory for inspection, or returned to the manufacturer from unaccepted shipments.
- c. Control measures to limit personnel access to materials during receiving inspection and storage.
- d. Facilities for interim storage of materials.
- e. Provisions for protective cushioning, as required, on storage area shelves, and in storage and transportation containers.
- f. Protective features of transportation equipment design to prevent packages from being dropped or dislodged in transit
- g. Protective bench surfaces on which materials are handled during operations such as test, assembly, inspection, and organizing kits.
- h. Unique materials criteria.
- i. Materials used in the handling of flight hardware (i.e. gloves, finger cots, wipes, swabs, etc.) shall be verified for cleanliness so that contact with hardware does not result in contamination of critical surfaces*.

12.11 DATA RETENTION

The program shall maintain records or incoming inspection tests, lot qualification and acceptance test data, traceability data and other data as determined by the MPCB for a period of time specified by the GSFC.

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

FIGURE 12-1: MUA

MATERIAL USAGE AGREEMENT			USAGE AGREEMENT NO.:			PAGE OF	
PROJECT:		SUBSYSTEM:		ORIGINATOR:		ORGANIZATION:	
DETAIL DRAWING		NOMENCLATURE		USING ASSEMBLY		NOMENCLATURE	
MATERIAL & SPECIFICATION				MANUFACTURER & TRADE NAME			
USAGE	THICKNESS	WEIGHT	EXPOSED AREA	ENVIRONMENT			
				PRESSURE	TEMPERATURE	MEDIA	
APPLICATION:							
RATIONALE:							
ORIGINATOR:				PROJECT MANAGER:			DATE:

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

FIGURE 12-2: STRESS CORROSION EVALUATION FORM

1. Part Number _____
2. Part Name _____
3. Next Assembly Number _____
4. Manufacturer _____
5. Material _____
6. Heat Treatment _____
7. Size and Form _____
8. Sustained Tensile Stresses-Magnitude and Direction
 - a. Process Residual _____
 - b. Assembly _____
 - c. Design, Static _____
9. Special Processing _____
10. Weldments
 - a. Alloy Form, Temper of Parent Metal _____
 - b. Filler Alloy, if none, indicate _____
 - c. Welding Process _____
 - d. Weld Bead Removed - Yes (), No () _____
 - e. Post-Weld Thermal Treatment _____
 - f. Post-Weld Stress Relief _____
11. Environment _____
12. Protective Finish _____
13. Function of Part _____
14. Effect of Failure _____
15. Evaluation of Stress Corrosion Susceptibility _____
16. Remarks: _____

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

DIRECTIVE NO. 300-PG-7120.2.2D Page 83 of 172
 EFFECTIVE DATE: July 21, 2004
 EXPIRATION DATE: July 21, 2009

GSFC 18-59A 3/78 **FIGURE 12-3: POLYMERIC MATERIALS AND COMPOSITES USAGE LIST**

POLYMERIC MATERIALS AND COMPOSITES USAGE LIST

SPACECRAFT _____ SYSTEM/EXPERIMENT _____ GSFC T/O _____

DEVELOPER/DEVELOPER _____ ADDRESS _____

PREPARED BY _____ PHONE _____ DATE _____
 DATE PREPARED _____

GSFC MATERIALS EVALUATOR _____ PHONE _____ DATE RECEIVED _____
 DATE EVALUATED _____

ITEM NO.	MATERIAL IDENTIFICATION ⁽²⁾	MIX FORMULA ⁽³⁾	CURE ⁽⁴⁾	AMOUNT CODE	EXPECTED ENVIRONMENT ⁽⁵⁾	REASON FOR SELECTION ⁽⁶⁾	OUTGASSING VALUES	
							TML	CVC/M
<p>NOTES</p> <ol style="list-style-type: none"> List all polymeric materials and composites applications utilized in the system except lubricants that should be listed on polymeric and composite materials usage list. Give the name of the material, identifying number and manufacturer. Example: Epoxy, Epon 828, E. V. Roberts and Associates Provide proportions and name of resin, hardener (catalyst), filler, etc. Example: 828/V140/Stiffake 135 as 5/5/38 by weight Provide cure cycle details. Example: 8 hrs. at room temperature + 2 hrs. at 150C Provide the details of the environment that the material will experience as a finished S/C component, both in ground test and in space. List all materials with the same environment in a group. Example: TV: -20C/+60C, 2 weeks, 10E-5 torr, ultraviolet radiation (UV) Storage: up to 1 year at room temperature Space: -10C/+20C, 2 years, 150 mile altitude, UV, electron, proton, atomic oxygen Provide any special reason why the materials were selected. If for a particular property, please give the property. Example: Cost, availability, room temperature curing or low thermal expansion. 								

Area, cm ²	Vol., cc	Wt., gm
1 0-1	A 0-1	a 0-1
2 2-100	B 2-50	b 2-50
3 101-1000	C 51-500	c 51-500
4 >1000	D >500	d >500

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

GSFC 18-59B 3/78 **FIGURE 12-4: INORGANIC MATERIALS AND COMPOSITES USAGE LIST**

INORGANIC MATERIALS AND COMPOSITES USAGE LIST		GSFC T/O _____					
SPACECRAFT DEVELOPER/DEVELOPER	SYSTEM/EXPERIMENT	ADDRESS	PHONE				
PREPARED BY _____	DATE PREPARED _____	DATE RECEIVED _____	DATE EVALUATED _____				
GSFC MATERIALS EVALUATOR _____	PHONE _____	DATE RECEIVED _____	DATE EVALUATED _____				
ITEM NO.	MATERIAL IDENTIFICATION ⁽¹⁾	CONDITION ⁽²⁾	APPLICATION ⁽⁴⁾ OR OTHER SPEC. NO.	EXPECTED ENVIRONMENT ⁽³⁾	S.C.C. TABLE NO.	MUA NO.	NDE METHOD
	<p>NOTES:</p> <ol style="list-style-type: none"> 1. List all inorganic materials (metals, ceramics, glasses, liquids, and metal/ceramic composites) except bearing and lubrication materials that should be listed on Form 18-59C. 2. Give materials name, identifying number manufacturer. Example: <ol style="list-style-type: none"> a. Aluminum 6061-T6 b. Electroless nickel plate, Enplate Ni 410, Enthone, Inc. c. Fused silica, Corning 7940, Corning Class Works 3. Give details of the finished condition of the material, heat treat designation (hardness or strength), surface finish and coating, cold worked state, welding, brazing, etc. Example: <ol style="list-style-type: none"> a. Heat-treated to Rockwell C 60 hardness, gold electroplated, brazed. B. Surface coated with vapor deposited aluminum and magnesium fluoride c. Cold worked to full hane condition, TIG welded and electroless nickel-plated. 4. Give details of where on the spacecraft the material will be used (component) and its function. Example: Electronics box structure in attitude control system, not hermetically sealed. 5. Give the details of the environment that the material will experience as a finished S/C component, both in ground test and in space. Exclude vibration environment. List all materials with the same environment in a group. Example: T/V: -20C/+60C, 2 weeks, 10E-5 torr, Ultraviolet radiation (UV) Storage: up to 1 year at room temperature Space: -10C/+20C, 2 years, 150 miles altitude, UV, electron, proton, Atomic Oxygen 						

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

DIRECTIVE NO. 300-PG-7120.2.2E

Page 85 of 172

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

FIGURE 12-5: LUBRICATION USAGE LIST

LUBRICATION USAGE LIST							
SPACECRAFT DEVELOPED/DEVELOPER _____		SYSTEM/EXPERIMENT _____		GSFC T/O _____			
PREPARED BY _____		ADDRESS _____		DATE _____			
GSFC MATERIALS EVALUATOR _____		PHONE _____		DATE RECEIVED _____			
PHONE _____		DATE PREPARED _____		DATE EVALUATED _____			
ITEM NO.	COMPONENT TYPE, SIZE MATERIAL ⁽¹⁾	COMPONENT MANUFACTURER & MFR. IDENTIFICATION	PROPOSED LUBRICATION SYSTEM & AMT. OF LUBRICANT	TYPE & NO. OF WEAR CYCLES ⁽²⁾	SPEED, TEMP., ATM. OF OPERATION ⁽³⁾	TYPE OF LOADS & AMT.	OTHER DETAILS ⁽⁴⁾
NOTES							
(1) BB = ball bearing, SB = sleeve bearing, G = gear, SS = sliding surfaces, SEC = sliding electrical contacts. Give generic identification of materials used for the component, e.g., 440C steel, PTFE.							
(2) CUR = continuous unidirectional rotation, CO = continuous oscillation, IR = intermittent rotation, IO = intermittent oscillation, SO = small oscillation, (<30°), LO = large oscillation (>30°), CS = continuous sliding, IS = intermittent sliding. No. of wear cycles: A(1-10 ²), B(10 ² -10 ⁴), C(10 ⁴ -10 ⁶), D(>10 ⁶)							
(3) Speed: RPM = revs./min., OPM = oscillations/min., VS = variable speed CPM = cm/min. (sliding applications). Temp. of operation, max. & min., °C Atmosphere: vacuum, air, gas, sealed or unsealed & pressure							
(4) Type of loads: A = axial, R = radial, T = tangential (gear load). Give amount of load.							
(5) If BB, give type and material of ball cage and number of shields and specified ball groove and ball finishes. If G, give surface treatment and hardness. If SB, give dia. of bore and width. If torque available is limited, give approx. value.							

GSFC 18-59C 3/78

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

GSFC Form 3-18 (10/01)

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

FIGURE 12-6: MATERIALS PROCESS UTILIZATION LIST

MATERIALS PROCESS UTILIZATION LIST					
SPACECRAFT _____	SYSTEM/EXPERIMENT _____	GSFC T/O _____			
DEVELOPER/DEVELOPER _____	ADDRESS _____				
PREPARED BY _____	PHONE _____	DATE PREPARED _____			
GSFC MATERIALS EVALUATOR _____	PHONE _____	DATE RECEIVED _____	DATE EVALUATED _____		
ITEM NO.	PROCESS TYPE ⁽¹⁾	DEVELOPER SPEC. NO. ⁽²⁾	MIL., ASTM., FED. OR OTHER SPEC. NO.	DESCRIPTION OF MAT'L PROCESSED ⁽³⁾	SPACECRAFT/EXP. APPLICATION ⁽⁴⁾
<p>NOTES</p> <p>(1) Give generic name of process, e.g., anodizing (sulfuric acid).</p> <p>(2) If process is proprietary, please state so.</p> <p>(3) Identify the type and condition of the material subjected to the process. E.g., 6061-T6</p> <p>(4) Identify the component or structure of which the materials are being processed. e.g., Antenna dish</p>					

GSFC 18-59D 3/78

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

DIRECTIVE NO. 300-PG-7120.2.2D
EFFECTIVE DATE: July 21, 2004
EXPIRATION DATE: July 21, 2009

Chapter 13. Contamination Control Requirements

13.1 GENERAL

The developer shall plan and implement a contamination control program appropriate for the hardware. The program shall establish the specific cleanliness requirements and delineate the approaches to be followed in a Contamination Control Plan (CCP), see DID 13-1.

Contamination includes all materials of molecular and particulate nature whose presence degrades hardware performance. The source of the contaminant materials may be the hardware itself, the test facilities, and the environments to which the hardware is exposed.

13.2 CONTAMINATION CONTROL VERIFICATION PROCESS

The developer shall develop a contamination control verification process. The verification process shall be performed in order

- a. Determination of contamination sensitivity;
- b. Determination of a contamination allowance;
- c. Determination of a contamination budget;
- d. Development and implementation of a contamination control plan.

Each of the above activities shall be documented and submitted to GSFC for concurrence/approval.

13.3 CONTAMINATION CONTROL PLAN

The developer shall prepare a CCP that describes the procedures that will be followed to control contamination. It shall establish the implementation and describe the methods that will be used to measure and maintain the levels of cleanliness required during each of the various phases of the item's lifetime. In general, all mission hardware should be compatible with the most contamination-sensitive components.

13.4 MATERIAL OUTGASSING

In accordance with ASTM E595, NASA RP 1124 may be used as a guide. Individual material outgassing data shall be established based on each component's operating conditions. Established material outgassing data shall be verified and shall be reviewed by GSFC.

13.5 THERMAL VACUUM BAKEOUT

The developer shall perform thermal vacuum bakeouts of all hardware. The parameters of such bakeouts (e.g., temperature, duration, outgassing requirements, and pressure) must be individualized depending on materials used, the fabrication environment, and the established contamination allowance. Thermal vacuum bakeout results shall be verified and shall be reviewed by GSFC.

13.6 HARDWARE HANDLING

The developer shall practice cleanroom standards in handling hardware. The contamination potential of material and equipment used in cleaning, handling, packaging, tent enclosures, shipping containers, bagging (e.g., anti-static film materials), and purging shall be described in detail for each subsystem or component at each phase of assembly, integration, test, and launch.

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

Chapter 14. Applicable Documents List

<u>DOCUMENT</u>	<u>DOCUMENT TITLE</u>
ANSI/ASQC Q9000-3	Quality Management and Quality Assurance Standards – Part 3: Guidelines for the Application of ISO 9001 to the Development, Supply and Maintenance of Software
ANSI/ISO/ASQ Q9001:2000	American National Standard Quality Systems - Model for Quality Assurance in Design, Development, Production, Installation and Servicing
ANSI/ESD S20.20	ESD Association Standard for the Development of an Electrostatic Discharge Control Program for protection of electrical and electronic parts, assemblies, and equipment (excluding electrically initiated explosive devices).
ANSI/IPC-A-600	Acceptability of Printed Boards.
ASTM E-595	Standard Test Method for Total Mass Loss and Collected Volatile Condensable Materials from Outgassing in a Vacuum Environment
EWR 127-1	Eastern and Western Range Safety Requirements
FAR	Federal Acquisition Regulations
GEVS-SE	General Environmental Verification Specification for STS and ELV Payloads, Subsystems and Components.
GMI 1700.2	Goddard Space Flight Center Health and Safety Program
GPG 8621.2	Processing Mishap, Incident, Hazard, and Close Call Reports

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

GPG 8621.3	Mishap, Incident, Hazard, and Close Call Investigation
GPG 8700.4	Technical Review Program
GPG 8700.6	Engineering Peer Reviews
GSFC S-312-P003	Procurement Specification for Rigid Printed Boards for Space Applications and Other High Reliability Uses
GSFC EEE-INST-002	Instructions for EEE Parts Selection, Screening, and Qualification and Derating
IEEE STD 610.12	IEEE Standard Glossary for Software Engineering Terminology
IEEE STD 730	IEEE Standard for Software Quality Assurance Plans
EEE STD 982.2	IEEE Guide for the Use of IEEE Standard Dictionary of Measures to Produce Reliable Software
IPC A-600	Acceptability of Printed Boards
IPC-A-610	Acceptability of Electronic Assemblies
IPC D-275	Design Standard for Rigid Printed Boards and Rigid Printed Board Assemblies
IPC/EIA J-STD-001	Requirements for Soldered Electrical and Electronic Assemblies
IPC-2221	Generic Standard on Printed Board Design

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

IPC-2222	Sectional Design Standard for Rigid Organic Printed Boards
IPC-2223	Sectional Design Standard for Flexible Printed Boards
IPC-6011	Generic Performance Specifications for Printed Boards
IPC-6012	Qualification and Performance Specification for Rigid Printed Boards
IPC-6013	Qualification and Performance Specification for Flexible Printed Boards
IPC-6018	Microwave End Product Board Inspection and Test
ISO 17025	General Requirements for the Competence of Testing and Calibration Laboratories
JSC 07700	Shuttle Orbiter/Cargo Standard Interfaces
JSC 26943	Guidelines for the Preparation of Payload Flight Safety Data Packages and Hazard Reports
KHB 1700.7	Space Transportation System Payload Ground Safety Handbook
KHB 1710.2	Kennedy Space Center Safety Practices Handbook
MIL-HDBK-217	Reliability Prediction of Electronic Equipment
MIL-HDBK-470	Designing and Developing Maintainable Products and Systems

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

MIL-HDBK-472	Maintainability Prediction
MIL-STD-461	Electromagnetic Emission and Susceptibility Requirement for Control of Electromagnetic Interference
MIL-STD-756	Reliability Modeling and Prediction
MIL-STD-1629	Procedures for Performing a Failure Mode Effects and Criticality Analysis
MSFC CR 5320.9	Payload and Experiment Failure Mode Effects Analysis and Critical Items List Ground Rules
MSFC-HDBK-527	Material Selection List for Space Hardware Systems
MSFC-SPEC-522	Design Criteria for Controlling Stress Corrosion Cracking
NASA RP-1124	Outgassing Data for Selecting Spacecraft Materials
NASA RP-1161	Evaluation of Multi-layer Printed Wiring Boards by Metallographic Techniques
NHB 1700.1	NASA Safety Policy and Requirements Document
NHB 1700.7	Safety Policy and Requirements for Payloads using the Space Transportation System
NHB 8060.1	Flammability, Odor, and Offgassing Requirements and Test Procedures for Materials in Environments That Support Combustion

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

NPD 8700.1	NASA Policy for Safety & Mission Success
NPD 8710.3	NASA Policy for Limiting Orbital Debris Generation
NPG 7120.5	NASA Program and Project Management Processes and Requirements
NPG 8000.4	Risk Management Procedures and Guidelines
NPG 8715.3	NASA Safety Manual
NASA-STD-2100-91	Software Documentation Standard
NASA-STD-2201-93	Software Assurance Standard
NASA-STD-2202-93	Software Formal Inspections Standard
NASA-STD-6001	Flammability, Odor, Off-gassing and Compatibility Requirements & Test Procedures for Materials in Environments that Support Combustion
NASA-STD 8719.13	NASA Software Safety Standard
NASA-STD 8719.14	Guidelines and Assessment Procedures for Limiting Orbital Debris
NASA-STD-8739.1	Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies
NASA-STD-8739.2	Workmanship Standard for Surface Mount Technology

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

NASA-STD-8739.3	Workmanship Standard for Soldered Electrical Connections
NASA-STD-8739.4	Workmanship Standard for Crimping, Interconnecting Cables, Harnesses and Wiring
NASA-STD-8739.5	Workmanship Standard for Fiber Optic Terminations, Cable Assemblies and Installation
NSS 1740.13	NASA Software Safety Standard
NSS 1740.14	Guidelines and Assessment Procedures for Limiting Orbital Debris
NSTS 1700.7	Safety Policy and Requirements for Payloads using the International Space Station
NSTS 14046	Payload Verification
NSTS 22648	Flammability Configuration Analysis for Spacecraft Applications
NSTS/ISS 13830	Payload Safety Review and Data Submittal Requirements
NSTS/ISS 18798	Interpretations of NSTS/ISS Payload Safety Requirements
RSM-93	Range Safety Manual for GSFC/WFF
S-302-89-01	Procedures for Performing a Failure Mode and Effects Analysis
S-311-M-70	Specification for Destructive Physical Analysis

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

DIRECTIVE NO. 300-PG-7120.2.2E
EFFECTIVE DATE: May 3, 2005
EXPIRATION DATE: May 3, 2010

SAE AS9100	Aerospace Standard, Quality Systems Model for Quality Assurance, Design, Development, Production, Installation and Servicing
SAE JA1002	Software Reliability Program Standard
SSD TD-0005	Pegasus Design Safety Requirements Document
SSD TD-0018	Pegasus Safety Requirements Document for Ground Operations
300-PG-7120.2.1	Mission Assurance Guidelines Implementation
541-PG-8072.1.2	GSFC Fastener Integrity Requirements
5405-048-98	Mechanical Systems Center Safety Manual

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

DIRECTIVE NO. 300-PG-7120.2.2E
 EFFECTIVE DATE: May 3, 2005
 EXPIRATION DATE: May 3, 2010

Chapter 15. Data Item Descriptions

15.1 DID 2-1: QUALITY MANUAL

Title: Quality Manual	CDRL No.: 2-1
Reference: Paragraphs 2.1	
Use: Documents the developer's quality management system.	
Related Documents: ANSI/ISO/ASQC Q9001:2000, SAE AS9100, and ISO 10013.	
Place/Time/Purpose of Delivery: Provide with proposal for GSFC review. Provide Quality Manual updates to GSFC Project Office for review prior to implementation. or Provide with proposal for information along with evidence of third party certification or registration of the developer's quality management system by an accredited registrar.	
Preparation Information: Prepare a Quality Manual addressing all applicable requirements of relevant quality standard (Q9001, AS9100, etc). Refer to ISO 10013 Quality Manual Development Guide for further guidelines on preparation of a quality manual. The Quality Manual shall contain: <ol style="list-style-type: none"> the title, approval page, scope and the field of application; table of contents; introductory pages about the organization concerned and the manual itself; the quality policy and objectives of the organization; the description of the organization, responsibilities and authorities, including the organization responsible for the EEE parts, materials, reliability, safety and test requirements implementation; a description of the elements of the quality system, developer policy regarding each element and developer implementation procedure for each clause or reference(s) to approved quality system procedures; system level procedures shall address the implementation of all requirements cited in this document. a definitions section, if appropriate; an appendix for supportive data, if appropriate. Quality Manual distribution and changes shall be implemented by a controlled process. The Quality Manual shall be maintained/updated by the developer throughout the life of the contract.	

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

15.2 DID 2-2: PROBLEM FAILURE REPORT

Title: Problem Failure Report (PFR)	CDRL No.: 2-2
Reference: Paragraph 2.2.3	
Use: Used to record instances of failure, and change in status of failed item.	
Related Documents: ANSI/ISO/ASQC Q9001 Quality Management Systems; GPR 5340.2 Control of Nonconformances.	
Place/Time/Purpose of Delivery: <ol style="list-style-type: none"> Deliver PFR to the GSFC Project Office within 24 hours of each occurrence by hard copy or in electronic format. Deliver updated PFR to the GSFC Project Office. Provide to GSFC Project Office for approval immediately after developer closure. 	
Preparation Information: Document all failures on existing developer PFR form that identifies all relevant failure information. Relevant failure information includes (who, what, when, and where): <ol style="list-style-type: none"> Identification of project, system, and sub-system. Identification of failed assembly, sub-assembly, or part. Description of failed item. Identification of next higher assembly. Description of failure including activities leading up to failure, if known. Names and contact information of individuals involved in failure. Date and time of failure. Status of failed item. Individual originating report including contact information. Date PFR submitted. 	

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

15.3 DID 3-1: SYSTEM SAFETY PROGRAM PLAN

Title: System Safety Program Plan	CDRL No.: 3-1
Reference: MAG, Paragraph 3.2.1, 5.2.2	
Use: The approved System Safety Program Plan (SSPP) provides a formal basis of understanding between the GSFC OSSMA and the developer on how the System Safety Program will be conducted to meet the applicable launch range safety requirements (ELV launch) or NSTS 1700.7B (Shuttle). The SSPP accounts for all contractually required tasks and responsibilities on an item-by-item basis. The SSPP describes in detail the tasks and activities of system safety management and engineering required to identify, evaluate, and eliminate or control hazards by reducing the associated risk to a level acceptable to Range Safety throughout the system life cycle.	
Related Documents: <ol style="list-style-type: none"> a. 302-PG-7120.2.1, Mission Assurance Guidelines Implementation b. AFSPCMAN 91-710, Range Safety User Requirements c. JMR 002, Launch Vehicle Payload Safety Requirements d. NPG 7120.5, Program and Project Management Processes and Requirements e. NPD 8700.1, NASA Policy for Safety and Mission Success f. NSTS 1700.7B, Safety Policy and Requirements for Payloads Using the STS g. CSG-RS-10A-CN Centre Spatial Guyanais (CSG) Safety Regulations Vol. 1: General Rules h. CSG-RS-21A-CN CSG Safety Regulations Vol. 2 Pt. 1: Specific Rules: Ground Installations i. CSG-RS-22A-CN CSG Safety Regulations Vol. 2 Pt. 2: Specific Rules: Spacecraft 	
Place/Time/Purpose of Delivery: <ul style="list-style-type: none"> • SSPP - The Range User submits the SSPP to GSFC OSSMA for review and approval at SRR or first program review (whichever comes first). • GSFC OSSMA approves the SSPP before its submittal to the launch range. 	

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

Product Preparation:

Provide a detailed SSPP to describe how the project will implement a safety program in compliance with launch range requirements. Integration of system/facility safety provisions into the SSPP is vital to the early implementation and ultimate success of the safety effort. The SSPP shall

- a.* Define the required safety documentation, applicable documents, associated schedules for completion, roles and responsibilities on the project, methodologies for the conduct of any required safety analyses, reviews, and safety package.
- b.* Provide for the early identification and control of hazards to personnel, facilities, support equipment, and the flight system during all stages of project development including design, fabrication, test, transportation and ground activities.
- c.* Ensure the program undergoes a safety review process that meets the requirements of NASA-STD-8719.8, "Expendable Launch Vehicle Payloads Safety Review Process Standard". Address compliance with the system safety requirements of range requirements.
- d.* Address compliance with the baseline industrial safety requirements of the institution, range safety, applicable Industry Standards to the extent practical to meet NASA and OSHA design and operational needs (i.e. NASA STD 8719.9 Std. for Lifting Devices and Equipment), and any special contractually imposed mission unique obligations (including applicable safety requirements).
- e.* Address the software safety effort to identify and mitigate safety-critical software products in compliance with NASA-STD-8719.13 "NASA Software Safety Standard".

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

15.4 DID 3-2: SAFETY REQUIREMENT COMPLIANCE CHECKLIST

Title: Safety Requirements Compliance Checklist	CDRL No.: 3-2
Reference: MAG, Paragraph 3.2.2	
Use: The checklist indicates for each requirement if the proposed design is compliant, non-compliant but meets intent, non-compliant (waiver required) or non-applicable.	
Related Documents: <ul style="list-style-type: none"> a. AFSPCMAN 91-710, Range Safety User Requirements b. JMR 002, Launch Vehicle Payload Safety Requirements 	
Place/Time/Purpose of Delivery: Deliver the Safety Requirements Compliance Checklist for <u>instrument/subsystems</u> with the SAR at PDR + 30 days. Deliver the Safety Requirements Compliance Checklist for the <u>spacecraft</u> with the SDP or MSPSP at PDR + 30 days (S/C or Mission).	
Preparation Information: A compliance checklist of all design, test, analysis, and data submittal requirements shall be provided. The following items are included with a compliance checklist: <ol style="list-style-type: none"> 1. Criteria/requirement. 2. System. 3. Compliance. 4. Noncompliance. 5. Not applicable. 6. Resolution. 7. Reference. 8. Copies of all Range Safety approved non-compliances including waivers and equivalent levels of safety certifications 	

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

DIRECTIVE NO. 300-PG-7120.2.2E

EFFECTIVE DATE: May 3, 2005

EXPIRATION DATE: May 3, 2010

15.5 DID 3-3: PRELIMINARY HAZARD ANALYSIS

Title:	CDRL No.:
Preliminary Hazard Analysis	3-3
Reference:	
MAG, Paragraph 3.2.3.1	
Use:	
<p>The Preliminary Hazard Analysis (PHA) is used to obtain an initial risk assessment and identify safety critical areas of a concept or system. Based on the best available data, including mishap data from similar systems and other lessons learned. Hazards associated with the proposed design or function shall be evaluated for hazard severity, hazard probability, and operational constraint. Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to an acceptable level shall be included.</p> <p>The PHA identifies safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to a level acceptable to GSFC OSSMA,</p>	
Related Documents:	
<ul style="list-style-type: none"> a. AFSPCMAN 91-710, Range Safety User Requirements b. JMR 002, Launch Vehicle Payload Safety Requirements b. NPR 8715.3, NASA Safety Manual c. MIL-STD-882, System Safety Program Requirements (provides guidance) 	
Place/Time/Purpose of Delivery:	
<p>Deliver the PHA as a component of the SAR, SDP, or MSPSP. <i>(Choose either a. or b.)</i></p> <ul style="list-style-type: none"> a. Deliver the PHA for <u>instruments or subsystems</u> with the SAR at PDR + 30 days. b. Deliver the PHA for the <u>spacecraft</u> with the SDP or MSPSP at PDR + 30 days (S/C or Mission). 	

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