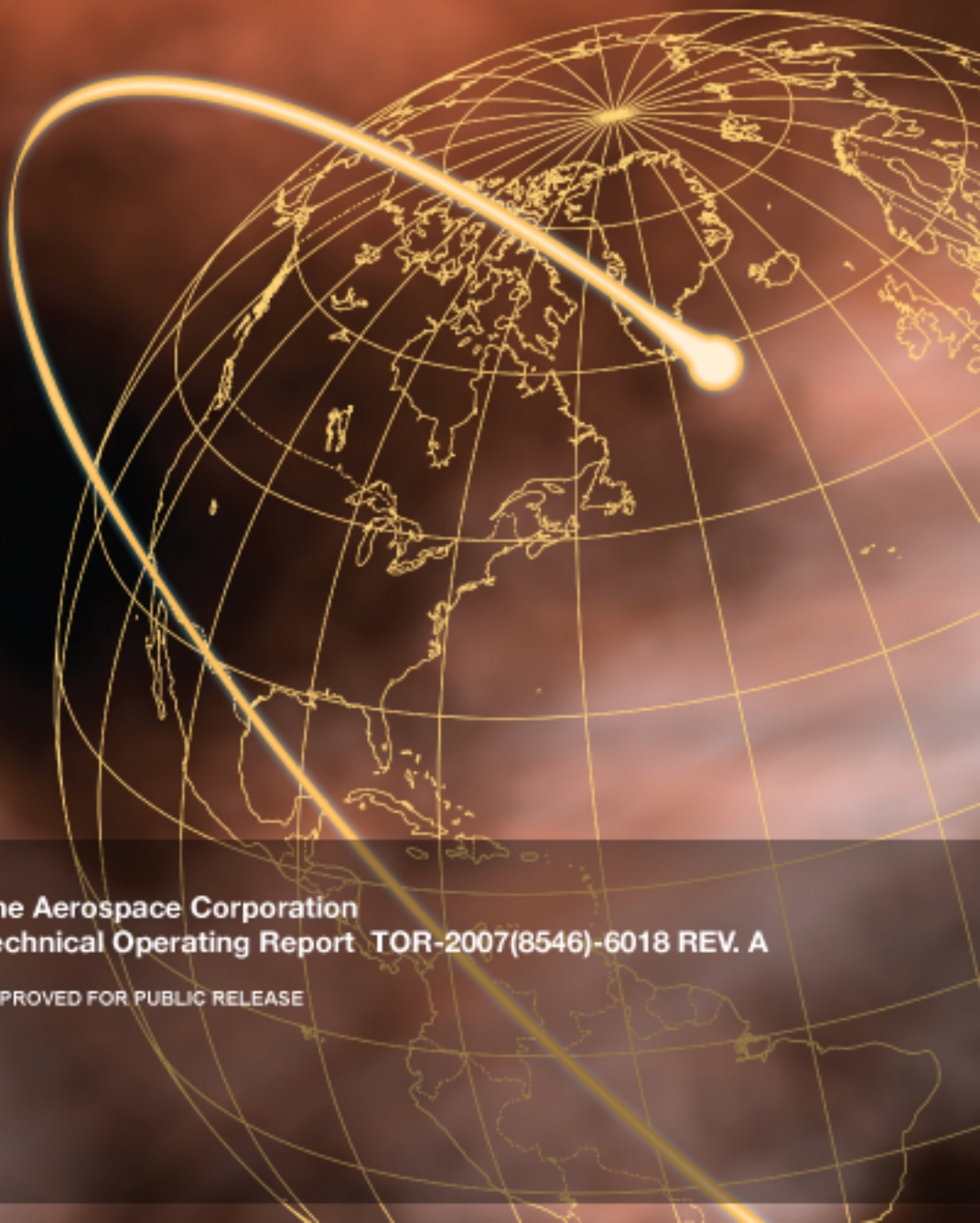
Mission Assurance Guide



The Aerospace Corporation
Technical Operating Report TOR-2007(8546)-6018 REV. A

APPROVED FOR PUBLIC RELEASE

AEROSPACE REPORT NO
TOR-2007(8546)-6018
Revision A

MISSION ASSURANCE GUIDE

Edited by

S. B. GUARRO and W. F. TOSNEY

1 July 2007

National Systems Group
THE AEROSPACE CORPORATION
El Segundo, CA 90245-4691

APPROVED FOR PUBLIC RELEASE

NOTE: contractually required signature pages and distribution lists for this document are on file in the Technical Publications Department, Corporate Communications Directorate, The Aerospace Corporation.

Acknowledgments

The *Mission Assurance Guide* was created by many authors throughout The Aerospace Corporation. Sergio Guarro coordinated the development of the document and of the associated Mission Assurance task database, also referred to as the Mission Assurance Verification Matrix (MAVM) task database, and wrote several sections. Senior advisors and contributing editors included William Tosney, Roland Duphily, Howard Wishner, and Dan Hanifen, all of whom provided invaluable direction, advice, review, and feedback. Rhoda Novak also provided invaluable help and editorial expertise in the organization and assemblage of the contributed materials into the final structure of the guide. The contributing authors are acknowledged in Table I and at the beginning of their chapters.

Table I. Contributing Authors

Paul G. Cheng	Mission Assurance Subdivision
George G. Cuevas	Parts, Materials and Processes Department
Roland J. Duphily	Acquisition and Risk Management Office
Colleen M. Ellis	Computer Applications and Assurance Subdivision
Suellen Eslinger	Software Engineering Subdivision
John G. Gebhard, III	Retired
James B. Gin	AWTR Systems Engineering
Sergio B. Guarro	Systems Engineering Division
Dan W. Hanifen	Baseline Systems/Payload
Paul H. Hesse	Navigation Division
Leslie J. Holloway	Software Engineering Subdivision
Andrew Y. Hsu	Acquisition and Risk Management Office
Gail A. Johnson-Roth	Acquisition and Risk Management Office
L. David Lutton	Computers and Software Division
Richard C. Maynard	CCAE Mission Assurance
Arthur L. McClellan	Parts, Materials and Processes Department
Steven R. Robertson	Parts, Materials and Processes Department
Gary D. Shultz	Product and Process Assurance Department
Mark M. Simpson	Electronics and Power Systems Department
Dana J. Speece	Product and Process Assurance Department
Joseph Statsinger	Retired
Lucio U. Tolentino	System Delivery and Operations Department
William F. Tosney	Cross Programs Systems Engineering Office
Linda J. Vandergriff	Sensor Engr. and Exploitation Department
Julia D. White	Cross Programs Systems Engineering Office
Howard D. Wishner	Navigation Division

Foreword

During the past several years, National Security Space (NSS) assets have been subject to an unacceptable increase in the number of preventable on-orbit anomalies. The reversal of this trend and the reestablishment of acceptably high levels of mission success have been identified as the highest priority for the NSS acquisition community. Detailed analyses and investigations of these anomalies have led to the conclusion that there is no single technical or phenomenological cause that predominate; instead, these anomalies seem to be imputable to a combined weakening of systems engineering and mission assurance (MA) practices, with roots in attempts (beginning in the 1990s) to reduce NSS acquisition costs. Recent authoritative studies such as the *Tom Young Report* have stated unequivocally that in order to achieve mission success it is necessary to re-invigorate and apply with renewed rigor, i.e., in a formal and disciplined manner, the principles and practices of MA in all phases of NSS space programs. MA has thus been recognized as the key to overcoming the "faster, better, cheaper" approach and the resulting increase in on-orbit mission performance problems.

It is in the context of the concerted efforts by the NSS community to revitalize disciplined systems engineering and MA programmatic activities that the development of this *Mission Assurance Guide (MAG)* has been initiated and executed, with the encouragement of Dr. Ballhaus, President of The Aerospace Corporation (Aerospace), and the support of the NSS community government sponsors.

This *MAG* is applicable to all NSS government program office activities and, specifically, to Aerospace activities related to space and launch vehicles and ground systems procured by NSS customers. The *MAG* can be also readily tailored and applied to NASA, NOAA, and other civil and commercial (C&C) programs supported by Aerospace, as advisable and agreed upon by the sponsoring customers.

Introduction

Sergio B. Guarro
Systems Engineering Division
Dan W. Hanifen
Baseline Systems/Payload
Howard D. Wishner
Navigation Division

The primary purpose of the *Mission Assurance Guide (MAG*) is to provide practical guidance to personnel of The Aerospace Corporation[1] (Aerospace) and, in general, National Security Space (NSS) program office personnel, who are responsible for executing mission assurance (MA) functions that are key to achieving program and mission success.

The Aerospace program office, engineering and laboratory personnel routinely carry out MA functions within the scope of the General Systems Engineering and Integration (GSE&I) role that Aerospace fulfills in support and on behalf of its customers. Although the initial motivation for the guide was to directly address such Aerospace MA functions, its content has been produced and assembled with the intent that it be generally suitable for use by personnel belonging to any organization that has GSE&I and MA responsibilities. The main limitation of scope of the guide is determined by the underlying assumption of separation between acquisition authority functions, i.e., "government-side" acquisition management functions, and prime contractor system design and production functions, as normally defined in standard NSS space program contractual stipulations. Thus, the guide addresses MA functions and tasks that are to be carried out by an NSS acquisition-authority government organization, or by a GSE&I-support entity that carries out these functions and tasks on behalf of the acquisition entity. It does not concern itself with MA functions that are typically carried out by the production entity, i.e. the prime contractor that is responsible for developing and executing the NSS system design and production activities. Certain prime contractor tasks and products, however, are addressed and identified as "enabling tasks and products" in those frequent cases in which their execution and completion constitutes a necessary prerequisite and point of departure for the execution of acquisition-entity MA tasks.

The above distinction is key to understanding the assumptions underlying the *MAG* concept and content. The first assumption is that all NSS system

[1] The Aerospace Corporation may also be called Aerospace in this guide.

acquisitions are based on the same basic duality between a government acquisition entity with its supporting organizations, and a prime contractor entity with its subcontractor and supplier organizations. A parallel and related assumption is that the acquisition authority is usually responsible for defining system concept and user requirements, whereas the prime contractor is responsible for interpreting and decomposing requirements into system design specifications, and for executing the design onto the production of a functioning system that is delivered to the acquisition entity and one or more end-users. The final basic assumption follows from recognition of the above principle of contractually stipulated acquisition duality and is the most directly relevant to understanding the way the guide is conceived and organized: in the realm of acquisition entity responsibility, it holds that it is always possible to identify and define sets of tasks that have the primary purpose of validating and verifying program and system development activities carried out by the prime contractor entity. In essential simplified terms, the guide assumes that the prime contractor's fundamental responsibility is to design and produce a system that performs functions defined according to user needs and acquisition entity requirements. In addition, it assumes that, besides tending to other basic management acquisition responsibilities, the acquisition entity MA responsibilities must also focus on validating its own system requirements, on making sure that the prime contractor applies bona fide processes and practices in developing the system, and, ultimately, on verifying that the system can perform at the level specified by the validated requirements.

In accordance with the assumptions and concepts introduced above, this guide describes principles and practices used by informed and authorized MA participants in the acquisition process. As previously mentioned, this may include Aerospace and its government customers, as well as GSE&I contractors and support organizations that have properly executed and implemented the appropriate and necessary non-disclosure agreements with Aerospace and any other affected parties. Regardless of the specific case of application, the main objective of the guide remains that of providing practical guidance for executing tasks that are directly pertinent to the NSS independent technical assessment (ITA) function, such as those performed by Aerospace in its Federally Funded Research and Development Center (FFRDC) charter. Aerospace supports NSS MA with overall systems engineering assistance as well as detailed technical engineering and laboratory expertise. Aerospace corporate expertise spans all of the disciplines involved in space system acquisition and MA support functions. When applied to MA functions executed by other organizations, the guide may be tailored, in scope and/or depth of application, as deemed appropriate by the acquisition organization designated by the NSS acquisition authority as the organization primarily responsible for MA execution.

The *MAG* defines an overarching MA framework that describes processes, disciplines, and associated executable tasks which are recommended for and

applicable to all NSS programs supported by Aerospace. This MA framework includes "best practices" guidance that Aerospace program office, engineering, and laboratory personnel can apply, in the context of the real-life constraints associated with a specific program. Where necessary, the guide refers to and complements other reference instruments and documents that provide guidance for the definition, tailoring, execution, and assessment of MA functions and tasks performed according to Aerospace-recommended practices. Figure I-1 provides a conceptual framework of the role of the guide—represented by blocks shaded in red—in relation to these other instruments, such as The Aerospace Corporation's *Systems Engineering Handbook* and *Test and Evaluation Handbook*. Tailoring guidance (identified in the figure by the block shaded in striped pattern) may be available at the individual program level, but is currently not explicitly organized in generally applicable practices that can be effectively documented in the guide. When seeking more detailed guidance and insight for the execution of specific technical tasks, please consult the references provided as the elements that directly support and complement the purpose and contents of the guide.

In structural terms, the *MAG* is organized around the definition and discussion of core MA processes (CMPs) and supporting MA disciplines (SMDs), which are assigned to specific program contractual acquisition phases and may also be associated with specific system segments, elements and components that are defined in the system work breakdown structure (WBS). Chapter 1 introduces the core MA principles, processes, and disciplines. Chapter 2 is a MA verification roadmap that provides the structured hierarchy and organization of tasks, which relates them to the appropriate CMPs, SMDs, program phase, and WBS. Chapter 3 discusses MA metrics and methods for assessment and standardized evaluation of MA task plans and executions, which can be carried out utilizing the assessment tools provided with the prototype Mission Assurance Verification Matrix (MAVM) task database software that is referenced in the guide. Chapters 4 through 16 individually cover each of the six CMPs and seven SMDs. The guide also includes separate appendices for definitions, acronyms, and a sample of one of the MAVM task database outputs.

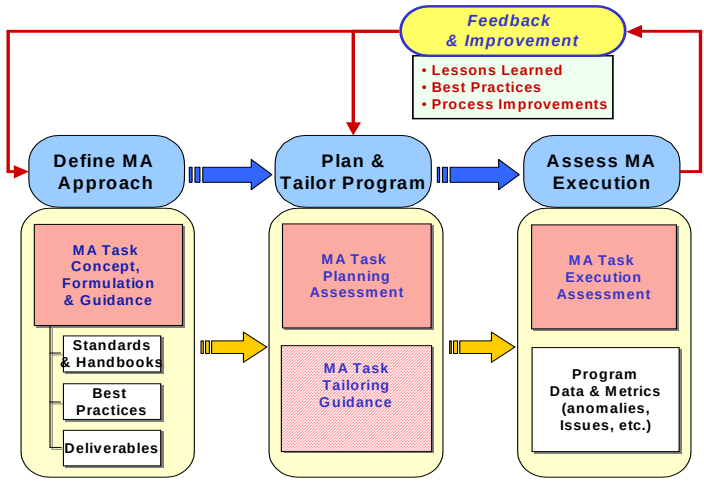


Figure I-1, MA Guide within Broader Mission Assurance Execution Context

At the task documentation level the guide is complemented by the associated MA task database, also referred to as the Mission Assurance Verification Matrix (MAVM). The guide database complement includes a detailed definition of MA tasks, and a number of specific task attributes, such as the identification of the benefits of performing such tasks along with the risks associated with not performing them, the level of resources allocated for task execution, and specific task closure and success criteria. The guide task execution guidance, together with the task tracking information, assessment metrics, and software implementation available within the MAVM database, provide an environment that permits the achievement of a high degree of consistency and accountability in MA implementation across all NSS programs.

It is worthwhile noting again that, since the prime contractors and their subcontractors are the providers of hardware and software, effective execution of MA oversight functions by the government customer/FFRDC/GSE&I teams depends not only on diligent implementation by the former of their own internal MA practices, but also on their execution of tasks that generate design documentation and product to be validated and verified by the latter via the execution of *MAG* tasks. Accordingly, contractual provisions must be in place to require that contractors, subcontractors, and suppliers operate in accordance with all applicable government MA requirements/actions. In addition, contractual provisions must also require that the customer/FFRDC team have full access to all relevant contractor and subcontractor data and activities. The verification that such provisions exist is identified by the *MAG* as a coordinated

set of MA tasks to be executed early on in any program acquisition lifecycle and at the start of every new acquisition phase within the life cycle.

Although in terms of system WBS, the primary focus of this guide is the space vehicle (comprised of the satellite bus and payload(s)), both ground systems and flight software are specifically addressed in the software assurance section. In addition, ground system and launch vehicle software and hardware elements are addressed in several other sections. On the other hand, certain aspects of MA related to the performance or replenishment of entire space vehicle constellations or system of systems (SoS)—e.g., those specific technical aspects of MA that address issues of availability and maintainability of such systems—are not directly and explicitly addressed in this guide.

The guide provides generally applicable guidelines, but is not intended to address all unique requirements. Its emphasis is to present how MA should be properly performed, and not necessarily how it is presently performed. MA tasks and supporting discipline tasks are defined and explained with the intent of ensuring the execution of repeatable processes that, by providing the greatest probability of mission success, will constitute truly effective MA. If all the procedures in this handbook are properly pursued, the MA function for the system will be accomplished. For the pursuit of this objective, the guide and the MAVM also identify, as appropriate, MA resources available to The Aerospace Corporation MA specialist, such as the cognizant Aerospace organizations, available tools, practices, and references.

To be of the greatest utility, the guide presents a consensus opinion or majority viewpoint and will be maintained as a living document by responsible communities of practice. Since MA is a living discipline, both the MAVM database (also more generically referred to within the guide as the “MA task database”) and any specific guide sections will be updated as appropriate.

Finally, the guide may have other uses besides that of implementation reference, such as documentation for training or refresher purposes or as a mentoring tool at introductory through intermediate levels of MA instruction.

Contents

Figures

Tables

Core Mission Assurance Policies, Directives, Specifications, and Standards

Sergio B. Guarro
Systems Engineering Division
Gail A. Johnson-Roth
Acquisition and Risk Management Office
Dan W. Hanifen
Baseline Systems/Payload

This section contains a compendium of core policies, directives, specifications and standards that provide the basis for a disciplined mission assurance (MA) program applicable to national security space (NSS) programs. The recommend set of specifications and standards is deemed necessary to adequately support and guide the successful implementation of proven engineering and program managements practices in U.S. space programs, in order to achieve mission success while at the same time minimize any unwarranted and costly impacts to system performance and program schedule. The specification and standard documents listed below should be evaluated for program applicability, tailored as necessary, and implemented as contract compliant requirements.

MA Policies and Directives

NSS-03-01	National Security Space Acquisition Policy, Guidance for DOD Space System Acquisition Process, Number 03-01, 27 December 2004
SMCI 63-1201	Assurance of Operational Safety, Suitability, & Effectiveness for Space & Missile Systems, 16 January 2004
SMCI 63-1202	Space Flight Worthiness, 01 October 2002
SMCI 63-1203	Space and Missile Systems Center, Air Force Space Command, United States Air Force, Independent Readiness Review Teams SMCI 63-1203, 16 January 2004
SMCI 63-1204	Space and Missile Systems Center, Air Force Space Command, United States Air Force, SMCI Readiness Review Process SMCI 63-1204, 01 August 2002

Core Specifications and Standards

The NSS community has recently defined and initiated the implementation of processes aimed at defining and adopting a core set of essential specification and standards that may be used across the spectrum of NSS acquisitions, regardless of the specific government agency executing a particular acquisition. To support this initiative, The Aerospace Corporation has instituted a Specifications and Standards Community of Practice (S&S CoP) and an Aerospace Standards Advisory Panel (ASAP). These entities represent, respectively, the company-wide technical forum and the institutional mechanism through which Aerospace recommendations and positions concerning specifications and standards are elaborated on and presented to government customer organizations. The list of core specifications and standards provided below represents the first consensus list produced via these institutions and associated processes.

ANSI/EIA 649	National Consensus Standard for Configuration Management, 04 October 2004
ASTM E 1548	Standard Practice for Preparation of Aerospace Contamination Control Plans, 05 June 2003
MIL-STD-1521B	Technical Reviews and Audits for Systems, Equipments, and Computer Software, 04 June 1985
MIL-STD-1542B	Electromagnetic Compatibility and Grounding Requirements for Space System Facilities, 15 November 1991
MIL-STD-461E	Requirements for the Control of Electromagnetic Interface Characteristics of Subsystems and Equipment, 20 August 1999
DOD-W-83575A	Military Specification Wiring Harness, Space Vehicle, Design and Testing, General Specification for, 22 December 1977

AIAA S-112-2005	Qualification and Quality Requirements for Space Solar Panels, 26 September 2005
TOR-2005(8583)-2	Electrical Power Systems, Direct Current, Space Vehicle Design Requirements, 11 May 2005
AIAA S-111-2005	Qualification and Quality Requirements for Space Solar Cells, 26 September 2005
TOR-2004(8583)-5 Rev. 1	Space Battery Standard, 01 April 2005
EIA HEB-1	Human Engineering—Principles and Practices, 02 June 2002
ISO 9241-1	Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs), 01 June 1997
COE UIS 4.3	Common Operating Environment (COE) User Interface Specifications (UIS) Version 4.3, 31 December 2003
MIL-STD-1472F	DOD Design Criteria Standard—Human Engineering, 23 August 1999
MIL-STD-1833	Test Requirements for Ground Equipment And Associated Computer Software Supporting Space Vehicles, 13 November 1989
SMC-TR-06-11 TR-2004(8583) -1 Rev. A	Test Requirements for Launch, Upper-Stage, and Space Vehicles, 06 September 2006
MIL-STD-810F	Test Method Standard for Environmental Engineering Considerations and Laboratory Tests, 01 January 2000
MIL-STD-1367A	Packaging, Handling, Storage, and Transportability Program Requirements for Systems and Equipments, 02 October 1989
MIL-PRF-29612B	Performance Specification for Training Data Products, 21 August 2001
MIL-PRF-49506	Performance Specification Logistics Management Information, 11 November 1996
MIL-STD-470B	Maintainability Program for Systems and Equipment, 30 May 1989
TOR-2005(8583)-3970	Mass Properties Control Standards for Space Vehicles, 20 July 2005

MIL-STD-1528A	Military Standard Manufacturing Management Program, 01 September 1986
DISR 06-3.0 Standards	DISR 06-3.0 Standards, 2006
DISR 06-3.0 Promulgation Memo	DISR 06-3.0 Promulgation Memo, 25 October 2006
AIAA S-113-2005	Criteria for Explosive Systems and Devices Used on Space and Launch Vehicles, 30 June 2005
TOR-2006(8583)-5235	Parts, Materials, and Processes Control Program for Space and Launch Vehicles, 08 November 2006
TOR-98(1412)-1	Parts, Materials, and Processes Control Program for Expendable Launch Vehicles, April 1998
TOR-2006(8583)-5236	Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles, 13 November 2006
ISO 9000	ISO 9000: An Aerospace Engineer's Handbook for Implementing the International Standards for a Quality System, 2001
ISO 9001	Quality Management Systems—Requirements, 15 December 2000
AS 9100B	Quality Management Systems—Aerospace—Requirements, January 2004
ANSI/EIA 748	Earned Value Management Systems, 28 August 2002
ISO 14300-2	Space Systems Programme Management—Part 2: Product Assurance—Policy and Principles, July 2002
ISO 14300-1	Space Systems Programme Management—Part 1: Structuring of a Programme, December 2002
TOR-2003(8583)-2895 Rev. 1	Solid Rocket Motor Case Design and Test Requirements, 22 December 2004
MIL-STD-785B	Reliability Program for Systems and Equipment Development and Production, 15 September 1980
MIL-STD-1543B	Reliability Program Requirements for Space and Launch Vehicles, 25 October 1988
ISO 17666	Space Systems—Risk Management, March 2003

NAS 411	Hazardous Materials Management Program, 19 January 1995
MIL-STD-882C	System Safety Program Requirements, 19 January 1993
AFSPCMAN 91-710 Vol 1	Range Safety User Requirements Manual Vol. 1—Air Force Space Command Range Safety Policies and Procedures, 01 July 2004
AFSPCMAN 91-710 Vol 3	Range Safety User Requirements Manual Vol. 3—Launch Vehicles, Payloads, and Ground Support Systems Requirements, 01 July 2004
AFSPCMAN 91-710 Vol 7	Range Safety User Requirements Manual Vol. 7—Glossary of References, Abbreviations and Acronyms, and Terms, 01 July 2004
AFSPCMAN 91-710 Vol 6	Range Safety User Requirements Manual Vol. 6—Ground and Launch Personnel, Equipment, Systems, and Material Operations Safety Requirements, 01 July 2004
AFSPCMAN 91-710 Vol 2	Range Safety User Requirements Manual Vol. 2—Flight Safety Requirements, 01 July 2004
MIL-HDBK-1785	System Security Engineering Program Management Requirements, 01 August 1995
AFSPCMAN 91-710 Vol 5	Range Safety User Requirements Manual Vol. 5—Facilities and Structures, 01 July 2004
TOR-2004(3909)-3537 Rev. B	Software Development Standard for Space Systems, 11 March 2005
ISO/IEC STD 15939	Software Engineering—Software Measurement Process, 11 July 2002
IEEE STD 1471-2000	IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, 21 September 2000
AIAA S-080-1998	Space Systems—Metallic Pressure Vessels, Pressurized Structures, and Pressure Components, 01 September 1988
AIAA S-081-2000	Space Systems—Composite Overwrapped Pressure Vessels (COPVs) (Current) 2000-01-01, 19 December 2000
AIAA S-114-2005	Moving Mechanical Assemblies for Space and Launch Vehicles, 30 June 2005
TOR-2003(8583)-2894	Space Systems—Structures Design and Test Requirements, 02 August 2004

TOR-2003(8583)-2896	Space Systems—Flight Pressurized Systems, 31 August 2003
AIAA S-110 2005	Space Systems—Structures, Structural Components, and Structural Assemblies, 12 July 2005
TOR-2003(8583)-2886	Independent Structural Loads Analyses of Integrated Spacecraft/Launch Vehicle Systems, 22 August 2003
ANSI/EIA 632	Processes for Engineering a System, 07 January 1999
TOR-2006(8506)-4732	Space System Verification Program and Management Process, 30 June 2006
TOR-2005(8583)-3, Rev. A	Systems Engineering Requirements and Products, 29 September 2005

Chapter 1
Core Mission Assurance Principles, Processes, and Disciplines

Sergio B. Guarro
Systems Engineering Division
Dan W. Hanifen
Baseline Systems/Payload
William F. Tosney
Cross Programs Systems Engineering Office
Howard D. Wishner
Navigation Division

1.1 Introduction

This chapter introduces (at a conceptual level) the core processes, disciplines, and tasks needed to validate and verify contractor concept development, design, manufacturing, integration, test, deployment, and operational processes and results, to maximize mission success.

1.1.1 Definitions

Mission success (MS^2) is defined as the achievement by an acquired system (or system of systems) to singularly or in combination meet not only specified performance requirements but also the expectations of the users and operators in terms of safety, operability, suitability and supportability. Mission success is typically evaluated after operational turnover and according to program specific timelines and criteria, such as key performance parameters (KPPs). Mission success assessments include operational assessments and user community feedback.

Mission assurance (MA) is defined as the disciplined application of general systems engineering, quality, and management principles towards the goal of achieving mission success, and, toward this goal, provides confidence in its achievement. MA focuses on the detailed engineering of the acquired system and, toward this objective, uses independent technical assessments as a cornerstone throughout the entire concept and requirements definition, design, development, production, test, deployment, and operations phases.

[2] In contrast, acquisition success can be defined in terms of performance, cost, and schedule.

Independent technical assessment (ITA) is defined as a formal or informal process, or combination of processes, formulated and executed using program, engineering, and laboratory resources to proactively evaluate system performance and independently validate contractor processes, techniques, and results using methods different from, and complementary to, those employed by the contractors. In some cases, ITA can be conducted by separate contractors. More commonly, ITA is performed in the context of the government program office-FFRDC-system engineering and technical assistance (SETA) team,[3] where The Aerospace Corporation performs that FFRDC role for national security space (NSS) systems.

1.2 NSS MA Principles

1.2.1 Independent Assessment

NSS MA requires detailed technical insight into each program by an independent organization with an independent reporting chain to measure the effectiveness and outcome of core requirement analysis, design, production, development, test, deployment, and operations processes and tasks. In this context, "independent" means executed independently of the normal activities performed by the prime contractor and sub-tier contractors/suppliers. In other cases, "independent" may mean that a separate technical team is established to conduct a technical or readiness review or audit to certify launch or mission readiness. In yet other cases, the independent nature of MA is manifest within the government program office team, where MA resources are routinely applied most effectively at the working level in a proactive, interactive, and continuous manner to focus on early discovery and correction of problems throughout the entire system life cycle. The independence of the MA function is deliberately set, not to create antagonistic roles, but to guarantee a high level of responsibility and objectivity while facilitating the free flow of mission-critical information.

1.2.2 Rigorous Process

NSS MA is driven by the unique nature of the associated NSS space systems. These systems are typically produced in small quantities, may go through final assembly at the operational site, have relatively low performance margins (e.g. weight, power, etc.), are exposed to extreme

[3] Hereafter in this guide known as the "government program office team."

environments, are not serviceable in operation, are not reusable (except for ground systems and flight software), and must satisfy unique requirements for nearly every mission. These characteristics require a rigorous MA process to maximize confidence in mission success. Although a number of validation and verification activities are part of a normal system design, production, and operations process, MA activities are characterized by an independent, formalized execution. That is, they are carried out by personnel and organizations that have a defined responsibility to execute and uphold the MA function to a pre-established level of implementation and quality. Furthermore, years of system engineering experience and practice show that the primary focus of mission and systems design activities is the achievement of acceptable cost, schedule, and technical performance, whereas MA places additional effort and attention on the further objective of assuring desired performance and user satisfaction over time with high levels of confidence and reliability.

1.2.3 Integrated Application

Different hardware and software elements of complex systems are usually developed by various provider organizations and then integrated by yet another separate organization before final delivery to the customer or user. As such, a uniform set of MA processes, disciplines, and tasks needs to be applied at all levels of integration to acquire the needed confidence in the end product. MA can be viewed as the overarching process that groups, integrates, and focuses the engineering disciplines and support processes toward providing and guaranteeing reliable, long-term performance that satisfies customer needs.

1.3 Necessary Conditions

In order for MA to be effectively applied, certain conditions must be true about the nature of the programs to which MA is applied.

1.3.1 Management and Technical Expertise

To successfully execute MA, NSS programs must have a sufficient workforce of properly trained, certified, and motivated technical and management personnel to:

- Proficiently analyze and translate the user's mission needs into requirements, standards, and design documentation, and to

further verify that the end items are produced and tested according to those same requirements, standards, and documentation using appropriate processes and practices.

- Proficiently execute or technically assess detailed engineering, production, integration and test, launch site, and operations processes to reduce risk and ensure product integrity. This applies to all levels of the entire contractor team, including the subcontractor and supplier levels.
- Ensure that the engineering and management products are consistent and technically sound, that MA tasks are specified in contractual documents and completed satisfactorily, that testing addresses MA, and that the resulting system will meet user needs as defined in the contractual documents.
- Proficiently examine and understand the program's programmatic and technical baseline, maintain configuration control, interpret published MA guidance and standards, and tailor MA processes, practices, tasks, and standards to maximize mission success benefits within the constraints of the program.

1.3.2 Appropriate Contractual Support for MA

The availability of contractor data and key personnel is critical to performing MA. Staff availability depends on the contractual provisions governing the contractors' activities, procedures, and reporting systems. These provisions are generally covered in statements of work (SOWs), applicable compliance documents, schedules, and specifications, as well as technical data requirements embodied in contract data requirement lists (CDRLs), data item description documents (DIDs), and similar items. These provisions must provide for adequate contractor implementation and information transmittal. If they do not, the government program office must identify and implement appropriate contractual changes.

1.3.3 MA Reporting Channels

Government program office and contractor program managers must create and maintain a management and communication environment that encourages the correct balance between the open communication necessary for effective system development and operations, and the ability to directly present issues and recommendations to key government and Aerospace decision makers if mission success is judged to be in jeopardy. Management and technical personnel at all

levels must be able to quickly and objectively communicate on serious issues affecting mission success in a streamlined fashion without fear of reprisal. Contractual mechanisms must be in place to enable effective communication processes and MA reporting needs.

1.4 MA Objectives by Life Cycle Phase

MA objectives complement key acquisition tasks by focusing on development processes and outputs to deliver a product (or system) ready for use in developmental testing or operational use. Figure 1.4-1 below summarizes the major acquisition phases (as defined in the DOD and acquisition policy documents), the key development activities by phase in a typical system's life cycle, and the correlations to companion MA life cycle phases. Note that while acquisition and MA life cycle phases share common terms, specific tasks that occur for MA are unique to furthering mission success. Specific MA objectives and tasks are summarized by MA life cycle phase following Figure 1.4-1.

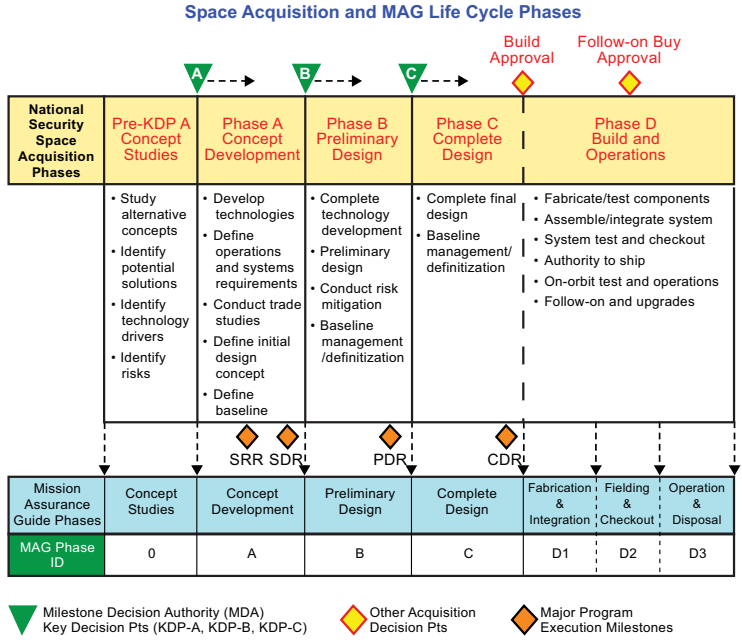


Figure 1.4-1, MA vs. Space Acquisition Life Cycle Phases[4]

[4] Based on NSS 03-01 Acquisition Life Cycles.

- **Pre-KDP A Concept Studies and Early Concept Development (MAG Phases 0 and A)**

  In MAG Phases 0 and A (concept studies and early concept development), the primary MA objective is to assure architecture and system requirements meet user, operator and other stakeholders' needs and expectations. A parallel and equally important objective is to provide the contractual groundwork for staffing, generation of design-relevant data, access, and open communications necessary for successful MA program execution.

  Phase 0 and early Phase A MA tasks assure that mission and system performance objectives, requirements, and specifications are set realistically and can be reasonably executed and verified given appropriate technology, cost, and schedule constraints. This effort includes validation and verification of the processes applied to flow-down requirements and specifications, with particular attention to mission analysis, architecture views, requirements, specifications, and interfaces that are established for execution with or by an entity other than the system prime contractor (e.g., external organizations and lower-level contractors). MA tasks also seek to ensure that the government program office establishes the policies, procedures, and contractual language within the SOW or objectives, CDRLs, and DIDs, so that the contractors provide the data for MA evaluations.

- **Concept Development, Preliminary Design, and Complete Design (MAG Phases A, B, and C)**

  In later concept development, preliminary design and complete design (MAG Phases A, B, and C), the primary MA objective is to assure system design and engineering integrity.

  MA tasks seek to verify and validate that the developed design solutions meet the requirements and specifications. This effort includes not only the verification of design from the point of view of meeting functional, interface, and performance requirements, but also requirements and specifications for reliability, availability, maintainability, safety and security. It also includes considerations of design and construction, parts, materials and manufacturing processes, quality, configuration management, producibility, testability, and any other aspects of the design that may affect the reliable execution of the program or system mission. Again, these validation and verification activities include the review of design

characteristics of elements provided by external organizations and lower level contractors.

- **Fabrication and Integration (MAG Phase D1)**

  In fabrication and integration (MAG Phase D1), the primary MA objective is to assure product and system integrity.

  MA seeks to verify that system components and elements are manufactured, programmed (software), assembled, integrated and tested in accordance with the qualified processes as well as verifying that the produced item demonstrates the required performance, reliability, operability and suitability. This effort includes the validation and verification of manufacturing processes, integration and test procedures, and test data provided by contractors, subcontractors and suppliers. It also includes the verification and certification of flight/mission readiness and the assessment of performance risk.

- **Fielding and Checkout and Operations and Disposal (MAG Phases D2 and D3)**

  In system and checkout and operations and disposal (MAG Phases D2 and D3), the primary MA objective is to assure that product integrity is maintained while demonstrating the required, specified performance at the system level.

  Prior to launch, MA tasks implement proven processes to collect development and test data to verify, review, and certify NSS systems as space flight worthy and the ground system operationally ready. Post deployment, MA tasks focus on the collection of system data to verify and validate that system functionality and performance satisfies both systems requirements and users' needs. In operations, MA task implementation continues to require collection of operational data to validate that the system requirements concerning performance, reliability, operability, and suitability are met under operational service conditions and to identify any corrective measures that may be necessary to assure that they are met in the future. For future missions and ongoing ground system operations, the collection of Lessons Learned data that may support future system design or potential operational changes is also a key objective of the operations and maintenance MAG phase. This feedback into the requirements and/or design processes essentially closes the loop,

enabling continuous system improvement. Aerospace's "Lessons Learned" database continues to capture key lessons that will enhance how future programs are acquired and managed.

The implementation of the MA objectives described above is executed and verified via core MA processes (CMPs), as illustrated in Figure 1.4-2. Within the CMPs, tailored sub-processes from a set of supporting MA disciplines (SMDs) are also folded, as shown in Figure 1.4-3. The nature and depth of CMPs are usually time and acquisition phase dependent. SMDs can theoretically be implemented as self-standing processes that cut across the full range of program phases, but more normally they feed into and support CMPs in tailored form and fashion. Also underlying the entire MA framework are all the other key traditional engineering disciplines (see section 1.6.2.3) applied during detailed technical design processes and analyses. A full discussion of the interrelation of MA processes and disciplines is provided in sections 1.6.2.2 and 1.6.2.3. For the practical implementation of MA, each program will have to conduct a deliberate and focused tailoring activity (as illustrated conceptually by Figure 1.4-3), in which specific blocks of SMD tasks shall be incorporated into appropriate CMP phases and task areas, and the CMPs themselves shall be shaped, via appropriate task selection and adaptation, into the form seen as best suited for execution within the practical constraints of time and resources available to that particular program.

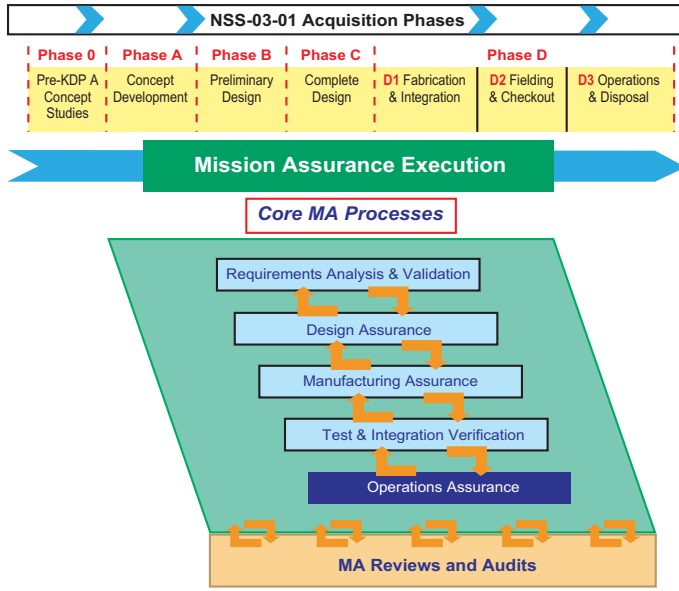


Figure 1.4-2, MA Execution via CMPs

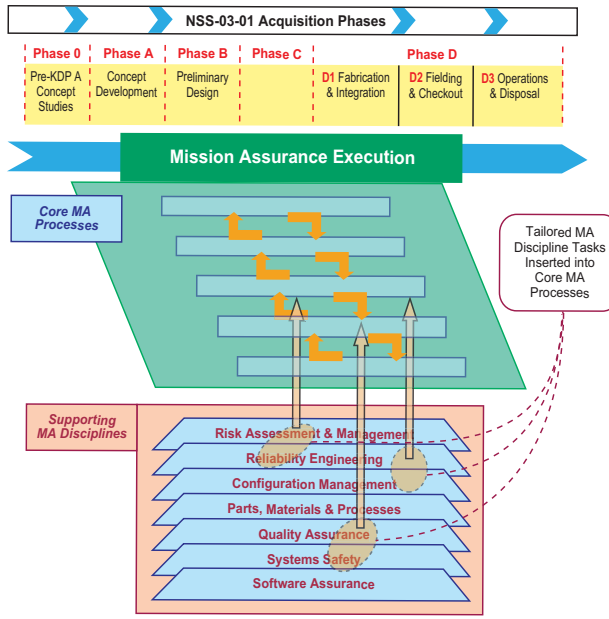


Figure 1.4-3, Relationships Between CMPs and SMDs

1.5 Current SMC MA Policy

The Space and Missile Systems Center (SMC)-sponsored MA policy is the "Assurance of Operational Safety, Suitability, and Effectiveness (OSS&E) for Space and Missile Systems."

1.5.1 SMC MA Policy

OSS&E assurance is implemented by SMC Instruction 63-1201, "Assurance of Operational Safety, Suitability, and Effectiveness for Space and Missile Systems." This SMC policy follows directly from Air Force (AF) Policy Directive 63-12, AF Instruction 63-1201, and AF Material Command Instruction 63-1201. The OSS&E process establishes and preserves baselines for operational safety, operational suitability, and operational effectiveness throughout the life of a system or end item (including operational and experimental systems). The OSS&E process includes the appropriate, program-specific government involvement in the full range of requirements, design, manufacture, test, operations, and readiness reviews accomplished by either contractors or the government.

Space flight worthiness is determined according to SMCI 63-1202 USAF (Space Flight Worthiness), which implements the requirements contained in AF Policy Directive 63-14, USAF Flight Worthiness. Space flight worthiness measures the degree to which a spacecraft, launch vehicle, or critical ground system as constituted has the capability to perform its mission throughout its life cycle along with associated risks. A space flight worthiness review process leads to a flight worthiness certification in support of the final launch campaign and flight readiness review.

1.6 MA Implementation Overview

1.6.1 Organizational Roles and Interactions

Figure 1.6-1 provides a top-level conceptual view of the complex interaction of the typical MA responsibilities associated with NSS programs, including: the development contractors' functional engineering, manufacturing, MA, CM, and QA functions; similar functions for subcontractors and suppliers; the government program office, with Aerospace as the program FFRDC support; and Defense Management Contract Agency (DCMA) as the delegated in-plant support. Primary Aerospace MA functions generally reside within the

government program office team, but involve all the participants to ensure mission success. When formed, an independent government MA technical review team also includes all the participants. **It is essential to understand that the FFRDC and government implementation of mission assurance cannot be successful without a solid foundation of MA activities assigned to and executed by the contractors and suppliers.** Although not shown, functional elements from the launch site participate in the development life cycle as part of the government program office team.

The DCMA team typically provides a program integrator (PI) as a focal point for the government program office at the contractor's facility, an administrative contracting office (ACO), and technical specialists in cost management, engineering, and quality. The DCMA is the DOD organization working directly with defense suppliers to help ensure that DOD, federal, and allied government supplies and services are delivered on time, at projected cost, and meet all performance requirements. Where appropriate, the PI delegates responsibility to other DCMA organizations at the contractors, subcontractors, and vendors.

Aerospace MA tasks, like all other GSE&I tasks executed by Aerospace, are assigned in accordance with the SMC FFRDC Users Guide[5] which not only identifies Aerospace's core functions and provides a process for tasking Aerospace, but clarifies procedures for interfacing with other contractors including SETA organizations. Typically, Aerospace, other FFRDCs and SETA organizations form a seamless government team in support of the system program office. However, Aerospace has a unique MA role providing independent and objective technical assessments reported through the Aerospace President to the SMC Commander.

[5] SMC FFRDC Users Guide, 20 January 2004.

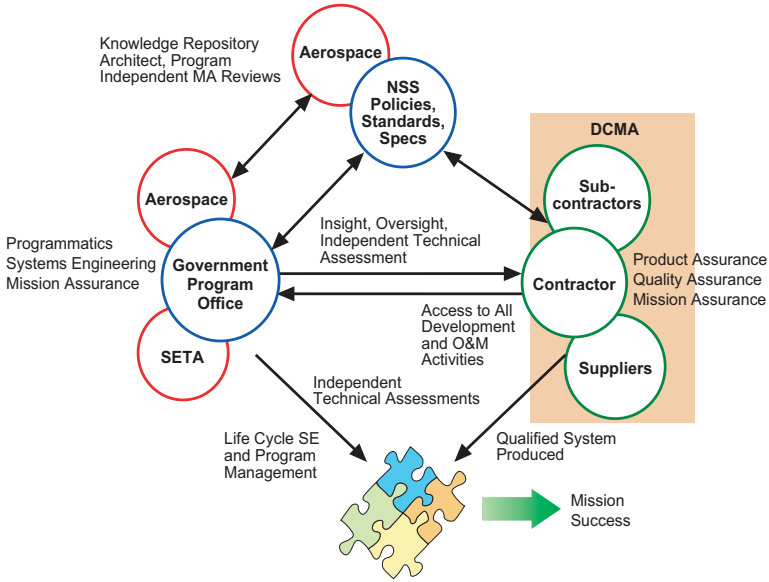


Figure 1.6-1, Distributed and Complementary MA Responsibilities[6]

1.6.2 Basic Structure and Organization of MA Activities

1.6.2.1 Definitions

A **process** is a series of tasks, involving the practical application of accepted principles, which are architected and organized in logical sequence to achieve a broad set of objectives. MA processes contribute to mission success in terms of directly attributable positive consequences.

A **core MA process (CMP)** is a systems engineering process that is defined and applied to support MA goals.

A **practice** is a limited set of interrelated tasks customarily accepted and routinely performed. MA practices are executed to achieve specific MA objectives that enhance mission success.

[6] SETA vs. FFRDC roles and SMC FFRDC Users Guide, 20 January 2004.

An **engineering discipline** is a well-established and documented technical body of knowledge governing the execution of a broad set of tasks to achieve a defined set of technical objectives.

A **supporting MA discipline (SMD)** is an engineering discipline that is specifically oriented and organized to support MA processes and the entire MA program. Because of practical constraints on resources available to a specific program, such support is often limited to a partial, rather than complete, application of the discipline within the MA program itself.

Lessons Learned capture the risks of flawed technical and management practices and processes, and the benefits of refinements to current practices and processes.

A **space vehicle** includes the bus and its payload(s).

The **ground system** includes all the assets, such as hardware, software, staff, and facilities, that form the ground component of the space system and are required to operate the space vehicle.

The **launch system** includes the launch vehicle and associated ground launch facilities.

1.6.2.2 MA Processes and Supporting Disciplines

MA can be viewed as a set of programmatic and engineering processes organized together toward the goal of mission success. When examined from an implementation point of view within the MA life cycle of a given NSS program, these processes belong to two basic, complementary classes, namely CMPs and SMDs.

CMPs treated in this guide are:

- Requirements Analysis and Validation
- Design Assurance
- Manufacturing Assurance
- Integration, Test and Evaluation
- Operations Readiness Assurance
- MA Reviews and Audits

CMPs tend to be associated with specific portions or phases of the system/program acquisition life cycle and can be executed with a combination of technical means that can vary in nature and depth. Conversely, the definition and tailoring of CMPs for specific program use involves the tailoring of tasks that may have been initially defined within the context of the various SMDs. Some CMPs cannot be defined in detail until the system design is reasonably mature. CMPs can be, and normally are, tailored (scoped) to fit within existing program resources and constraints. CMPs draw upon the SMDs as needed to construct an executable and effective MA program.

SMDs treated in this guide are:

- Risk Assessment and Management
- Reliability Engineering
- Configuration Management
- Parts, Materials and Processes Management
- Quality Assurance
- Systems Safety Assurance
- Software Assurance

SMDs tend to span across the entire program life cycle. Due to budgetary constraints and program-specific MA risks, only selected portions of their theoretical range of application tasks are usually executed by any single program. SMDs have execution instructions that are universally accepted in the broader technical community, including recommended and/or mandated tools, techniques, models, and technical standards. SMDs typically include tasks and practices that are used, in combination with tasks and practices from traditional engineering disciplines, to support the execution of certain portions of core MA processes. SMDs may be applied in each phase of the life cycle, as required by the CMPs they support.

As an example of the distinction between CMPs and SMDs, operational readiness assurance is a CMP, which is articulated for the majority of its composing tasks within MAG Phase D of the NSS acquisition cycle. Risk assessment and management, on the other hand, is a SMD, as it focuses on evaluating risks to mission success that may originate in any of the acquisition and operation activities. In fact, some form of risk assessment is used in MAG Phase A to support the MA operational readiness assurance planning process, and in another program phase to support a different MA process. Thus, this guide classifies risk assessment as a SMD, along with other technical

disciplines whose activities cut across life cycle phases and can be used to support core MA processes in various ways.

1.6.2.3 Development Engineering and Science Disciplines Used to Support MA

The ultimate foundation of mission success rests on all the individual areas of engineering expertise that are applied in the design, manufacturing, integration, and operation of a space system. This section provides a list, by no means exhaustive, of the engineering and science disciplines that provide the underlying expertise to successfully produce and operate space and launch vehicles. System engineering assists each discipline to decompose system requirements to identify driving requirements and performance allocations, and to verify that the end products satisfy those requirements. Each discipline maintains competency in the tools, techniques, processes, material, practices, technologies, and state of the art of their respective discipline in order to successfully translate allocated requirements/specification and performance into initial paper designs, performance predictions, breadboards, and/or prototypes and the final design. Again, the list of disciplines shown below is illustrative of the broad scope of expertise required, but is not exhaustive:

- Structures and Mechanisms
- Propulsion
- Dynamics and Controls
- Guidance, Navigation, and Control
- Flight Mechanics
- Thermal
- Fluid Mechanics/Aerodynamics
- Electrical Power and Distribution
- Ordnance
- Telemetry, Tracking and Commanding
- Flight Termination and Range Safety
- Data Management
- Ground Control System Software Development
- Communications and Data Handling
- Instruments and Payloads
- Instrumentation
- Flight and Special-purpose Ground Computers
- Flight and Mission Software Development
- Survivability

- Mission Planning
- Mission Management
- Mission Data Processing
- Human Factors Engineering
- Launch Support and Services
- Manufacturing Engineering
- Electromagnetic Compatibility Engineering
- System Architecting
- Space Science
- Test Engineering
- Systems Engineering
- Integrated Logistics Support
- Environmental Engineering
- Electrical Engineering
- Mechanical Engineering
- Physics
- Chemistry
- Tracking Systems Engineering
- Astronautical Engineering
- Optical Engineering
- Security Engineering
- Computer Science
- Software Engineering
- Miscellaneous

1.6.2.4 Tailoring the Programmatic Execution of MA

Key to the philosophy of this guide is the point that successful MA implementation requires a baseline set of criteria that can be applied to a specific program's needs with accompanying tailoring guidance. Figure 1.6-2 shows a process by which programs tailor their specific needs using prescribed criteria that will be described in a future revision of this guide. Resource and schedule constraints require that a specific program define an overall MA process that is tailored to program-specific needs and places emphasis on those aspects of MA that the program considers most important for its success. Thus, in each program, the targeted breadth and depth of applied MA processes will depend on several factors, including program budget, program schedule, state of maturity of the underlying technology, nature of the program (i.e., demonstration vs. operational) and, perhaps more importantly, the criticality of the mission.

Since CMPs and engineering disciplines listed can be expressed in terms of sets of executable tasks, a program-specific, tailored version of a full MA process can be envisioned as a composite process, which:

1. Identifies, within the above phase-dependent processes and specialty disciplines, the specific tasks that are believed to have greater MA value for the program; and
2. Threads these tasks together in an execution flow that, in depth and timing, is compatible with the program goals and resources.

In general, a tailored MA program will still contain the CMPs identified in this guide (see the preceding section). The SMD tasks included in these processes, however, would normally be a selected subset of those included in the disciplines themselves.

1.6.3 Program-integrated MA Execution

Figure 1.6-2 represents an overall MA implementation process fully integrated within a space program life cycle, and making explicit reference to the underlying structure of core processes and disciplines that were first introduced with Figures 1.4-2 and 1.4-3. Core processes, disciplines, specifications and standards, other CDRLs, and government program office and contractor MA programs are all tailored according to program criticality, priority, schedule and available resources. Specific test and evaluation or systems engineering tasks or discipline guidance is provided by companion handbooks to this guide. Final program execution of MA is documented and executed according to program-specific plans supporting MA.

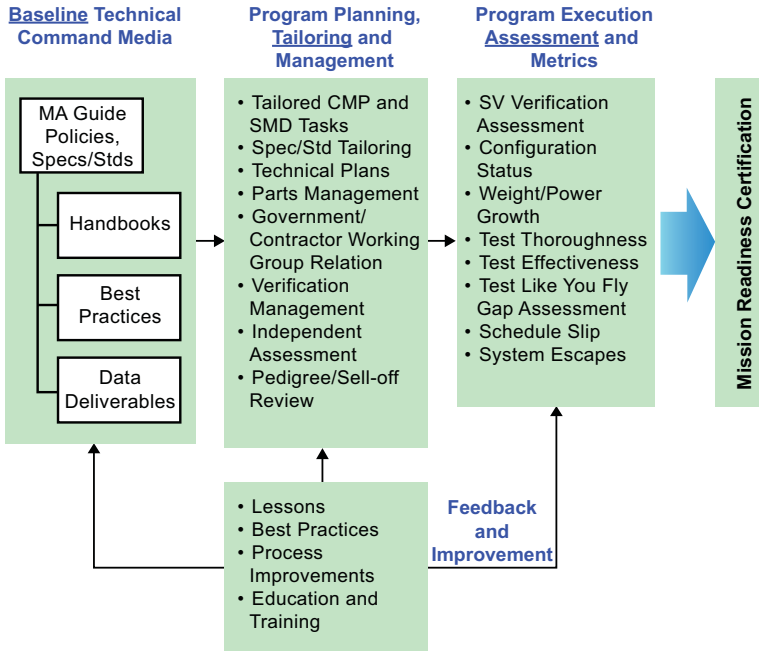


Figure 1.6-2, MA Implementation Process

1.7 References

NSS-03-01	National Security Space Acquisition Policy, Guidance for DOD Space System Acquisition Process, Number 03-01, 27 December 2004
SMCI 63-1201	Assurance of Operational Safety, Suitability, & Effectiveness for Space & Missile Systems, 16 January 2004
AFI 99-101	Developmental Test and Evaluation, 01 November 1996
AFI 99-102	Operational Test and Evaluation, 01 July 1998
Aerospace TOR-2004(1901)-3101	*Recommended Missile Defense Agency Mission Assurance Practices*, 17 October 2003.

Space System Risk Management: Launch Assurance," Whitehair, C. L. and Wolfe, M. G., 30 March 1995.

Welch, General L., Report of the Panel for Reducing Risk in Ballistic Missile Flight Test Programs, DOT&E-98-01, 99-01, 1998.

Young, T., Report of the Defense Sciences Board/Air Force Scientific Advisory Board on Acquisition of National Security Space Programs, Department of Defense, 2003.

Lyles, General L., Space Launch Vehicles Broad Area Review Final Report – Appendix A, *BAR-99-02*, 1999.

When Is a Satellite Mission Too Fast and Too Cheap?" Bearden, D., The Aerospace Corporation, 11 September 2001.

Acquisition of National Security Space Programs," DSB/AFSAB Task Force Report, November 2002.

Major Management Challenges and Program Risks: Department of Defense," GAO-03-98, January 2003.

Independent Assessment Team on Mission Success (Tom Young Report), 24 March 2000.

DOD-HDBK-343 (USAF), Design, Construction, and Testing Requirements for One-of-a-kind Space Equipment," 01 February 1986.

Chapter 2
Mission Assurance Verification Roadmap

Sergio B. Guarro
Systems Engineering Division

2.1 Introduction

Mission assurance (MA) verification as described in the *Mission Assurance Guide (MAG)* is focused primarily on the identification, tailoring, and assessment of sets of tasks related to core MA processes (CMPs) and supporting MA disciplines (SMDs). The identification and tailoring activities have the objective of selecting and refining, from a generic, comprehensive set of possible MA tasks, a tailored set that is believed to be practically executable within the scope and constraints of any single specific program.

For both reference and eventual execution purposes, both the comprehensive set of MA tasks and any derived program-specific sets need to be organized according to a taxonomy that reflects the hierarchical relation of tasks to CMPs or SMDs, as well as the appropriate acquisition phase. The *MAG* includes an appendix (Appendix 3) describing this hierarchical organization of tasks, which reflects the contents of a configuration-managed relational database produced by the MAG initiative for the purpose of facilitating (in practical terms) the entire MA verification process, referred to as the MA Verification Matrix (MAVM) task database.

To effectively structure the MAVM for implementation in a typical program or system program office (SPO) it was also necessary to align the tasks' structures documented therein with a common set of practical implementation targets that represent an organizational and system-oriented view generally accepted and used in national security space (NSS) SPOs. Thus, within each phase, tasks are also assigned, for execution tracking and assessment purposes, to distinct levels of application, vertically organized according to a standard work breakdown structure (WBS) hierarchy (reflecting the WBS definition guidance provided by MIL-STD-881B—see section 2.2.3.1), which is partially reported below:

- 1st Level: Program Planning, System Engineering, System
- 2nd Level under "System": Space Segment, Launch Segment, Ground Segment

- 3rd Level under "Space Segment": Space Vehicle
- 4th Level under "Space Vehicle": Bus, Payload
- 5th Level under either "Bus" or "Payload": Subsystems
- 6th Level under any of the "Subsystems": Units

The following discussion will describe how the architecture of the MAVM task database is constructed, what a typical data record consists of, and how each task or data record allows for a means to assess the task plan and execution quality via criticality, depth of effort, completeness, and quality ratings (see Chapter 3).

2.2. MA Execution in the NSS Acquisition Cycle

2.2.1 NSS Acquisition Cycle Phases

Section 1.4 provides an introduction of the NSS system and program acquisition phases that define the broad context within which the execution of MA is articulated.

The five basic sequential phases that cover the full acquisition cycle of an NSS system are formally defined in the directive NSS-03-01. These basic program acquisition phases are identified in Figure 1.4-1 and are listed below for ready reference:

1. Pre-KDP A Concept Studies – referred to as "MAG Phase 0" in this guide
2. Phase A Concept Development – referred to as "MAG Phase A" in this guide
3. Phase B Preliminary Design – referred to as "MAG Phase B" in this guide
4. Phase C Complete Design – referred to as "MAG Phase C" in this guide
5. Phase D Build and Operations – referred to as "MAG Phase D" in this guide

2.2.2 Program Office Technical and MAG Phases

NSS program office and contractor activities generally follow the acquisition phase organization discussed above. However, some programs also use a nomenclature of technical activity breakdown that does not completely coincide with the acquisition phase terminology presented in the preceding section. Since MA activities are practically associated with program technical execution activities, this parallel

terminology is also relatively common in MA practice and can be often encountered alongside the one based on the formal acquisition phase definitions discussed earlier.

To help clarify for the reader the alternative phase definition language that can be found in the MAG and acquisition arenas, the table below provides a mapping of traditional technical and MA execution phases into the acquisition phases referred to in NSS-03-01.

Table 2.2-1, Mapping of MA and Technical Program Phases to NSS Acquisition Phases

Program Technical Phase	Within-Phase Program Milestones	Concluding Program Milestones	MA Guide Phase	Acquisition Phase	Within-Phase Acquisition Milestones	Concluding Acquisition Milestones
Requirements and Concept Definition/ Acquisition Planning	N/A	N/A	Phase 0 Concept Studies	Pre-KDP-A Concept Studies	N/A	KDP-A
			Phase A Concept Development	Phase A Concept Development	N/A	N/A
System Definition	SRR	SDR	Phase A Concept Development	Phase A Concept Development	N/A	KDP-B
Design and Development	PDR	CDR	Phase B Preliminary Design	Phase B Preliminary Design	N/A	KDP-C
			Phase C Complete Design	Phase C Complete Design	N/A	Build Approval
Production, Integration and Test	N/A	N/A	Phase D1 Fabrication and Integration	Phase D Build and Operations	Follow-on Approval	N/A
Deployment, Test and Checkout	N/A	N/A	Phase D2 Fielding and Checkout	Phase D Build and Operations	N/A	N/A
Operations and Maintenance	N/A	N/A	Phase D3 Operations and Disposal	Phase D Build and Operations	N/A	N/A

The table includes an identification of the major acquisition and technical milestones that are included in, or conclude, each of the listed phases. It also identifies the shorthand phase labels that are used in the phase-grouping of MA tasks in the remainder of this guide and in the MAVM task database, which is documented in summarized form in Appendix A3.

2.2.3 Phase-dependent Organization of MA Tasks

The discussion in this section addresses the logic and execution-related organization of MA tasks, and its relation to the reference structure of CMPs and SMDs.

2.2.3.1 Organization of CMP Tasks

The CMPs include comprehensive sets of MA activities that a given program is expected to execute. The actual breadth and depth of each specific program activity execution is determined by program objectives and available resources. The basic CMP definitions are expanded in dedicated portions of the guide (Chapters 4 through 9), which are also complemented by the associated MAVM task database, with its full hierarchical framework of detailed task definitions. This framework is intended to be fully inclusive and comprehensive, and serve as a general reference—i.e., it provides an overarching definition that is not specifically addressed at an individual program. Thus, by design, it is also meant to undergo program-specific tailoring before actual task deployment and execution in any given program. The subject of MA process and task tailoring, according to criteria that address both program-specific criticality of MA activities and overall program resource constraints is further discussed in section 2.2.5, with more detailed and complete guidance planned to be made available in a future update of this guide or in a companion document. Appendix A3 documents the task headings and structural organization of the MAVM task database, and provides the baseline reference of task activities from which the program tailoring process is meant to proceed.

Sequential Flow of MA Processes and Tasks

The CMPs reflect the basic MA functions of validating and verifying the correctness of all the fundamental steps of space system definition, development, fabrication, fielding, and operation. Thus, the formulation and logic organization of these MA processes directly follows the intrinsic acquisition phase dependence and sequential order of execution of the generally recognized and executed space system conceptualization, design and build processes. For easy reference, the CMPs are again listed in the table below.

Table 2.2-2, Core MA Processes

Core MA Processes	Chapter	Appendix
Requirements Analysis and Validation	4	A3-1
Design Assurance	5	A3-2
Manufacturing Assurance	6	A3-3
Integration, Test and Evaluation	7	A3-4
Operations Readiness Assurance	8	A3-5
MA Reviews and Audits	9	A3-6

The program phase dependence of a MA task's execution is determined at a first level by its belonging to a specific CMP. Although each of the MA processes is usually designed to span more than one acquisition and program phase, and partially overlap in time with other MA processes, a definite phase-sequential order governs the intended execution of the set of CMPs, and the majority of the tasks under a specific process tend to be concentrated in a particular program phase. Thus, for example, most of the key tasks under the requirements analysis and validation process are to be executed in MAG Phase A (concept development) and Phase B (preliminary design), corresponding to, in the day-to-day terminology in use by some programs, the requirements and concept definition and system definition phases, and to the design and development phase. On the other hand, the majority of key tasks that belong to the design assurance process are, as one may expect, to be executed in MAG Phase B (preliminary design) and MAG Phase C (complete design), which together map into what programs often refer to as the design and development phase. Similarly, most of the activities pertaining to the manufacturing assurance process are for execution in MAG Phase D1, which, in the program language is often referred to as the production, integration, and test phase and, in MAG terminology, the fabrication and integration phase.

As one may expect, the one CMP that spans in almost equal measure all acquisition and program phases is "MA reviews and audits" (and associated "Lessons Learned" process). The tasks and activities are in general self-contained and individually designed for each of the phases of execution.

Functional and Hierarchical Organization of MA Tasks

In addition to the sequential organization that reflects their eventual order of execution within program technical and system acquisition phases, MA process tasks are also associated and executed according to a system-oriented hierarchical organization that takes into account the typical subdivision of activities in the technical tradition of NSS acquisition programs. Thus, regardless of which specific process is being defined, the associated tasks are organized into standard WBS activity areas. These, at the top level, are intended to group together tasks that pertain to the following types of activity:

- **Program planning**
- **Systems engineering**
- **Hardware/software product oriented**

The **program planning** group includes those tasks within a given CMP that are part of the general planning aspects of a program and which are intended to verify that adequate provisions are incorporated in the contractual and planning aspects of that program as to assure the feasibility and integrity of all the other MA activities that the program will be responsible for executing in later phases.

The **systems engineering** group defines those tasks within a given CMP intended to assure the integrity of requirement, design, and operation provisions that address "system of systems" characteristics and interfaces, as well as the integrity of application of engineering best practices that have general applicability across all areas of a program. With respect to the latter, the systems engineering group of tasks will normally include by reference certain sets of tasks that originally have been defined and functionally organized under the parallel framework of SMDs. More extensive discussion and clarification on this subject is provided in section 2.2.3.2 below.

Finally, the **hardware/software product oriented** group defines the MA activities under a given core process that are associated with a specific hardware or software product, starting at the top level with the system being produced and proceeding top-down along the hierarchy of a standard, generalized work breakdown structure (WBS). The generalized WBS used in this guide is, for the practical purpose of defining product-oriented sub-tasks, not developed further than the subsystem level, i.e., the level directly above the unit level.

Table 2.2-3 illustrates the hierarchical organization of tasks within a generic CMP and acquisition phase, reflecting the above discussion. The definition of generalized WBS levels depicted in the table follows the generic WBS structure recommended by MIL-STD 881B, **"**Work Breakdown Structures for Defense Material Items."

Table 2.2-3, Hierarchical Organization of Task within a Generic MA Process and Phase

Program Planning
Systems Engineering
System
- **Space Segment**
  - **Space Vehicle**
    - **Spacecraft**
      - **Spacecraft Subsystems**
        - **Thermal Control**
        - **Electrical Power and Distribution**
        - **Propulsion and Ordnance**
        - **Structures and Mechanisms**
        - **Guidance, Navigation and Control**
        - **Data Management**
        - **Software**
        - **Telemetry, Tracking and Command**
        - **Communications**
    - **Payload**
    - **SV Ground Support Equipment**
  - **Launch Segment**
  - **Ground Segment**

2.2.3.2 Organization of SMD Tasks

As discussed earlier in Chapter 1, the CMPs are complemented by a set of SMDs. These are a body of engineering disciplines that are generally recognized as providing the basic technical-analytical support and sustainment of MA objectives. The list of SMDs included in the MAG task structure is provided again, for easy reference, in the table below:

Table 2.2-4, Supporting MA Disciplines

Supporting MA Disciplines	Chapter	Appendix
Risk Management	10	A3-7
Reliability Engineering	11	A3-8
Configuration Management	12	A3-9
Parts, Materials and Processess Management	13	A3-10
Quality Assurance	14	A3-11
Systems Safety Assurance	15	A3-12
Software Assurance	16	A3-13

In discussing the sequential and hierarchical organization of SMD tasks the key consideration is that each discipline can be viewed as existing in two distinct, although inter-related contexts; that is:

- The discipline as an end-to-end, standalone and self-contained process
- The discipline as the provider of content to one or more CMPs

The task organization from the two above perspectives is discussed in the two following subsections.

Organization of SMD Tasks in Standalone MA Discipline Context

In the first perspective introduced above, each of the disciplines can be viewed as applicable to a given program or project in its entirety, as an end-to-end, self-contained process that organizes and tracks the tasks pertaining to that discipline in a sequential and logical order.

In terms of sequential order, the tasks in any one of the SMDs are grouped in sub-processes that reflect the same basic acquisition phases that govern the sequential execution of the CMPs. It may also be noted that, when considered in their whole, most of the disciplines will often include some tasks in each of the basic program acquisition phases.

In terms of hierarchy, and in the self-contained perspective discussed in this section, the SMD tasks are grouped functionally, each according to its own scope and depth of articulation.

Organization of SMD Tasks as Core Process Content Providers

In typical program application practice, an SMD process is commonly interwoven with other program execution activities, and may also be tailored to fit specific program needs and constraints. As a result of such tailoring, certain groups of risk management tasks may be programmatically associated with one of the CMPs (e.g, design assurance, manufacturing assurance, etc.), and with one or another portion of the system being designed and produced (e.g., the spacecraft, or a specific payload subsystem). Thus, in programmatic practice, the execution of a group of tasks belonging to a discipline will not only be tailored to the specific needs of a given program, but, as part of the tailoring itself, will also be incorporated into one of the appropriate CMPs and coordinated with the execution of all the other tasks belonging to that core process.

The overall effect of tailoring on the SMD task organization is therefore twofold, as explained below.

In terms of sequential order, each group of discipline tasks is expected to be executed in the same acquisition phase for which it was originally defined and intended within the discipline self-contained, “theoretical” execution. However, depending on which tasks may be dropped as a result of the tailoring process and how the remaining tasks may be inserted into the flow of one or more of the CMPs, “gaps” may be introduced between the execution of a group of tasks and the following group of the same discipline.

In terms of hierarchy, when tailored and inserted into a given core process, a group of discipline tasks will be hosted in that process according to the hierarchical organization of the host process itself (see section 2.2.2 above). Generally speaking, and according to the established practice of the aerospace industry, the MA discipline tasks will be usually inserted under the systems engineering task header (see Table 2.2-3). In some cases, however, when the scope of the group of tasks is more limited, they may be hosted under the header of a more specific WBS item. This would be the case, for example, if the execution of a failure mode and effects analysis (FMEA) is planned by a program only for a specific payload sensor, but not as a general activity covering the entire system that is the object of the program acquisition.

Tailoring of SMDs and CMPs, in terms of the rationales, criteria, and limitations that may apply to different types of programs and acquisition conditions, will be addressed in detail in a future release of the guide.

2.2.4 Government and Contractor Input to MA Tasks

A significant fraction of the tasks documented in the MAVM task database concerns assessment, validation, and/or verification by Aerospace and other MA-dedicated (e.g., SETA) personnel of activities and programmatic products produced by external parties, most commonly the program prime contractor organization, but in certain instances also the government customer organization. For these tasks, the task database includes data fields that identify the task(s) and associated products, such as data items and/or program documents and reports that are needed as items enabling the execution by Aerospace of the task of interest.

2.2.5 Tailoring of MA Process Executions

The definition of MA processes in terms of the task structures documented in the MAVM task database is intended to be as comprehensive and as general as possible. Thus, it represents a "gold standard" reference baseline of MA processes and tasks. This baseline will require tailoring before implementation and execution in any individual program. The nature and degree of tailoring will vary according to a number of factors that are specific to each program, such as program and technology maturity, magnitude and complexity of the program, and amount of Aerospace or other MA-related resources allocated to support the program.

Discussion of the features of the MAVM task database that support program-specific tailoring can be found in section 2.3.1.

2.3 Uses of the MAVM Task Database

Besides being a comprehensive repository of MA process and task guidance and information, the MAVM task database (see Appendix A3) serves three complementary practical uses:

- MA process and task planning and tailoring
- MA process and task plan assessment

- MA quality of execution assessment

The practical use of the database is made possible by the associated software tool and user interface. After the user enters the database using the associated software tool, there are several choices for viewing and tailoring the organization of tasks, and associating them to specific elements in a program WBS structure. The association of SMD tasks with CMP tasks, and of either type with WBS elements, is facilitated by split-screen user tree-views of task hierarchies, as illustrated by the example in Figure 2.3-1. Within each type of MAVM view, specific commands are available to select, delete, move, and associate groups of tasks with one another or with WBS elements. Task hierarchy drilldown can be executed by clicking on the (+) symbol next to any "parent task" heading. Figure 2.3-2 further depicts an example of what type of data is recorded in the database and tool, and displayed when the user wishes to view and/or edit task details, by double-clicking on a specific task title.

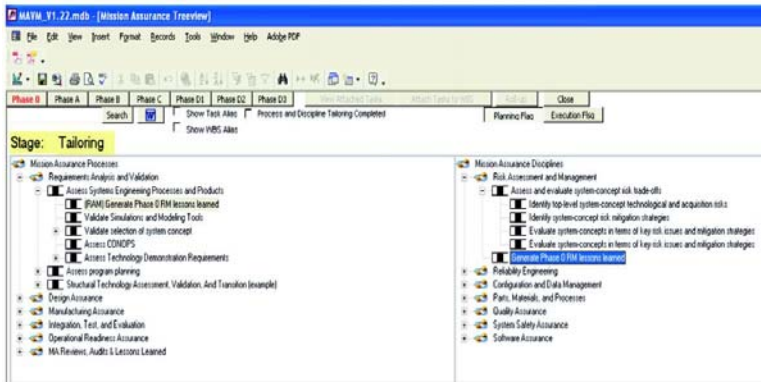


Figure 2.3-1, MAVM Process and Discipline Tree View Screen

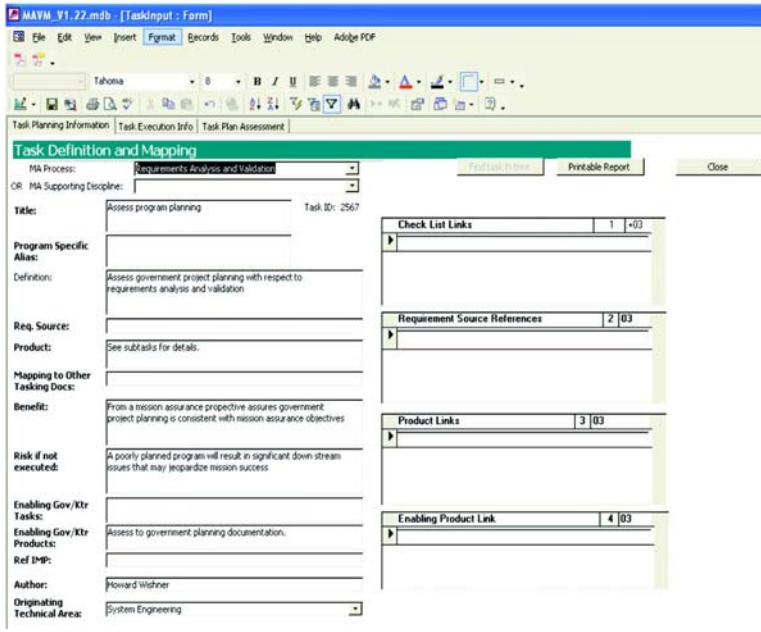


Figure 2.3-2, MAVM Task Details Screen

2.3.1 Planning and Tailoring Use of the MAVM Task Database

The MAVM task database tool includes features that allow a user to edit the task structures according to the type of programmatic tailoring that is desired. Among these features it enables:

- A parent task to be disabled at any level of the hierarchical task tree structure, together with all of its "children tasks."

- A user-selected SMD task (e.g., such as a task belonging to the risk management discipline) to be linked, along with all its "children tasks," to any one of the CMPs and viewed by users of the database as belonging to that core process.

The above MAVM task database editing capabilities permit a relatively straightforward program-specific MA task plan to be defined, configured, and documented by each program.

2.3.2 Assessment Uses of the MAVM Task Database

At the core of both types of assessment usage of the MAVM task database is a classification of MA tasks in terms of criticality, that is, an assessment, for each level of task indenture, of the relative importance of each task in relation to program and mission success. This task criticality assessment and other assessment implements that support the practical uses of the database are discussed in detail in Chapter 3.

Task Plan Assessment

In the plan assessment use, the criticality rating of the MA tasks is combined with a rating of the "depth of effort" planned for their execution within a given program execution plan. The combination of the criticality ratings and planned depth-of-effort ratings produces a set of "MA plan risk" ratings. In this use of the database, "MA plan risk" signifies the potential for future impact on program execution that may result from the depth of effort planned at the onset of a program, or in any case at the pertinent planning stages, in the various MA areas associated with specific groups of tasks. The "MA plan risk" ratings can be used to negotiate and adjust the programmatic level of effort planned for the execution of Aerospace MA tasks and activities.

Task Quality of Execution Assessment

In the execution assessment use, the criticality rating of the MA tasks is combined with an assessment of the completeness and quality of products and results produced by such tasks in their actual execution by a given program. The MA task product/result completeness and quality is judged against a set of evaluation criteria pre-established and documented for each applicable task in the MAVM task database.

The combination of the MA task criticality ratings and execution ratings produces a set of "MA residual risk" ratings. In this use of the database, "MA residual risk" signifies the potential for negative impact on program and its mission success that may result from incomplete and/or poor execution of specific sets of MA tasks.

2.3.3 Alternative User Views of the MA Task Hierarchy

A number of alternative user views are available within the MAVM database tool, depending on the particular user activity being executed. For example, for one of the above mentioned assessment purposes, the

MA task database is normally viewed in its WBS-associated hierarchical format. In this type of view, illustrated by the example in Figure 2.3-3, the program acquisition phase to which the assessment refers is selected via a tab at the top of the user screen. Then the set of tasks to be assessed in relation to a specific program WBS element is displayed on the right side of the split-pane screen when the WBS element itself is selected by the user from the WBS tree displayed on the left side of the screen.

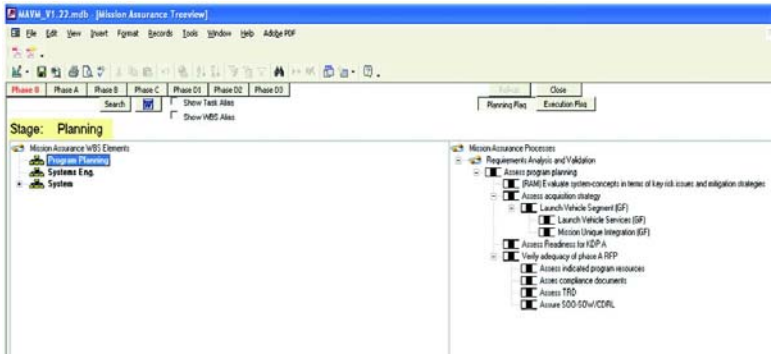


Figure 2.3-3, MAVM WBS Element Task Tree View Screen

As a further example, the assessment of "MA residual risk" remaining after the completion of a specific task may be carried out in the user view illustrated by Figure 2.3-4, which displays a "color-rating" of such a risk, which the MAVM can be asked to derive on the basis of the criticality assigned to the task and whether a set of "task closure criteria" has been met. The rationale and technical underpinning of this type of assessment are discussed in detail in Chapter 3.

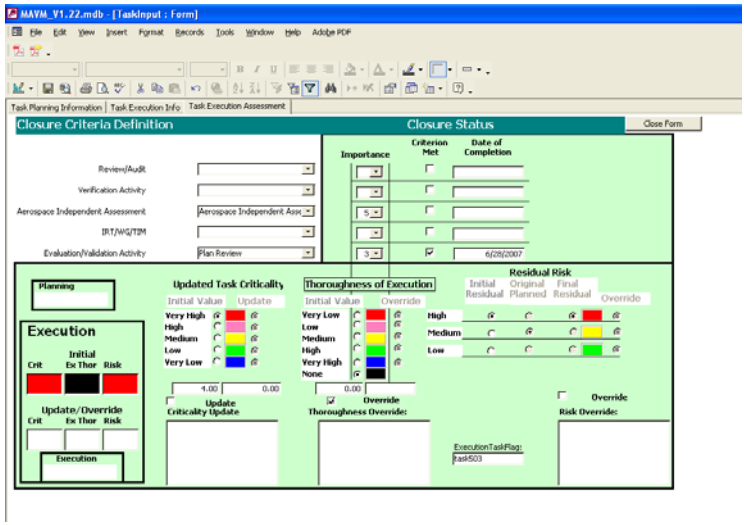


Figure 2.3-4, MAVM Task Execution Assessment Screen

In closing this section, we note that the MAVM database tool is expected to evolve over time. Thus, the examples provided here are to be considered notional illustrations. For detailed information on how to utilize the tool, the user is referred to the MAVM user manual, which will be produced and updated with each new release of the database and associated software.

Chapter 3
Mission Assurance Metrics and Assessment

Sergio B. Guarro
Systems Engineering Division

3.1 Introduction

The preceding sections of this guide have introduced the basic principles and tenets of mission assurance (MA) and have provided, via the associated MA Verification Matrix (MAVM) task database, the overall framework and specific definitions of processes, activities, and tasks through which such principles and tenets can be implemented in the actual execution of a space systems acquisition program. The discussion in this section, and those that follow under the general heading of **MA metrics and assessments,** tackles the subject of "measuring" and assessing the quality of MA planning and execution activities.

The ultimate and most objective metric of successful MA planning and execution is of course the degree of mission success achieved by an organization over the years and over a range and variety of acquisition programs. Unfortunately, this not a "headlight metric" and thus provides information with an intrinsic time lag that is usually too long for either being useful in predicting future MA plan outcomes, or for making effective corrections of course to achieve MA improvements before it is too late to influence the outcome of a specific acquisition program.

Because of the above, the estimation of the effectiveness and quality of MA plans and program execution must in practical terms be based on a combination of metrics that are as objective as possible in their definition and information content, yet by necessity need to rely on subjective judgment. The quality and impartiality of the assessor(s) charged with the responsibility of their estimation will thus be crucial in determining the quality of the assessment itself. The sections that follow explain the basic nature, logic, and practical foundation, as well as the mechanics of formulation and estimation, of the metrics that have been selected for assessment of the MA planning and program execution activities addressed by this guide.

3.2 Basic Types of MA Assessments

As alluded to earlier in this guide, there are two basic types of MA effectiveness assessments that are of interest to most NSS acquisition programs and are accordingly supported by the structure of the MAVM task database and by the associated software tools. These are:

1. The MA Program Plan Assessment (MPPA)
2. The MA Program Execution Assessment (MPEA)

The MPPA seeks to determine the effectiveness of an MA program or set of tasks well ahead of their actual execution, and primarily on the basis of the *planned* breadth and depth of manpower support that an acquisition program intends to put into effect for their execution. The objectives of this type of assessment can thus be summarized essentially in the following terms:

- Evaluating the balance of resources allocated in the MA program plan toward the execution of different types of MA tasks and activities, and assuring that highly important (i.e., "critical") areas and items receive sufficient support and dedicated resources
- Establishing and documenting the final baseline of allocated MA resources, so that both the FFRDC providers of MA services and their government customers recognize an agreed upon level of effort in every MA area of interest

The MPEA, on the other hand, is conducted upon or after the completion of a set of MA program tasks and activities, on the basis of the *actual* breadth and depth of resources applied toward their execution, as well as other more technical and specific indicators of the quality and thoroughness of the actual execution (e.g., the satisfaction of task closure criteria, the resolution of any technical issues, etc.). The objective of this type of assessment can be summarized as follows:

- Evaluating the balance of thoroughness and the timeliness of execution of MA tasks and activities, and assuring that highly important (i.e., "critical") areas and items have received sufficient support and technical attention
- Assessing the level of "residual risk" remaining in any program and mission technical area or system, and accordingly determining the level of readiness for the program to proceed through any major milestone of interest (e.g.,

preliminary design review (PDR), critical design review (CDR), launch readiness review (LRR), Aerospace president's readiness review (APR), etc.)

3.3 Foundation of MA Assessments

Consistently with the types of MA assessment discussed in the preceding section, the foundation and nature of the metrics that have been formulated for the benefit of the users of this guide is oriented toward the estimation of two basic types of MA-related program risk, namely:

- A "*MA plan risk level*," i.e., the level of risk that can be predicted, in any program areas, on the basis of the level of planned resources allocated in the full range of MA activities
- A "*post MA execution residual risk level*," i.e., the residual level of program and mission risk that is predicted to remain in any program areas, after the actual execution of all related MA tasks and activities

The first type of risk metric is to be utilized in support of the MPPA type of assessment, the latter in support of the MPEA type. In the following, for simplicity the two basic measures of risk will be referred to as the "MA plan risk" (MPR) and the "MA execution residual risk" (MERR).

3.3.1 Concurrent Dimensions of MA Related Risk

The most widely accepted and objectively formulated definition of risk is based on the dual dimensions of "likelihood" and "severity of consequences." When applicable in quantitative terms, this concept translates into the use of the directly related dimensions of "probability of occurrence" and "magnitude of consequence severity."

The formulation of MPR and MERR metrics adopted in this guide follows these well-established conceptual tenets, although they are adapted both in terminology and substance to the types of risk to be assessed and to the predominantly qualitative nature of the related assessments that are possible.

The inference and assessment of MPR and MERR risk levels are based on the following reasoning and assumptions:

1. The severity of program and mission consequences that can be projected in relation to the execution or non-execution of a given MA task or set of tasks is directly proportional to the importance of that task. In this guide and from here on, this will be referred to as the "task criticality," and will be assessed with an associated "level of criticality—i.e., a very important MA task will be referred to as being highly critical, whereas a marginal one will be referred to as having a very low level of criticality.
2. The likelihood of a MA task or group of tasks being thoroughly and effectively executed is directly proportional, when referring to MPR, to the planned level of breadth and depth of task execution, and, when referring to MERR, to the actual level of breadth, depth and quality of task execution. For simplicity of terminology, from now on the former will be referred to as the planned "depth" of task execution, and the latter as the actual "quality" of task execution.

   The level of depth of MA task execution that can be predicted at the time of task planning, i.e., when the ultimate objective is to estimate an MPR level, may be assumed to be directly proportional to:

   - The level of program resources allocated to the task in the task planning stages, i.e., in administrative language, to the Staff Time Equivalent (STE) level planned for the task (or group of tasks)

   Applying similar reasoning, the level of quality of MA task execution that can be assessed after the task has been closed out, i.e., when the ultimate objective is to estimate an MERR level, may be assumed to be directly proportional to:

   - The STE level actually applied in the execution of the task or group of tasks

   - The degree of actual satisfaction, by the task execution, of the combination of closure and exit criteria that are technically and programmatically applicable to the task (and which have been identified as such).

1. Finally, the level of risk that can be estimated for either MPR and MERR, using as a basis the metrics definitions and related assumptions discussed above, is directly proportional:

    - When estimating MPR level, to the difference between the estimated task criticality level and the planned level of depth of task execution (e.g., a task assessed as being highly critical for which the level of planned resources is very low will result in a high MPR estimated risk level)

    - When estimating MERR level, to the difference between the estimated task criticality level and the actual level of quality of task execution (e.g., a task assessed as being highly critical for which the level of assessed quality of execution is very low will result in a high MERR estimated risk level)

3.4 Formulation of the Assessments Supported by the MAVM Task Database

As mentioned earlier, the structure of the MAVM task database and the associated software tool support the execution of both basic types of MA effectiveness assessment that are of interest to most NSS acquisition programs, i.e. a MPPA and a MPEA. The detailed mechanisms of this assessment, as executed by the MAVM task database software tool are discussed in the following sections.

3.4.1 MPPA

This section discusses and documents in detail the framework, algorithms, and logic rules applied in a MPPA type of assessment.

3.4.1.1 Assessment of Task Criticality

The task criticality level is the assessed level of importance of a given MA task, “measured” on a qualitative scale that ranges from “Very Low” to “Very High.” The full set of possible criticality levels is provided below in Table 3.4-1, which also provides the geometric progression of quantitative criticality weights currently associated with each qualitative level, for the purpose of task criticality “roll-up,” as discussed below.

Table 3.4-1, Task Criticality Levels

Qualitative Level	C (Quantitative Criticality Weight)		
VH (Very High)	4	or	> 3.36 for “derived”
H (High)	2.83	or	> 2.38 and <= 3.36 for “derived”
M (Medium)	2	or	> 1.68 and <= 2.38 for “derived”
L (Low)	1.41	or	> 1.19 and <= 1.68 for “derived”
VL (Very Low)	1	or	<= 1.19 for “derived”

A geometric, rather than linear, progression of criticality weight has been assumed in the definition of criticality levels. This is based on the assumption that a “Medium” criticality task is believed to be twice as important as a “Very Low” criticality, and that a “Very High” criticality one is believed to be twice as important as a “Medium” criticality one. The “High” criticality and “Low” criticality quantitative weights have then be obtained from the standard laws of geometric series progression, i.e., they satisfy the following formulations:

$$C(H) = \sqrt{C(VH) \times C(M)} \qquad (1)$$

and:

$$C(L) = \sqrt{C(M) \times C(VL)} \qquad (2)$$

3.4.1.1.1 Roll-up of Task Criticality Ratings

As it has been discussed in the sections that describe the MA task organization, the tasks within a core MA process (CMP) or supporting MA discipline (SMD), or within a program work breakdown structure (WBS), are hierarchically linked through a parent task to children tasks ordered association. It is therefore natural to consider the level of criticality of a parent task as being, under normal circumstances, determined by the combination of the criticality levels of all its children tasks. Thus, for example, if a task is the parent of a set of tasks that have all been rated as having “Very Low” criticality, it is reasonable to also deduce for that task a criticality rating of “Very Low,” rather than one of “High” or “Very High,” or even “Medium” or “Low.”

The criticality roll-up algorithm directly reflects the above line of reasoning and assigns the parent task criticality weight an average value calculated from the set of criticality weights assigned to its children tasks. That is:

$$C = \frac{\sum_{i=1}^{N} CC_i}{N} \qquad (3)$$

where:

C = criticality of the parent task

CC_i = criticality of i-th child task under the parent task

N = number of children tasks under the parent task

3.4.1.1.2 Override of Task Criticality Roll-up

The criticality roll-up scheme discussed above is based on logical assumptions, and may also be adjusted to reflect special program conditions—for example, adopting a different geometric progression ratio between contiguous criticality levels, or even using a linear rather than geometric scale progression (however, the latter is not recommended, as it tends to blur the distinction between different criticality levels as the assessment is rolled up the task hierarchical structure).

There may exist special circumstances under which the criticality assessor may desire to override the blending effect of the roll-up scheme, in order to preserve the program attention to a task of extremely high criticality and importance. An example of this is presented by tasks concerning the handling of “single-point failure” mission items, i.e., hardware, or software items that, if improperly developed or integrated into the system, may by themselves induce a total system and mission failure, without possibility of salvage or recovery via redundant function or work-around.

For the above circumstances, the software tool associated with the MAVM task database allows an assessor to override the calculated criticality level of a parent task with a level that he or she will directly assign. The logging of a rationale and justification is required in these special cases of criticality roll-up override.

3.4.1.2 Assessment of Planned Allocation of Task Resources

The planned depth of MA task execution is assessed on the basis of a six-level qualitative scale, which is mirrored in the MAVM task database software tool by a quantitative planned depth linear scale, as shown in Table 3.4-2.

Table 3.4-2, Task Planned Depth Levels

Qualitative Level	D	(Quantitative Planned Depth Weight)	
D5	5	or	> 4.5 for “derived”
D4	4	or	> 3.5 and <= 4.5 for “derived”
D3	3	or	> 2.5 and <= 3.5 for “derived”
D2	2	or	> 1.5 and <= 2.5 for “derived”
D1	1	or	> 0.3 and <= 1.5 for “derived”
D0	0	or	<= 0.3 for “derived”

A “D0” level of depth simply indicates that there is no existing plan to execute the task of interest. In this regard, depending on the more specific type and nature of the assessment being carried out, the assessor may assign a level “D0” if a task is not planned to be executed by any organization, or when it is not planned for execution by The Aerospace Corporation program office personnel, although it may be assigned for execution to another organization.

3.4.1.2.1 Roll-up of Planned Task Depth Ratings

The roll-up of planned depth along the task hierarchy takes into account both the criticality and the planned depth of children tasks to obtain a “derived” parent task depth. The same algorithm is applied, whether the children task metrics have directly been assigned by an assessor, or themselves have been derived from the metrics established for their own children tasks. The roll-up algorithm applies a weighted sum formulation as indicated in Equation (4) below:

$$D = \frac{\sum_{i=1}^{N} (CC_i \times DC_i)}{\sum_{i=1}^{N} CC_i} \qquad (4)$$

where:

D = depth-of-execution of a parent task

CC_i = criticality of i-th child task under the parent task

DC_i = depth-of-execution of i-th child task under the parent task

N = number of children tasks under the parent task

3.4.1.2.2 Override of Planned Task Depth Ratings Roll-up

As in the roll-up of task criticality, the MAVM task database software tool allows the assessor to override the derived assessment of planned task depth with a directly assigned level. Again this may occur under special circumstances and require the logging of a rationale and justification to document the override and its reasons. A typical situation under which the application of an override may be necessary is when one individual child task overwhelmingly outweighs in criticality all the other children tasks of a given parent task, so that the assessor judges that the planned depth of the parent task must almost directly mirror that of the "super-critical" child task.

3.4.1.3 Estimated Level of Task Plan Risk

Once both the criticality and the planned depth of any given task have been established, whether by direct assessor's assignment or algorithmic roll-up, a level of resulting MPR can be obtained for that task, based on the principles previously discussed.

More specifically, the three levels, "High," "Medium," and "Low," are used in the definition of the MPR metric, and the actual MPR rating for a task is determined according to the combination of its criticality and depth ratings, according to the simple mapping scheme illustrated by Table 3.4-3 below.

The rationale underlying the mapping is essentially that the higher the (positive) gap between the criticality and depth level values, the higher the risk. As a general rule, no gap or a negative gap will result in an MPR rating of "Low." This scheme could also be expanded to a situation where the number of MPR levels was extended to five instead of three—for example, by introducing the levels "Very High" and "Very Low" at the two extreme opposites of the risk spectrum.

Table 3.4-3, Task MPR Risk Rating Derived from Criticality and Depth

Criticality Rating	Depth Rating	Derived MPR Rating
Very High/High	D5 / D4	Low
Very High/High	D3 / D2	Medium
Very High/High	D1 / D0	High
Medium	D4 / D5 / D3	Low
Medium	D2 / D1	Medium
Medium	D0	High
Low	D5 / D4 / D3 / D2 / D1	Low
Low	D0	Medium
Very Low	Any	High

3.4.1.4 Roll-up and Estimation of MPR by MA Area

The roll-up algorithms can in theory be applied recursively through many levels of task hierarchy to obtain criticality, depth, and MPR ratings at any level of MA task indenture, including the very extreme of obtaining one triad of values for an entire MA program plan. While this is theoretically and practically allowed by the MAVM task database structure and by the algorithms just discussed above, the reader and MA assessor are cautioned to carefully consider the meaningfulness of obtaining and communicating such an oversimplified and over-summarized risk picture of what is usually a very complex and variegated MA program plan and associated risk.

3.4.2 MPEA

This section discusses and documents in detail the framework, algorithms, and logic rules applied in a MPEA type of assessment. The MPEA assessment process is similar in concept and basic execution steps to the MPPA process discussed in section 3.3.1. The principal differences of substance between the two processes are summarized below:

- The MPEA uses the assessed quality of task execution as the indicator of the likelihood that the MA task, as actually executed, may have a negative program and/or mission impact, whereas the MPPA uses the planned depth of task

execution as the indicator of the likelihood that the MA task, as planned and staffed, may have a negative program and/or mission impact.

- Unlike the MPPA "planned depth of execution," which is directly estimated on the basis of program resource information, the MPEA "quality of task execution" is estimated via a sub-process that includes the consideration of whether a set of task closure criteria and technical quality standards have been met. This sub-process is discussed in detail in section 3.4.2.2 below.

- The MPR risk measure used in the MPPA process is only a function of task criticality and planned depth of execution, whereas the MERR residual risk measure used in the MPEA process is a function of the task criticality and quality of execution, but also of the initial MPR level itself that has been established for the task or set of tasks of interest. That is, unless other special activities are added to a task beyond the planned depth of execution level at execution time, the MERR rating of a task cannot ever be better than the MPR rating. That is the residual risk after task execution can never be lower than the task "planned risk."

Further discussion of the key points presented above is given in sections 3.4.2.1, 3.4.2.2, and 3.4.2.3 below.

3.4.2.1 Update of Task Criticality

The task criticality scales used for the MPEA assessment are the same as these discussed in section 3.4.1.1 and illustrated in Table 3.4-3. However, at the time of carrying out the MPEA assessment it may be determined that the criticality of a task and/or set of tasks needs to be revisited and updated with respect to the value(s) assigned or derived at the time of task planning, when the MPPA assessment was executed. If this is the case, it is important to make sure that the MPPA portions affected by the criticality rate changes also be updated and verified, as any significant criticality changes can and will result in changes to the original MPR risk ratings. This is also very significant for the MPEA assessment itself because, as implied by the discussion given in the last bullet above, any MPR rating changes establish a new risk baseline that represents the best possible risk ratings achievable in terms of MERR residual risk.

3.4.2.2 Assessment of Quality of Task Execution

The quality of task execution is assessed via a discrete scale that mirrors the one used in rating the planned depth of task execution metric used in the MPPA assessment. This scale is illustrated in Table 3.4-3 below. As mentioned earlier, however, the actual rating in the quality of execution scale is normally not assigned directly by an assessor, but instead it is derived by a weighting algorithm that takes into account different sets of task closure criteria that have been defined for each task, and their relative importance. The quality rating "Q0" signifies that the task has not been executed at all.

Table 3.4-4, Task Execution Quality Levels

Qualitative Level	Q (Quantitative Quality Weight)		
Q5	5	or	> 4.5 for "derived"
Q4	4	or	> 3.5 and <= 4.5 for "derived"
Q3	3	or	> 2.5 and <= 3.5 for "derived"
Q2	2	or	> 1.5 and <= 2.5 for "derived"
Q1	1	or	> 0.3 and <= 1.5 for "derived"
Q0	0	or	<= 0.3 for "derived"

The process of quality of execution assessment is summarized below in its basic steps:

1. The task closure criteria are reviewed and/or established, according to the nature of the task and using pre-established classifications that are provided by the MAVM task database tool (and can be expanded further as needed). Typical "classes" of closure criteria are:
   - Satisfaction of formal technical verification of technical activity products
   - Satisfaction of program reviews "exit criteria"
   - Satisfaction of independent assessment "exit criteria"
   - Satisfaction of independent quality and product assurance audits, etc.
2. The relative importance of a closure criterion in determining the quality of execution of a task is rated by the assessor on a discrete scale from 1 to 5.
3. The satisfaction of all closure criteria is verified and assessed by assigning a 1 value to the criteria satisfied at

task completion and a 0 to the criteria not satisfied at task completion.

4. The task quality of execution is algorithmically rated using the formula:

$$Q = Q5 \times \frac{\sum_{i=1}^{M} (IC_i \times TC_i)}{\sum_{i=1}^{M} IC_i} \qquad (5)$$

where:

Q = task quality rating (a value between 0 and 5)

TC_i = rating of i-th task closure criterion (= 0 if criterion not met, = 1 if met)

IC_i = relative importance of i-th task closure criterion (a discrete value between 1 and 5)

3.4.2.2.1 Roll-up of Task Quality Ratings

The task quality ratings are propagated upward through the MA task structures in exactly the same fashion as the planned depth ratings, i.e., via a weighted algorithm that implements Equation (6) below:

$$Q = \frac{\sum_{i=1}^{N} (CC_i \times QC_i)}{\sum_{i=1}^{N} CC_i} \qquad (6)$$

where:

Q = quality of execution of a parent task

CC_i = criticality of i-th child task under the parent task

DC_i = quality of execution of i-th child task under the parent task

N = number of children tasks under the parent task

3.4.2.2.2 Override of Task Quality Ratings Roll-up

As for the planned depth of execution ratings roll-up, the MAVM task database software permits an override of the derived, rolled-up rating of task quality to be overridden by the assessor, provided a rationale and justification is provided and recorded. A typical situation where this may happen is when a parent task quality is predominantly influenced by the quality of execution of only one, very crucial, child task.

3.4.2.3 Estimated Level of Residual Risk after MA Task Execution

If the criticality rating of a task has not been changed and updated after the time of MPPA assessment execution, the MERR rating (which expresses the residual program risk impact of a task or group of tasks that remains after task execution) will be based on:

1. The "planned task risk" MPR rating derived at MPPA time
2. The task quality rating assessed according to the discussion in section 3.4.2.2

The MERR rating follows a simple mapping scheme that determines the "High," "Medium," or "Low" risk value based on the combination of MPR and "quality of execution" ratings that have been determined for a task or group of tasks. Table 3.4-5 below illustrates this mapping.

Table 3.4-5, MERR Risk Rating Derived from Task MPR and Quality

MPR Rating	Quality Rating	Derived MERR Rating
High	any	High
Medium	Q5 / Q4 / Q3	Medium
Medium	Q2 / Q1 / Q0	High
Low	Q5 / Q4	Low
Low	Q3 / Q2	Medium
Low	Q1 / Q0	High

3.4.2.3.1 Override of MERR Ratings

It is very important to understand that the basic assumption underlying the rating scheme expressed in Table 3.4-5 is that the task closure

criteria established for a given task are set to verify that the task is being carried out according to planning. In other words, meeting these criteria simply ensures that the task execution will meet the MPR risk "target" rating established in the planning stages. Meeting the criteria *does not* insure that the task execution is as good as possible and thus will result in a minimal level of risk, i.e., a level of risk that is actually lower than the "planned level."

If the assessor believes that the execution of the task, for whatever combination of reasons and unplanned circumstances, actually has exceeded the planned depth of execution and has met a much higher level of quality and closure criteria than those initially planned, then he or she will have ground and justification for overriding the MERR "derived rating" and for possibly allowing the MERR rating to be better than the initial MPR risk baseline. As in any other case of rating override, such action requires the logging of a rationale and justification in order to be allowed by the MAVM task database software.

3.4.2.4 Roll-up and Estimation of Residual Risk by MA Area

MERR risk ratings may be rolled up as high in the MA task structures as the user desires. The same caution expressed in section 3.4.1.4 regarding the roll-up of MPR ratings applies to MERR roll-up as well.

Chapter 4
Requirements Analysis and Validation

Howard D. Wishner
Navigation Division
Dan W. Hanifen
Baseline Systems/Payload
Sergio B. Guarro
Systems Engineering Division

4.1 Introduction

In mission assurance (MA), the **requirements analysis and validation** core MA process (CMP) includes joint program development and MA activities conducted primarily at the front end of a system acquisition life cycle. This does not include the actual verification that the system design and the as-built system product meet the original requirements and specification, as the latter activities are included in the framework under the design assurance, manufacturing assurance, integration, test and evaluation, and operational readiness assurance (ORA) processes.

While the contractor is responsible for mission analysis, system synthesis, requirements analysis and allocations, and requirements/specification development and validation activities, The Aerospace Corporation in partnership with the government program office team performs associated independent requirements analysis activities supporting MA. Parallel government and contractor processes involve a set of orderly tasks using analytical tools and simulations to synthesize, develop, and ensure a self-consistent set of program requirements that are expected to meet user needs within affordable costs and acceptable schedules. User needs and mission requirements (including those for MA – i.e., reliability, availability, and maintainability) are decomposed into system requirements and flowed to build-to specifications and interfaces. The following discussion treats the term “specifications” as being synonymous with the term “requirements.”

As mentioned above, requirements development, analysis, and validation activities are most active in the earlier stages of the system development life cycle beginning with system requirements formulation in MAG Phase A, and continuing through MAG Phase C activities of development and design. Later in the life cycle and before

system deployment, ORA ensure the existence of a closed loop process that provides confidence that the built-to system meets the intended needs of the users.

4.2 Definitions

Validation provides confidence (through independent analysis or test) that the technical means and processes accomplish their intended purpose[7], in this case to meet user needs. At the system level, validation occurs before the as-built system is transitioned into mission operations.

Verification is a system engineering process that proves the as-built item complies with the requirements baseline as determined by test, analysis, demonstration, inspection, and/or similarity performed at all levels from the lowest level configuration item (CI) to the system. Verification is typically done in a hierarchical fashion from the lowest level requirements up to systems requirements. Test, analysis, demonstration, and inspection are known as verification methods and are applied at the appropriate and lowest level of assembly where the selected method is most perceptive at providing the needed data.

4.3 Objectives

The objective of requirements analysis is to produce a complete and optimal set of requirements based on rigorous analysis of user needs. The optimization may be constrained by overall acquisition strategies such as design to cost (DTC) or spiral development, based on use of thresholds and objectives requirements. Requirements analysis transforms those needs into architecture concepts and views, models/simulations, functional and system performance requirements, life cycle costs, schedules (including capabilities milestones), and risks that must be considered and mitigated in order to meet top-level system requirements. A system's requirements baseline also includes external and internal interface requirements that are iteratively adjusted as feedback is received from the government program office, the design and manufacturing process, the integration and test process, the operators, and the end users. In most instances, cost drives considerations and it is allowed to vary so that a clear understanding of

[7] Validation definition adapted from T.D. Hoang, Aerospace TOR-2004 (3909)-3360, *Systems Engineer's Major Reviews for National Security Space System Programs*, page 16, 11 May 2004. Restricted distribution.

the cost of incremental capabilities can be obtained. This closed loop allows for feedback into the requirements process that drives development during the start of a new acquisition, and also provides continuous feedback from the end users to improve product quality, maintainability, and utility based on operational experience. Requirements analysis is successful when the users' needs have been successfully captured and a completed baseline of verifiable requirements, concept of operations (CONOPS), and specifications (including interfaces) is established.

The objective of **requirements validation** is to ensure that the right set of requirements, if used properly to guide a system's development, will result in a system that meets user expectations and needs and performs the required functions. Due to the importance of modeling and simulation in the ORA process, special emphasis is placed on accurate modeling and simulation as part of MA. Therefore, the objective of model/simulation validation is to ensure all the contractor models are understood and built according to their respective specifications (verification), and to ensure that the model/simulation fairly represents the item (component, unit, subsystem) or system it is intended to model or whose behavior it simulates.

The objective of requirements verification is to produce physical evidence proving that each requirement in the requirement/specification hierarchy has been satisfied using approved verification methods. The objective of verification planning is to establish the process, tools, and forums to successfully verify system requirements.

It is important to take note of an important difference between a *validation* activity and a *verification* activity. In general terms, *validation* addresses the rationality and reasonableness of a technical approach or process, whereas *verification* seeks to prove the correctness and goodness of the products that are generated by a technical approach and/or process.

From the above distinction, it follows that it is always possible to execute a validation activity in parallel with the definition of the approach or process, and yet before the products out of such approach or process become available. Whereas in general, a true verification activity cannot be fully executed and completed until the products of the technical approach or process have become available. Accordingly, this guide considers the requirements validation process as being executable in the early acquisition phases of a program, whereas the

requirements verification process, which is also considered in this guide to be part of the requirements analysis and validation CMP, can only be planned in these phases (acquisition Phases A and B). The actual overall requirements and system verification process is considered by the guide as being apportioned between the design assurance and the integration, test, and evaluation CMPs, and as such it is executed for the most part in the complete design and build and operations phases (acquisition Phases C and D).

4.4 Practices and Tasks

4.4.1 Requirements Analysis

Although requirements analysis is applied in an iterative fashion during all program acquisition phases, the initial acquisition phases are the most intense and focused on the functional analysis and allocations, system requirements, architecture, and design synthesis. As established by National Security Space Acquisition Policy (NSS 03-01, 12 December 2005), top-level capability/mission needs are defined in a Joint Oversight Requirements Committee (JROC) initial capabilities document (ICD) which addresses needed functional war fighting capabilities along with a recommended approach. This document forms the framework for the pre-key decision point (KDP) A concept studies. In these studies operational concepts are documented and analyzed, functional architectures examined and alternative solutions addressed using a variety of analytical tools and simulations leading to the KDP A decision.

During MAG Phase A (concept development), the preliminary concept is further developed by examining synthesized architectural solutions and requirement sets using more refined tools and simulations. The resulting systems are assessed in terms of their ability to meet the desired performance levels, technology availability, robustness, growth potential in meeting user objectives (goals), interoperability within a system of systems, life cycle cost, program schedule and associated acquisition plan. Numerous technical interchanges are held with the various stakeholders (e.g., users) until a consensus is reached on selected performance, and associated cost and schedule risk. The user then documents the selected set of capabilities in a capabilities development document (CDD) and associated key performance parameters (KPPs). The CDD is then used to feed to the acquisition strategy and associated acquisition baseline and test and evaluation approach required for a KDP B decision.

In parallel to this government effort, the contractor further refines the selected requirement set and associated architecture decomposes the operator's CONOPS by developing a set of operational architecture views and the system specification, and prepares for a system requirement review (SRR) and subsequent system design review (SDR). Additional program planning documents are also prepared by the contractor/government team such as the system acquisition and management plan (SAMP), and preliminary test and evaluation master plan (TEMP), program protection plan, logistic plan, and system safety and hazard management plans. Additionally, launch and space vehicle, launch base and launch infrastructure, and other system interface requirements are addressed and documented.

Given a mature set of system requirements consistent with program planning, system allocations are made to lower-level elements, subsystems, units, and components to establish performance, environmental, functional, design and construction, operability, and interface requirements within a typical system's requirements baseline.

MA tasks supporting requirements analysis are:

- **Independent evaluation of requirements traceability,** which traces top-level system requirements documents such as capability development documents, CONOPS, and government or procuring agency directives and policy. Top to bottom traces are conducted as well as bottom to top to identify orphaned or derived requirements. The resulting set of allocated system requirements (functional, performance, interface, environment, and process) are subjected to a final review to assure that they are verifiable with the verification methods selected. Different system and operational views are also developed to assure a self-consistent across the functional areas, an operable set of requirements, and the mission effectiveness of the system. Access to and use of the program's requirements database containing the system requirements and lower-tier allocations is required. Access to and use of the program's requirement database or tool that correlates verification methodology to each requirement also is required.

- **The independent mission effectiveness** task verifies expected system performance through system modeling and simulations. The system's performance attributes are

quantified and compared against baseline design reference case tests that are conducted by the developing contractor and independently conducted on a different set of tools than those used by the developing contractor(s).

- **Cost and schedule elements** may be independently evaluated at different levels within the government to assure that realistic cost profiles and detailed schedules are being used by the procuring agency and that adequate management reserves exist to handle unforeseen problems. While cost and schedule are not the focus of The Aerospace Corporation's technical MA effort, it is nevertheless important to recognize that without adequate resources, the desired technical performance may not be achievable. It is also important to ensure that adequate staff, schedule, and funding are allocated to MA tasks.

- **Mission analysis validation** ensures that the user's needs have been correctly captured and system performance parameters distilled to evaluate system capabilities as the system concepts evolve and trade studies emerge.

- **Models and simulations used in requirements analysis must be verified and validated** in order to have confidence in their output. This task includes an examination of the design and architecture of each model or simulation; all design-to requirements (if applicable); any assumptions and constraints; data used by the model or simulation; the operating characteristics of the targeted unit, subsystem, or system; comparison benchmarks; and the behavior of the model and/or simulation to actual or predicted behavior provided from an independent source or means, such as another simulation.

4.4.2 Requirements Validation

The objective of requirements validation is to ensure that the right set of requirements, if used properly to guide a system's development, will result in a system that the meets the user's expectations and needs. The primary means to accomplish this is through modeling and simulation. After development, requirements verification (using test and demonstration as the primary means) will certify that the system satisfies the requirements. Specific requirements validation tasks include:

- Evaluation of user operational scenarios and the establishment of design reference cases

- Evaluation of DRCs and the establishment of KPPs

- Evaluation of architecture alternatives against operational scenarios, DRCs, and KPPs

4.4.3 Verification Planning

Verification is a systematic, thorough, rigorous and iterative, hierarchical process that certifies system requirements, including interfaces, and mission requirements and all lower-tier requirements have been fully satisfied by the end item being acquired. While the goal is to verify all requirements before launch, on–orbit testing may be required due to ground test and simulation limitations. The verification process is mandated contractually and led by the prime contractor with participation from subcontractors and the government program office. Diverse teams participate through verification working groups (VWGs), integrated product teams (IPTs), or subsystem development WGs. These WGs include system engineering, quality assurance, hardware engineering, software engineering, and test engineering. The strategy and methodology for a program's verification process is defined in its program-unique verification plans, test plans, and modeling/simulation plans. A successful verification process includes active participation, open communications, and timely and comprehensive data exchange between all participants. Specific tasks include:

- Establishing an engineering and program management consensus on the verification methods applied to each requirement, tracking tools, and the roles/responsibilities of organizations and individuals. Requirements can be verified by the following methods: analysis, test, physical measurement, inspection, destructive physical analysis, similarity, and demonstration. Choice of method often requires significant risk tradeoffs due to practical limitations (cost, schedule, and testing constraints) in using the preferred verification method, testing. Where the preferred method (test) is not used, rationale is provided for employing alternative methods. The planning is directly linked to system and lower-level integration and test (I&T) planning efforts and documents the "agreed-to" verification evidence of

completion (EOC) for each level in the requirement or specification hierarchy. A key product of this set of tasks in the planning process is a contractor developed verification plan that becomes a cornerstone document for program management and MA.

- Providing the necessary forum(s) to ensure that there is a common understanding of the requirements, that the requirements are stated in verifiable language, that the verification method and approach are clearly established, that realistic testing with realistic data is planned, and that the proper tools/processes are in place to proceed with verification activities when the design is sufficiently mature and as-built items are available. This also includes creating forums to ensure there is a comprehensive plan to execute all verification methods within the given resources and schedule.

The overall verification process is shown in Figure 4.4-1 as it evolves through the planning to implementation phase. As the design is further defined in detail, the corresponding verification planning becomes more specific and detailed.

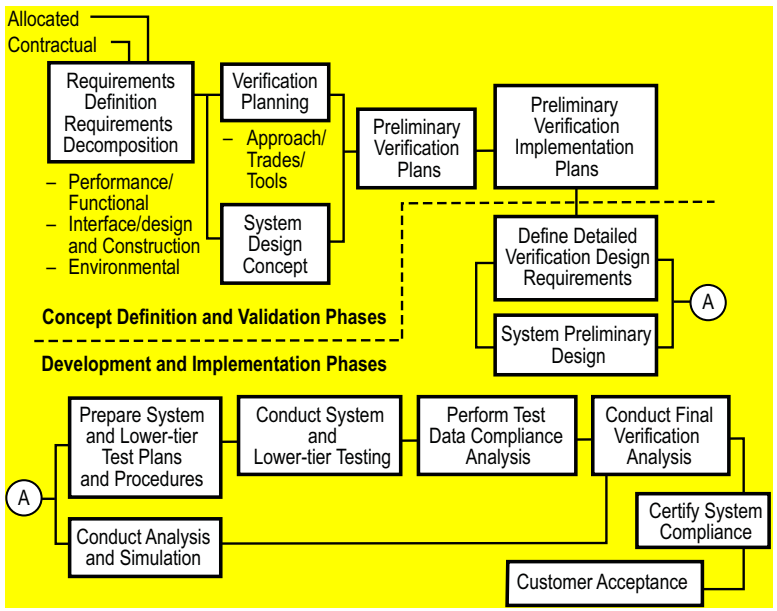


Figure 4.4-1, Typical Verification Process

Verification planning and implementation are also accomplished in a hierarchal fashion, as depicted in Figure 4.4-2 which parallels the requirement decomposition and allocation process.

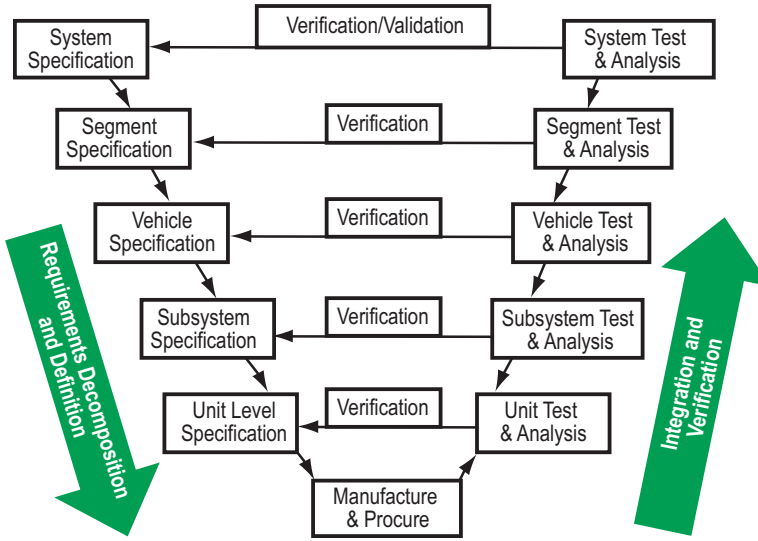


Figure 4.4-2, Hierarchal Verification Process

4.5 Strategies and Execution by Acquisition Phase

As identified in section 4.3, the objective of the requirements analysis and validation process is to produce a complete and optimal set of requirements based on rigorous analysis of user needs. Requirements analysis transforms those needs into architectural concepts and views, models/simulations, and functional and system performance requirements. The process that generates these products is primarily executed by the prime contractor. However, the associated Aerospace MA process has a distinct role in assuring the adequacy of these products in achieving mission success. Within this section, the Aerospace detailed tasks, which are implemented in assuring the requirements analysis process, are described.

The tasks are presented as a unique set of tasks distinct from other MA processes. However, by necessity the MA processes often overlap in some areas of program activity. Consequently, there may be some requirements analysis and validation tasks that have some degree of overlap with tasks conducted under an associated MA process or

discipline. This sort of occasional overlap or duplication should not be viewed as a hindrance in using this guide, since in general it is the necessary consequence of the definition of a logically flowing and complete set of MA tasks for each CMP or supporting MA discipline (SMD). It is recommended that the complete set of processes and disciplines be examined for possible overlaps when tailoring the set of MA tasks for a specific program.

While Aerospace's requirements analysis and validation effort continues throughout the program life cycle, it is most active during the early phase of the program. This early concentration of tasks is demonstrated by inspecting the database shown in Appendix A3 where there are many more tasks identified in early MAG phases than in the later phases. Appendix A3 more clearly shows the organization of the requirements analysis and validation MA area. As can be seen, the tasks area is organized by the phases. Starting with MAG Phase 0, the pre-milestone A time period, MA is focused on the adequacy of the acquisition planning and the Phase A request for proposal (RFP) and readiness for KDP A. Additionally, Aerospace will typically conduct mission concept studies, assessing mission feasibility in terms of achievable performance, technology readiness, and risk. Consistency with the initial concept capability document and preliminary CONOPS will be verified. For technology demonstration programs, Aerospace will assure the adequacy of the planned demonstration requirements in terms of measures of performance, scale, and fidelity and technology readiness to support that demonstration. The outline of these tasks can be seen in Appendix A3.

After Phase A contractor award, requirements analysis and validation activities shift to assuring the accuracy and completeness of system requirements and associated requirement allocations to the system segments. A key MA product in this phase is the system requirement set. Verification planning will also be initiated in this phase, with Aerospace assuring that the verification process addresses all hierarchical level of integration leading to a final system-level validation of the "system-of-system" (SOS) interfaces and requirements. Related specialty engineering and system engineering products such as the reliability program plan, configuration management plan, etc. are reviewed with respect to MA provisions. Phase A is the most active and critical phase relative to assuring the proper development of requirements that will be baselined, flowed down, and followed during the remainder of the program. The end of Phase A is again focused on the adequacy of acquisition planning and

Phase B RFP and KDP B readiness. The overall outline of Phase A tasks, as well as the outline for all other phases, is shown in Appendix A3.

Some programs will carry two or more contractors through this phase leading to a down-select via the Phase B RFP. This RFP may in turn cover the scope of work through Phase C and possibly Phases D1 and D2 with options for D3 as well as follow-on production. It is important that the requirements analysis and validation MA provisions are closely examined in not only the immediate Phase B effort, but in all follow-on contract phases.

Phases B and C are similar in content, establishing the preliminary and final designs, respectively. During these phases the requirements analysis and validation CMP focus will shift from verifying the allocated baseline system requirements to maintaining the integrity of the total requirements set through the end of Phase C. During both phases, the system requirement set validation process will continue as requirement changes and clarification requests are created in response to design issues encountered in the detailed design process. At the lower subsystem and unit levels, Aerospace will assure the accuracy and completeness of the associated allocated requirement set as well as verify its feasibility relative to its enabling technology readiness level.

Verification planning should be complete by PDR with subsequent detailed verification criteria being established by CDR. System validation planning completion may be delayed to Phase C. In turn, MA will focus on assuring that a viable verification planning process has been developed and is producing an effective verification plan that emphasizes verification by test whenever possible. The plan should also be applied seamlessly across all associated and subcontractors. For those requirements being verified by analysis, those analyses would normally be complete by CDR with Aerospace's MA activities under the design assurance process providing an independent assessment of the associated verification reports. Based on the criticality of the specific design area, those activities could range from merely verifying that the contractor's activity was completed to a fully independent analysis by Aerospace.

The normal design development activities during MAG Phases B and C routinely overlap in time as detailed design and verification requirements are flowed down to lower levels and verifications are completed and flowed up to the next higher level of integration to

support an integrated verification. In some cases where MAG Phase C activities include pre-production manufacturing, unit-, or assembly-level demonstrations and qualifications will actually be completed during Phase C. MA would assure the adequacy of these verifications while determining whether that verification can be repeated at a higher level of integration and ultimately validated in a SOS environment. This activity is viewed distinctly from the design assurance process, which often uses the same data to assure the adequacy of the design. For example, in this later case, test results that demonstrate requirements compliance could be further used to verify their consistency with the detailed design documentations. Discrepancies between the test results and design documentation would need to be reconciled even though the results have met requirements.

As in previous phases, during MAG Phases B and C, MA will verify the adequacy of the follow-on RFP and government program planning and readiness for the production decision with respect to requirements analysis and validation.

During MAG Phase D1, the requirements analysis and validation CMP is focused on completing the requirements verification based on the first flight articles while maintaining the requirements set integrity. For ground system and ground support equipment, MAG Phase D1 will consist of the build and test of the associated hardware and software elements. Formal hardware acceptance tests and software formal qualification test will be the principal vehicles to assure verification of requirements are completed. These unit-level tests may be supplemented by lower-level demonstration and tests, which may have greater perception. All planned validation and verification activities should be shown to directly support the program's TEMP. As during the MAG Phase B and C design phases, this production phase will also generate requirement changes and clarifications as production issues are encountered. MA will assure that any resulting requirement change complies with system-level requirements.

Requirements analysis and validation (MAG Phase D2) will focus on validating requirements in a pre-launch system environment. For the space segment, this activity will involve assuring that the space vehicle and support equipment are compatible with the launch site facilities, range, and launch vehicle interface. External interfaces to satellite ground control and mission processing may also be verified in this field environment. For the launch segment, this activity will similarly address launch vehicle internal interfaces, and compatibility with

support equipment and launch site facilities, range, and payload interfaces. For the ground system, the environment for the ground control and mission processing elements will normally involve installation and integration into the actual ground site with follow-on demonstrations of compatibility of external system interfaces. In some instances, this activity will be supplemented with system performance demonstrations in level 1 organic maintenance facilities prior to installation at the ground sites. Preliminary operational assessments by independent test organizations could occur at this time. These higher level demonstrations would feedback to the system validation effort with noted critical discrepancies being addressed prior to launch.

During MAG Phase D3, Aerospace's requirements analysis and validation process will verify flight test and operational performance do indeed fully meet system requirements. System requirements analysis and verification simulation and modeling tools should be updated to reflect flight results. When necessary, adjustments in the system requirements set should be made to reflect the actual delivered system capability.

The last MAG task category (an equivalent of which is actually repeated throughout the various CMPs and SMDs) is not a specific program phase as defined in NSS 03-01, but a bin to capture non-program-specific MA tasks that enable Aerospace to develop and refine organic capabilities to conduct requirements analysis and validation MA activities as needed in any future program. For example, a task to support the development of a standard to be required for future programs could be placed into this bin.

4.6 Organization of Tasks

The basic task structure in requirements analysis and validation as well as in other processes is subdivided into three principal areas that practically repeat themselves in all the MAG phases: program planning, systems engineering, and system segments. The basic organization is shown in Appendix A3.

The program planning tasks are subdivided into tasks which assess current program executability, readiness for associated KDPs and adequacy of follow-on RFP, all considered from a requirements analysis and validation viewpoint.

The systems engineering task subdivision varies by phase, but in general addresses the system requirements set and supporting analyses, system engineering process assessments including verification planning, supporting SMDs, and specialty engineering areas, and the capturing of "lessons learned." The supporting engineering discipline task area identifies links to the seven SMDs identified within the *Mission Assurance Guide* and other specialty engineering areas such as electro-magnetic compatibility, contamination control, survivability, etc.

The third part, system segments, is structured along a typical program hierarchal work breakdown structure (WBS) addressing requirements development, allocations, and validation. Additionally, at the lower level, the feasibility of the implementation of associated concept and technology requirements is addressed. These latter areas are organized by engineering disciplines, e.g., electro-optical, mechanical, electrical, etc.

At the lowest level, very specific MA task examples may be defined. These examples are considered valid MA tasks, but identified as examples as they represent an incomplete set. As the MA verification matrix (MAVM) task database grows, more detailed examples will be added until a complete set is developed and configured. Accordingly, the reference guidance may be expanded and checklists may be provided to govern the execution of certain MA tasks. Thus, the database should be considered a living entity that will mature over time.

4.7 Key Requirements Analysis and Validation Tasks and Associated Objectives

While the complete set of MA tasks given in the database represent the best practices leading to mission success, some specific tasks are deemed more important in achieving mission success. This guide and especially the requirement analysis and validation process emphasize the early phase, for it is this phase that establishes not only the baseline requirements, but the required design and construction standards, parts, material, and process program, and quality control practices to be implemented during the follow-on phases.

During MAG Phase 0, the program acquisition strategy becomes a key area to assure that adequate resource requirements, i.e., schedule and funding, are being identified in the acquisition strategy plan that are

consistent with historical data. If the program does not have sufficient resources at start-up, the outcome will most likely put MA activities and required design and construction standards at risk as attempts are made to live within these resource constraints. An independent MA assessment can serve to identify this shortfall outside of the normal program acquisition office that is pressing for acquisition strategy approval. Also, assuring a sound Phase A RFP with a complete and clearly defined set of technical requirements and best practice-based compliance documents and standards is crucial in achieving both program and mission success. The MA tasks, which focus on these issues, have been identified within the database of Appendix A3.

Similarly in MAG Phase A, requirements analysis again must assure that the updated acquisition strategy has identified sufficient resource requirements consistent with the technical requirements of the program as reflected in the follow-on RFP. This key task together with assuring the Phase A program, as negotiated after contract award, are executable are significant proactive MA assessments made early in the program development. During Phase A execution, MA requirements analysis and validation is also asked to assess relevant system engineering processes such as the requirements change board to verify their adequacy and seamless operation across the program. These tasks can often identify major shortfalls whose programmatic impacts, delays, and cost overruns can be prevented through timely action within the program phase. As identified in the MAVM task database, the set of up-front MA activities is repeated for each MAG phase and provides the independent MA review to establish a solid program baseline needed to enable mission success.

As important as assuring the requirements analysis process is verifying the resulting optimized system requirements and segment requirements allocations. In accomplishing this task, key elements as given in the database are the assurance of the contractor's models and simulations that are used to assert the performance represented by the system requirement set. Often this task involves an independent analysis by Aerospace using different tool sets than those used by the contractor. Differences in results over a wide range of case studies are scrutinized to understand simulation nuances, which may build confidence in the contractor's products.

Lastly, during MAG Phase A, the requirements for each segment and their allocations are assured relative to their completeness in identifying all segment elements and their functional relationship and interfaces.

Additionally, the requirements set is assessed in terms of its characteristics and associated performance, physical characteristics, design and construction, personnel and training, and specialty engineering requirements.

During Phase B, detailed allocations assessments are continued, normally down to each configuration item (CI) at the unit level. Aerospace MA assessments are provided based on verifying that the system requirements have been accurately and completely flowed down to this level. The high use of nondevelopment items (NDIs) and commercial off-the-shelf (COTS) products in ground systems present a unique challenge in assessing the adequacy of these elements in meeting the system requirements. This topic is discussed under the software assurance discipline.

The requirements analysis and validation CMP also assures that each requirement as stated in the various critical item specifications is verifiable. Completion of this task will establish the framework for the subsequent verification planning activity. The database tasks include assessments of system and lower level allocated verification plans to assure that the requirement methodology is consistent with the required fidelity and comprehension for that level of integration. Overall, the assessment should assure a well integrated vertical verification plan where system-level requirements are validated at the highest practical level, but build confidence that that validation will be successful based on lower-level verification results.

Key tasks for the follow-on MAG Phase C are similar to those of MAG Phase B, but more refined as the final design is completed. Emphasis is placed on assuring the requirement control process is functioning properly and that the requirement set integrity relative to meeting system requirements and stakeholder needs. This activity continues through the follow-on MAG phases, i.e., Phases D1, D2, and D3. Similarly, the verification planning and implementation process is also continuously assessed during Phase C and follow-on phases for accuracy and timeliness in reporting its findings. During Phase C, MA would evaluate the sufficiency of the final verification plan, including the correct allocation of verification methods to each requirement. The rationale for substituting a less discernible method than testing (e.g. analysis, demonstration, similarity, etc.) should also be assessed. In addition, the MA assessment should specifically address qualification by similarity approaches by examining in detail the original

qualification program, results, and residual issues, as well as environment and application differences.

4.8 Government and Contractor-enabling Tasks and Products

In order to successfully execute the identified MA tasks identified within the database, enabling government and contractor processes and products is required. A basic MA need common to all MAG phases is access to the government's draft and final RFP, the negotiated contract, the system acquisition management plan, cost analysis and requirements document, program cost estimates, and high-level concept documents such as the ICD, CDD, CONOPS, and TEMP. Contractor MA enabling products that are also common to all MA phases are system and segment system specifications, lower-tier configuration items, system engineering planning documentation such as the system engineering management plan, verification plan, part, material and process (PM&P) management plan, and radiation hardness assurance plan. The execution of MA activities also requires open access to contractors' IPTs and boards, such as the requirement change control board, PM&P control board, EMC control board, and verification planning IPT, in order to assess the adequacy of the associated processes. Additionally, for each MAG phase the requirements analysis and validation MA personnel need to participate in the program initial baseline review and design reviews.

During MAG Phase A, access to contractors' simulation and models often present problems, especially at the subcontractor level. Provision should be made in the RFP to have access to simulation assumptions, simulation and model source code, and detail results for an agreed upon set of case runs. In Phases C and D1, MA personnel would need similar access to the contractors' mission planning tools.

4.9 References

Guidance for the requirements analysis and validation process can be found in the Aerospace report *Systems Engineering Requirements and Products*, TOR-2005(8583)-3. The document describes the overall system engineering process relative to requirements development and verification. A separate Aerospace report, *General Guideline for Space Vehicle (SV) Verification Plan Development and Execution*, TOR-2004(3901)-3242, describes the overall recommended verification planning process to be used by the contractor. In performing the

associated MA activities, the *Space Vehicle Systems Engineering Handbook*, TOR-2005(8506)-4494, which has been recently developed, will be useful in understanding detailed engineering activities associated with requirements development. Finally, the recently published SMC's *Systems Engineering Revitalization of Specification and Standards* is a useful guide in identifying those specifications and standards that represent Aerospace's current understanding of best practices to be applied to NSS and civil programs.

Policy-related

NSS-03-01	National Security Space Acquisition Policy, Guidance for DOD Space System Acquisition Process, Number 03-01, 27 December 2004
SMCI 63-1201	Assurance of Operational Safety, Suitability, & Effectiveness for Space & Missile Systems, 16 January 2004
AFI 99-101	Developmental Test and Evaluation, 01 November 1996
AFI 99-102	Operational Test and Evaluation, 01 July 1998

Specifications and Standards

ANSI/EIA 632	Processes for Engineering a System, 07 January 1999
IEEE STD 1516/2000	IEEE Standard for Modeling and Simulation High Level Architecture – Framework and Rules, 01 September 2000
Aerospace TOR-2006(8506)-4732	*Space System Verification Program and Management Process*, 30 June 2006
Aerospace TOR-2005(8583)-3, Rev. A	*Systems Engineering Requirements and Products*, 29 September 2005

Handbooks

Aerospace TOR-2006(8506)-4494	*Space Vehicle Systems Engineering Handbook*, 31 January 2006
Aerospace TOR-2006(8546)-4591	*Space Vehicle Test and Evaluation Handbook*, 30 June 2006
INCOSE-TP 2003-016-02	Systems Engineering Handbook, Version 2a, 01 June 2004
NAVAIR Guide, 01 May 2003	Naval Air Systems Command Systems Engineering
IPPD	DOD Integrated Product and Processes Development Handbook, August 1989
MIL-HDBK-881	Work Breakdown Structure, 02 January 1998
MIL-STD-499B	Systems Engineering Handbook, 1999
AoA Handbook	A Guide for Performing Analysis Studies: For Analysis of Alternatives or Functional Solution Analyses, July 2004

Best Practices

CMMI Version 1.1	Combines EIA 731, System Engineering Capability Model, and the Software Capability Model (previously independently used for process, development, improvement and assessment)
Aerospace TOR-2002(3105)-1668	*Acquisition Strategy Consideration*, 31 March 2002
Aerospace TOR-2004(3909)-3360	*Systems Engineer's Major Reviews for National Security Space System Programs*, p. 16, 11 May 2004

Deliverables

DI-MGMT-81024	System Engineering Management Plan (SEMP), 27 August 1990
DI-IPSC-81430A	Operational Concept Description (ODC) 10 January 2000
DI-ILSS-81335	Design Review Data Package, 02 April 1993
DI-IPSC-81431A	System/Segment Interface Control Specification, 25 January 1993
DI-IPSC-81434A	Interface Requirements Specification (IRS), 15 December 1999
DI-IPSC-81432A	System/Subsystem Design Description (SSDD), 10 August 2002
DI-CMAN-81248A	Interface Control Document (ICD), 30 September 2000

Other

Critical Process Assessment Tool (CPAT)

Chapter 5
Design Assurance

Mark M. Simpson
Electronics and Power Systems Department
Howard D. Wishner
Navigation Department
Linda J. Vandergriff
Sensor Engineering and Exploitation Department

5.1 Introduction

The **design assurance** process is a set of planning, analysis, and inspection activities performed to assess the sufficiency of the conceptual, preliminary, and detailed design of all three segments (space, launch, and ground) to perform its intended function over all operating conditions and throughout its design life. There are two types of design assurance activities: 1) system design assurance, which addresses the basic system design performance, and 2) mission design assurance, which addresses mission-specific design performance.

While the contractor is responsible for significant design assurance activities, The Aerospace Corporation, in partnership with the government program office team, performs independent design assurance activities. All of these design assurance activities are an integral part of the proven disciplined mission assurance approach employing well-defined system engineering and technical, management, and organizational processes to ensure mission success. The design assurance process explicitly assumes that the architecture, concepts, requirements, requirements allocation, and design specifications have been performed, reviewed, approved, and stabilized. In addition, it is assumed that all contractual provisions have been made to guarantee appropriate contactor participation, and to provide needed data and documentation to perform design assurance activities.

Significant portions of the design assurance tasks occur throughout the design synthesis phase of the program. Design assurance is accomplished through development of government/consultant design assurance management plan; review and monitoring of the contractor-generated design assurance plans and general design requirement specification; performing independent assessment of the various levels

of maturity designs at the contractor's design reviews (e.g., preliminary design review (PDR) and critical design review (CDR)) and targeted design audits. To enable a learning enterprise, design assurance activities also include updating and maintaining the design assurance component of a corporate knowledge base. Because of the importance of limited production runs and the cost factors involved in manufacturing and test, special design assurance activities include ensuring that appropriate design considerations have been given to manufacturing, testing, maintenance, and logistics. These considerations can be easily incorporated by including appropriate technical experts in the design team using a "concurrent engineering design" paradigm.

5.2 Definitions

System design[8] is the process of defining, selecting, and describing solutions to requirements in terms of products and processes. It also is the product of the design activities that describes the solution (conceptual, preliminary, or detailed) of the system, system elements, or system end-items. A detailed design, usually in graphical form, describes the arrangement of parts, how the parts are attached, process features and notes, and details of the end-item to be produced, manufactured, constructed, or acquired traceable to the requirements and standards identified for the system.

Design assurance is the traceable systematic multi-level activity ensuring accurate translation of all requirements/specifications/ standards into a detailed producible, testable, supportable design.

Design synthesis[9] is the translation of requirements, standards, concept of operations, and functions (functional architecture) into solutions (physical architecture) through tradeoffs, technology evaluations, and design optimization.

Mission design analysis provides assurance that the system is capable of delivering the specific space vehicle to its planned orbit with sufficient margin to guarantee mission success.

[8] INCOSE Systems Engineering Handbook, Appendix E, page 288.
[9] Based on INCOSE System Engineering Handbook definition of "synthesis," Appendix E, page 303.

5.3 Objectives

There are six main objectives for design assurance:

- Design-to-requirements compliance. During the design synthesis phase as space, launch, and ground solutions are being developed at the conceptual, preliminary, or detailed level, it is important that requirements and standards are appropriately translated and incorporated. This effort focuses on traceability and compliance of proposed solutions to the requirements baseline and meeting the user's needs.

- Design accuracy and completeness. Space, launch, and ground segment designs are examined for accuracy and completeness to prevent design drawings (or their electronic counterparts, design files), from containing missing, ambiguous, or incorrect parts descriptions or identifiers. Critical design areas are targeted in audits looking for common problems or new technologies. Design assurance is guided in these audits by Aerospace's extensive explicit and tacit knowledge of space systems, including limitations and appropriate uses. Independent analyses are performed to validate dynamic loads and clearances, structural margins, thermal protection, link margins, power margins, and control stability.

- Producibility. During the manufacturing process, design drawings are always open to some manufacturing interpretation and parts can be left off the assembly instruction or installed in an unintended manner. Design assurance ensures that what is produced is a valid interpretation of the design and manufacturing drawings and that this product can be reliably replicated and integrated into the system in a cost-effective manner.

- Testability. Design assurance supports the concept "design-to-test" and the product integration and test processes by ensuring that appropriate design integration and verification is planned and performed and that the design has not been misinterpreted.

- Supportability. Design assurance supports the maintenance and logistics support functions by ensuring that the design, once produced, can be maintained.

- Minimized programmatic risk. Design assurance provides confidence in the design in an incremental fashion early in the engineering and manufacturing cycle to minimize program risk.

5.4 Practices and Tasks

5.4.1 Develop Design Assurance Management Plans

System design and synthesis is an iterative process performed in cooperation with the whole acquisition team, to transfer the customer/user's needs into a cost-effective solution. "Cost effective" implies finding a solution that appropriately balances the solution for a user's needs with an acceptable amount of risk. The contractor needs to define the processes and procedures it will employ to translate the requirements and constraints into a practical architecture. At the same time the government program office team needs to develop a complementary design assurance management plan that defines roles, responsibilities, practices, and tasks to validate and verify the accurate translation of specifications into producible, testable, and maintainable designs.

Mission-unique analysis is performed independently to verify adequate mission planning for all flight conditions and for combinations of dispersed conditions. Mission analysis includes examining system level and integration requirements; confirming all mission-specific payload integration requirements to ensure that baseline reliability is preserved and new requirements have been met; and to ensure that all prior flight and test anomalies have been adequately resolved. Mission analyses include establishing that the flight trajectory environments and mission design are optimized, satisfy flight and safety constraints, and provide adequate RF link, power, propellant, and consumable margins. Dynamic loads are analyzed to verify booster hardware capability and initial capabilities document (ICD) compliance. Guidance, navigation and control (GN&C) performance is analyzed for acceptable injection accuracy and control stability. Particular emphasis is placed on new hardware, software, or unique applications. Other analyses such as separation clearance, aerodynamic, thermodynamic, vibroacoustic, electromagnetic interference/electromagnetic compatibility

(EMI/EMC), and contamination are performed to verify operation within vehicle capabilities and ICD requirements.

The government design assurance plan goes beyond passively identifying the normal design reviews and audits as described in Aerospace TOR-2004(3909)-3360, Rev. 1, *Systems Engineer's Major Reviews for National Security Space System Programs*. It provides an independent roadmap for the government team detailing necessary design assurance activities and their needed rigor. At a fundamental level the government must decide what areas it will be satisfied in reviewing the contractor work and what areas will need to be independently checked through analysis, developmental test, inspections, witnessing, and/or audits.

In general, the plan describes the tasks that the government program office will execute within the resources available. These tasks include (but are not limited to) identifying the number, scope, and entrance/exit criteria for needed formal design reviews and audits, identifying risk areas for additional attention, developing design assurance oversight processes and procedures, evaluating the contractors' relationship with subcontractors and suppliers, identifying required independent performance analysis, assessing the contractors' design processes and corresponding design assurance processes, understanding the contractors' manufacturing, integration and test processes, defining contractor design assurance incentives, developing processes and procedures to handle engineering change proposals and design change notices, and developing design assurance metrics.

When developing the plan, several key issues affecting a contractor's design process should be addressed. Some of the Lessons Learned include:

- **System specification process.** The most common source of development issues results from the incorrect and undisciplined implementation of the system specification hierarchy. When not aggressively managed, schedule pressures can force programs to proceed with implementation before specifications and designs are acceptable. This usually leads to unintended or abandoned requirements that must be fixed later at a greater cost.

- **Failure to follow processes.** In many cases, test anomalies are caused by the contractors' failure to follow their own plans

and procedures for design and manufacturing assurance. This issue is sometimes acerbated by the prime contractor not uniformly enforcing these required program specific processes at the subcontractor and supplier levels. There should be no illusion that merely producing a design assurance plan will prevent the large number of design escapements now being seen. The plan should identify government and contractor gaps, so that the government can plan to best apply its scarce resources strategically and tactically.

- **Design assurance metrics.** It is important to establish design assurance metrics that can discern problems. For example, examining drawing inspection metrics can be used to identify unacceptably fast and therefore superficial drawing checks resulting in downstream errors that must be corrected at a greater cost.

- **Risk management.** Risk management is an integral part of the concurrent engineering process. It can resolve risks in an early phase, thus lowering costs because of the "leverage of time."

- **Government oversight.** The government should describe procedures for reviews and independent checks. Chapter 6 addresses the major reviews and audits. Sample in-process audits are a powerful government tool that should be used more often and the contractors' award fee should be tied to the audit results.

5.4.2 Monitoring of Contractor Design Assurance Plans and Design Process Implementation

The design engineers create design options for configuration items and their relationships within a system. Each design team will have its own processes to ensure that the design meets specified requirements and can be produced in a timely, cost-effective manner. These processes and procedures should be identified in a contractor-developed and delivered design assurance plan(s). In addition, the appropriate metrics to ensure compliance with the contractor's plan should be provided as part of each delivered plan. The principle components of the plan include but are not limited to the following tasks: providing performance and environmental analyses, developing design best practices and processes, producing drawing check plans and

procedures, producing part check plans and procedures, planning the use of concurrent engineering, producing modeling and simulation plans, prescribing the use of mockups, breadboards, and prototypes, and producing developmental test plans. This plan illuminates developmental test results in order to feed them back into the design assurance process.

A design assurance plan goes beyond the normal list of performance and environmental analyses by looking at how to verify every requirement before drawing release. The plan also goes well beyond a requirements verification matrix that calls for inspection, analysis, test, or demonstration. What this plan seeks is to illuminate the "black hole" interval that exists between generation of the requirements and release of the drawing highlighting the design synthesis process to provide the government program office adequate insight and oversight. Thus, when reviewing the contractor design assurance plan, several key issues should be carefully evaluated and vetted.

5.4.3 Accurate Translation of Requirements to Design

The contractor should provide a clear and auditable process of accurately translating requirements into a design. Design choice is based on careful trade studies with rigorous triple checks and well-documented analyses. The process of checking and using heritage designs should be transparent and have clear safeguards to prevent undefined single self-checks. The plan should describe clear roles and a responsibility to ensure that the design is subject to adequate peer review and oversight.

- **Design defect detection**. Proper analysis and inspection is needed to uncover unwanted design defects. Design defects caught before manufacturing represents significant program savings. These defects fall into several categories:
  - Missing, incorrect, or noncompliant parts
  - Manufacturing complexity that renders the design unproducible
  - Noncompliance with specialty and environmental standards
  - Disregard for user needs or true requirements validation with respect to real-world operations
- **Use of commercial off-the-shelf or government off-the-shelf (COTS)/(GOTS) non-developmental items (NDIs).** In today's systems, significant savings can be realized with the

use of off-the-shelf solutions or components. Use of COTS and GOTS and NDIs should be evaluated for applicability for space systems utilization against the new development as a cost-effective (or cost risk) means to implement a design solution. Special attention should be paid to a qualification by similarity approach to assure that the end item is still being produced in the same facility with identical processes and that the test environments and operating conditions do indeed fall within its intended use.

- **Engineering specialty sign-off.** All requirements must be examined for compliance. This requires the assistance of all the subsystem and specialty engineering disciplines. Specialty engineering checks every requirement on every drawing and signs off according to training and documented procedures, preventing unfocused and undefined checks that could result in a high testing failure rate. Management should also double-check that every requirement is being met on every drawing.

5.4.4 Implement Government Program Office Design Assurance Management

- **Perform Independent System Engineering Design Evaluations**

  Perform independent assessments of key design choices with respect to cost, risk, schedule, and system performance. Build consensus on the top-level requirements and interfaces between the contractor, the government program office, and the users.

- **Perform Independent Space System Engineering Support Tasks**

  Perform multi-disciplinary analysis, special studies, technology assessments, decision support, and special integration and test activities outlined in the government program office mission assurance plan. In addition, ensure space system technologies research and development is performed.

- **Participate in Contractor Design Reviews**

  Design assurance includes the independent assessment of the maturity level of various designs, issues and resolution plans at formal design reviews (e.g., system design review (SDR), PDR, CDR). It is prudent to use independent assessment of designs starting early in the design synthesis process. It is important to

select meaningful reviews for the given program and schedule them based on design maturity criteria, not just the calendar. Major reviews should serve as gates before proceeding to the next step of the program. As a result of design-related reviews, action items, risks, issues, and needed additional focused reviews, audits and technical interchange meetings (TIMs) are identified for follow-up.

- **Conduct Independent Assessment Design Audits**

  Targeted independent assessment audits at different levels of design maturity are performed, with issue identification and resolution plans being generated to bring the design back into agreement with the requirements. However, it should not be expected that these audits will ensure "quality," since quality must be "designed in" from the outset. Planned and/or short-notice audits of the design and contractor compliance with contract-defined design processes should be used. Short-notice audits are a critical tool to insure contractor compliance. Because the contractors are supposed to be following their own design assurance plan, their design assurance process compliance should always be ready to be audited. See also Chapter 6.

- **Perform Independent Performance and Environmental Analysis**

  In developing new space systems, the drive to maximize performance pushes designs to adopt new technologies and innovative solutions. Thus, significant unknowns and risks to mission success can be introduced if issues are not properly identified, documented, analyzed, and mitigated. Contractors sometimes are overly optimistic in their projection of the performance of proposed design solutions or given parts capabilities. During audits of the designs, significant issues can be identified that must be analyzed, including mass properties, power, thermal dissipation, propellant usage, data throughput rates, memory, and other resource limitations. These design solutions must be properly analyzed and managed over the evolution of the design/manufacturing period to ensure mission success.

  Design assurance also requires analytical determination of design responses to normal and abnormal service conditions occurring during factory test, ground handling and transportation, launch processing, launch, and on-orbit operations. In addition, design

constraints such as sizing, weight, and interfacing systems place inherent limitations on design solutions. A typical analysis can range from the impact of the operating environment on new technology/equipment to launch operations impacts (e.g. weight, forces, size) to technology trades and evaluation to performance assessment.

- **Ensure Design Producibility**

  Design assurance has a responsibility to make sure the design was not compromised by misinterpretation or error during the manufacturing process. Early interaction with manufacturing engineering can identify long-lead-time items, material source limitations, availability of materials and manufacturing resources, and special production processes.

- **Perform Design Support to Integration and Test**

  Designs can be compromised by inaccurate translation of design details, misinterpretation, or error during the integration and test phases. Traditionally, ill-defined processes and lack of contractor and government resources fail to catch these errors. However, when using concurrent engineering effectively, opportunities for improved communication and reduced cost testing and integration can be realized. Multidisciplinary teams participating in concurrent design activities simplify the design, build in appropriate test functionality, identify early test items and needed test beds or test equipment, long lead test items for joint or integrated tests, and capture needed documentation. In this fashion, design can include appropriate diagnostics to unambiguously detect and isolate mission, safety, and maintenance faults known or expected to occur when the system is operational; for example, embedded testability, built-in test (BIT), and automatic and manual testing.

- **Perform Design Support to Logistics**

  It is important to adequately address maintenance considerations while design solutions are being considered. This is especially true of software design where long-term maintenance costs can far exceed the cost of the initial design phase. Trades against different solutions need to consider how handling and support equipment, test and checkout equipment, logistics support, sparing, facilities, and the maintenance operations concept will be accommodated by

the various designs. This also includes verifying that support equipment meets reliability and mean-time-to-repair (MTTR) requirements including launch-on-time considerations.

- **Create, Maintain, and Use a Design Assurance Knowledge Base**

  One of the major contributions of Aerospace is its well-developed explicit and tacit knowledge base of past systems performance; current technologies and trends; and the potential concerns for future government acquisitions. Design assurance should actively make use of this knowledge base and augment it by creating, updating, and maintaining Lessons Learned for each program throughout its life cycle. However, this goes beyond the mere listing of Lessons Learned and includes the development of clear processes and procedures and training to ensure knowledge is maintained and used for future programs.

5.5 Strategies and Execution by Phase

As described under the operational readiness assurance process, the design assurance mission assurance (MA) process is organized by Mission Assurance Guide (MAG) phases as shown in Appendix A3. The process is active during all program phases with peak activity in the system design and detailed design phases associated with MAG Phases A, B, and C. As in the other processes, the Phase 0 activity addresses the Phase A request for proposal (RFP), but with a sole focus on its adequacy relative to design assurance. Specific areas addressed are the system design standards, design processes, and design products being required by the RFP. The design products are assured to include those items needed to support Aerospace's design assurance process, along with provisions for Aerospace's access to those products and where needed, access to the contractor's design teams. During Phase 0, Aerospace and other FFRDCs or SETAs may be asked to develop alternate system designs, conduct design implementation trade studies, and provide detailed "sizing" of selected design concepts. MA activities as indicated in the database tasks of Appendix A3 would then independently assess the accuracy, completeness, and associated system performance of these design studies and trades. From a MA prospective, these studies are significant as they establish the overall program funding profile, schedule, and feasibility that the program will be held accountable to in the later phases. If this baseline does not provide sufficient resources, often shortcuts are taken which can jeopardize mission success.

There is some overlap in these system concept studies between the design assurance and operational readiness assurance processes, for both of these processes examine the resultant concepts. However, the latter process would emphasize the concept relative to its consistency with the initial concept capabilities while design assurance would emphasize the design implementation.

At the start of Phase A, design assurance would examine program plans to assure that the design assurance standards and processes that are invoked reflect best practices. This is an important step, as due to regulatory privacy restriction, the independent Aerospace MA management oversight is normally not in place during Source Selection Board activities. However, the negotiated contract is available after source selection is completed and would form the basis of this assessment. Given an acceptable contract baseline, the design assurance process (as shown in the detailed tasks in Appendix A3) would examine program execution plans in terms of the allocated resources during the integrated baseline review (IBR). Some smaller programs may skip this formal review process, but it is nevertheless important to gain this insight into allocated resources in both prime and major subcontractors' program planning as early as possible to identify MA risks in downstream design activities.

During the conduct of Phase A, the design assurance process would continue as the system design is refined. Its overall objective is to assure the feasibility, completeness, and accuracy of alternate design concepts and trades leading to the selection of an optimized system design. For technology push programs (i.e., those programs not driven by a specific mission need), the design assurance MA objective would be to assure that the selected technology demonstration adequately addresses the required technology scale and appropriate measures of performance. Phase A also establishes the detailed design processes, standards, and guidelines to be applied in subsequent phases.

Design assurance tasks are identified in Appendix A3 under the general heading of system engineering processes and products. These processes, standards, and guidelines are documented in the contractor's plans, including those plans developed for specialty engineering areas. The proposed design tools and design databases are evaluated for adequacy. Additionally, both the contractor's and government program office's internal design assurance plans are assessed in terms of their adequacy and completeness. Toward the end of Phase A, in support of the SDR, design assurance addresses segment and subsystem design

concepts in terms of their design feasibility, technology readiness, design risks, and associated design attributes such as supportability, producibility, and testability. As in other processes, the MA design assurance tasks closely assess the follow-on RFP for the subsequent program phases for adequacy, focusing again on the compliance design and construction standards being invoked and ensuring that the enabling design assurance products are being produced.

In Phases B and C, the design assurance MA tasks address the accuracy and completeness of the preliminary and final designs relative to meeting their system and allocated and derived requirements at the system, lower-level segment, subsystem, and unit level. They would also assure the completeness and accuracy of subsystem and unit-level design trade studies leading to the selected design. These phases are the most active periods for the design assurance process as the engineering disciplines are normally fully engaged with the prime and subcontractors teams. As breadboards, brass-boards, and flight-like prototypes are built, MA would assess the associated demonstration and test results to verify that they not only meet requirements, but are consistent with design analyses. Higher-level mockups would also be used to develop detailed design criteria and help support design analyses and required models, such as a space vehicle dynamics and thermal math model. Software prototypes may be used to provide early assurance that the proposed design will meet performance criteria. As depicted in the task descriptions, the MA team will scrutinize these products in order to verify not only the contractor's design analyses, but support independent Aerospace analyses. Assuming adequate Aerospace program funding levels, independent design analyses are often performed by Aerospace's MA assurance team in order to verify the contractors' designs in what is considered complex and high or moderate risk areas.

In addition to assessing the design products, the MA activities also audit related design processes and assess related design metrics as well as verify the contractor's internal design assurance reviews are being conducted in accordance with the approved plan. At the system, segment, and lower level of equipment hierarchy, MA would assess the adequacy of deign margins and robustness and check the design for compliance to industry standards, Aerospace's best practices, and for applicable Lessons Learned databases for similar developments.

Where COTS/NDI and heritage hardware and software items are being used, MA (as identified in specific task descriptions in Appendix A3)

will perform detailed evaluation of this equipment's ability to satisfy the unique program performance, quality, and environmental requirements. Additionally, if the Phase C activity includes unit-level qualification, MA will again verify that the associated results are consistent with design analyses and predictions.

As with Phase A, Phases B and C of the design assurance effort would assess the negotiated contract resulting from the source selection, assess program preparation to assure executability, and verify any follow-on RFP relative to design assurance.

During Phase D1, production and qualification program, demonstration and test results will be similarly used to verify the design meets requirements as well as assure consistency with design analyses and predictions. Tested and qualified items are assured to have been subjected to the proper environmental design conditions. This process will be reiterated as the unit under test evolves from the unit level to subsystem to vehicle level or end item level. MA will also assure that design errors encountered in this phase and follow-on phases are fully resolved and that the correction action not only includes an adequate design change, but the design process is matured such that these types of design errors will not occur again. Phase D1 will also focus on the general mission design, assuring that all constraints are met over the mission envelope, while Phase D2 will focus on the mission-specific design for which Aerospace will normally perform an independent mission design verification. Mission-specific targeting and selected database parameters are verified to meet design requirements. Additional design verification activities that have been deferred until the segment or vehicle is further integrated in the field with other segment elements or other systems in Phase D2 are also addressed by design assurance. Finally, in Phase D3, O&M design assurance tasks will focus on the flight software and ground system software and hardware upgrades and bug fixes.

5.6 Organization of Tasks

As shown in the task outline in Appendix A3, the design assurance tasks are organized by MAG phases. An additional phase called Non-Program Specific (NPS) has been created to capture those MA activities that build general capabilities within Aerospace to perform design assurance type work. An example under design assurance would be the development of unique structure tools to establish composite structure failure criteria. Within the other MAG phases, the

MA design assurance tasks are organized under three groups: program execution, system engineering processes and products, and design verification. As in the other processes, program execution MA tasks are subdivided into an executability review of the current program phase and the assessment of the follow-on RFP. System engineering tasks are subdivided into the system design and system design verification assessments, and supporting specialty engineering design-related tasks. The last group, design verification, addresses the detailed design and is organized by system segment, vehicle and ground support equipment, vehicle elements, and subsystems. The subsystem level is aligned to the engineering disciplines that are found within Aerospace's Engineering and Technology Group, which has supplied the bulk of the detailed MA tasks. The ground segment design assurance tasks in this last group are further grouped into telemetry, tracking and command (TT&C), mission management, mission processing, and other elements. Each element is then subdivided into hardware and software configuration items.

Each identified task list the author, task title, associated engineering discipline, task title, and a short description. Also identified are related policy and guidance for executing that task, and the desired MA product as a result of performing that task, together with a risk and benefit statement and identification of the enabling products or tasks required to support Aerospace's effort. As the database matures, it is planned that these task descriptions will be expanded with the use of checklists and further guidance as to the execution of tasks. It is the intent to eventually hyperlink each task to specific paragraphs within the guide and to use checklists where practical to further identify the items that must be considered in the associated assessment. Requests for clarification or suggested changes to the task statement should be sent to the identified author.

5.7 Key Tasks and Associated Objectives

As discussed earlier, the basic objectives of design assurance are to assure that the synthesized design at all levels complies with all performance, design, and construction requirements, and is accurate and complete in its description while offering a producible, testable, and supportable design. These objectives directly support mission success and are considered among the most important MA processes, for recent studies have shown that nearly one-half of the failures encountered during the first year of operations are attributable to design error. In achieving these MA objectives, the design assurance process

assesses design planning and guidance, and associated processes. Design assurance also performs independent analysis and review activities to assess the sufficiency of the conceptual, preliminary, and detailed final design of all three segments (space, launch, and ground) at all levels of design, i.e., from the system architectural design down to the detailed design of subassemblies. Sufficiency is viewed as the ability of a design element to perform its intended function over all operating conditions and throughout its mission life. An additional objective is to assure that the design displays sufficient robustness to accommodate expected growth in requirements or changing requirements as the mission needs evolves. Common examples of this required robustness is the ability of the power and thermal subsystems to accommodate growth in requirements as the other subsystems they support mature through the design process. Robustness is also desired with regard to ability to operate through unexpected conditions that may be encountered. This capability is difficult to define as these conditions are unknown.

A key task common to all phases is the assurance that the contractual compliance set of standards and specifications and design guidelines reflect the current best practices of the industry and Aerospace. A review of the compliance documents identified in the final RFP and negotiated contract provide the mechanism to accomplish this task. A follow-up task to review the prime contractor's design management plan to assure that these compliance documents are being invoked is recommended. This review should also include a detailed review of the contractor's internal standards, where the contractor has claimed equivalence to compliance standards imposed in the contract. Additionally, tasks are identified to verify the design processes are being executed in accordance to these standards within the prime and subcontractors design teams. Design verification tests (as distinct from requirements verification) are also a key element of design assurance, which are executed through the program phases. In the detailed tasks descriptions, there are numerous references to assuring early and comprehensive design-related tests to not only verify the design concepts, but to acquire the necessary design information to complete the design. Verifying that the "up-front" design assurance planning is adequate has the greatest potential for assuring mission success for the least amount of Aerospace effort.

During Phases 0 and A, focus is placed on assuring the system design and assuring that the aforementioned planning is in place. Typically independent Aerospace design analyses and simulations are conducted

to assure the system architect, design, and interfaces will meet the selected requirement set. These tasks are often extended to the design concept trade-off studies. A common tool used at Aerospace is the Concept Design Center (CDC), where Aerospace conducts computer-aided design (CAD) studies and analyses to optimize the design concept, to provide design recommendations, and to identify non-feasible conceptual design options. These design studies will also assure that the enabling technologies have been identified together with the required readiness level and roadmap for growth to the required level. Aerospace should independently assess the technology roadmap feasibility to assure that program is not based on unwarranted assumptions as to the success of the associated demonstrations. Similarly, tasks have been identified to assess Phase A technology demonstrations relative to the achieved readiness level, required technology scale, and performance.

In verifying the system design, Aerospace should also independently verify that the design is fully supportable across its life cycle. This is especially true in the ground system, where Aerospace should assure the equipment/software obsolescence and planned upgrades have been adequately considered. As outlined in the task database, emphasis is placed on assuring that NDI, reuse code, and COTS/GOTS products are fully supportable.

As the system design is promoted to the detailed design phase, a key task early in Phase B is to assure that planned equipment "qualification by similarity" is appropriate. Aerospace should conduct an independent and thorough review of the original qualification test report, along with an evaluation of its new application and operating environment. Additionally, Aerospace should assure that the same manufacturing facilities and processes will be used in manufacturing the follow-on units before concluding that a requalification need not be done. During the detailed design effort of both Phases B and C, a key MA task is to monitor the design process, assuring that the steps outlined in the design guidance are being followed using validated design databases and part application notes. Design documentation should be assessed against a drawing checklist and have the appropriate signoff from the supporting specialty engineering areas. These lists are helpful in assuring the completeness of the design documentation. If possible, design error metrics should be collected and treaded. Also, outlined in the MA task database are numerous reviews and independent design analyses at the subsystem level to assess the design adequacy in meeting the allocated requirements. In these task

statements, references are made to other engineering checklists, in which the specific design can be further evaluated against. Prototype demonstrations may be conducted in the detailed design phase, when test results are used verify the design.

During the Phase D1 manufacturing, the first production "as built" items are similarly reviewed to assure they reflect the "as designed" baseline and that the manufacturing results are consistent with design analyses. The mission design tools should be available during these later phases. A key associated Aerospace MA task would be to verify that this tool can satisfy all the mission constraints while fully meeting mission objectives. As the first flight articles are integrated and sent to the field in Phase D2, a key task would then be to assure that higher-level integration and system demonstration results are consistent with previous design analyses. Additionally, Aerospace would assure that flight test results are used to refine simulations and models and project system and subsystem performance across the mission envelope. As final flight preparations are made, a key Aerospace task would verify the final flight trajectory and dispersion while assuring that adequate propellant margins exist and that the ground system and flight software designs are compatible with the changes to the space vehicle.

5.8 Key Government and Contractor Enabling Processes and Products

As identified in the MA task data, each task is dependent on receiving specific products or access to specific processes from the contractor and government program office. In addition, to requiring access to the government's draft and final RFP, and the negotiated contract, the design assurance MA team needs access to the contractor's design policy and guidance documentation across the prime and subcontractors. The MA task team will also need unfettered access to the contractors' design teams at all levels of the program through the active design period.

Design review data packages that are associated with SDR, PDR, and CDR are important vehicles in providing the needed information. The RFP should require submission of these items with sufficient depth and at least 30 days prior to the review to permit an adequate independent review. The data package should be supplemented with specifications, part application notes, drawings and timing, and logic diagrams of sufficient detail to enable independent Aerospace evaluation. With the advent of CAD, many of the products can be submitted as CAD files,

but provisions must be made to assure that industry standard tools are used to assure compatibility with Aerospace resources.

To support an independent loads analysis, Aerospace would require delivery of the contractor's finite element model, model survey test results, launch vehicle forcing functions, and contractor computed loads.

5.9 References

As identified in Chapter 1 References, there are specific reference to handbooks, standards and Aerospace Technical Operation Reports that provide detailed guidance in executing the associated task. A good overview of the design review areas can be found in MIL-STD-1521C (draft), TOR-2006(8506)-4494, the *Space Vehicle System Engineering Handbook*, and TOR-2005(8583)-3, *Systems Engineering Requirements and Products*. These documents not only delineate the areas to be reviewed, but give checklists or attributes to consider in evaluating the design-related products. For specific engineering discipline areas, references are made to other government MIL-STDs or industry standards under the auspices of IEEE, AIAA, and ASTM standards' groups.

These top-level compliance documents are generally included as part of an initial program contract agreement. The documents listed below represent those documents or their equivalent tailored versions that are applicable to SV design assurance are:

Policy-related

NSS-03-01	National Security Space Acquisition Policy, Guidance for DOD Space System Acquisition Process, Number 03-01, 27 December 2004
SMCI 63-1201	Assurance of Operational Safety, Suitability, & Effectiveness for Space & Missile Systems, 16 January 2004
AFI 99-101	Developmental Test and Evaluation, 01 November 1996

AFI 99-102	Operational Test and Evaluation, 01 July 1998

Specifications and Standards

ANSI/EIA 632	Processes for Engineering a System, 07 January 1999
IEEE STD 1516/2000	IEEE Standard for Modeling and Simulation High Level Architecture – Framework and Rules, 01 September 2000
Aerospace TOR-2006 (8506)-4732	*Space System Verification Program and Management Process*, 30 June 2006
Aerospace TOR-2005(8583)-3, Rev. A	*Systems Engineering Requirements and Products*, 29 September 2005
Aerospace TOR-2005 2005(8583)-1	*Electromagnetic Compatibility Requirements for Space Equipment Systems*, M. Dunbar, 08 August 2005
MIL-STD-810F Notice 3	Environmental Engineering Considerations and Laboratory Tests, 05 May 2003
MIL-STD-461E	Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, 20 August 1999
MIL-STD-1542B	Electromagnetic Compatibility and Grounding Requirements for Space System Facilities, 15 November 1991
MIL-STD-1543B	Reliability Program Requirements for Space and Launch Vehicles, 25 October 1988

MIL-HDBK-217F	Reliability for Electronic Equipment
EIA/IEEE J-STD-	Software Development Specification, Program-unique Documents 016 3.2
AFSPCMAN 91-710	Range Safety User Requirements Manual, Volumes 1–7, (Replaces EWRR 127-1), 01 July 2004
SMC-TR-04-17	*Test Requirements for Launch, Upper-Stage, & Space Vehicles*, 31 January 2004 (replaces MIL-STD-1540C). See also Aerospace TOR-2004(8583)-1, *Moving Mechanical Assemblies Standard for Space and Launch Vehicles (Draft 1)*
Aerospace TOR-2004(8583)-3275	*Survivability Program Management for Space Systems*, 31 March 2005
AIAA S-111 2005	Qualification and Quality Requirements for Space Qualified Solar Cells, 01 May 2005
AIAA S-112 2005	Qualification and Quality Requirements for Space Qualified Solar Panels (draft), 01 May 2005
Aerospace TOR-2005(8583)-2	*Electrical Power Systems, Direct Current, Space Vehicle Design Requirements*, 11 May 2005
Aerospace TOR-2004(8583)-5 Rev. 1	*Space Battery Standard*, 11 May 2005
ASTM E1548-04	Standard Practices for Preparation of Aerospace Contamination Control Plans, Tailoring and Background, 12 September 2004

Aerospace TOR-2005(8583)-3970	*Mass Properties Control Standard for Space Vehicles*, 20 July 2005
AIAA S-114-2005	Moving Mechanical Assemblies Standard for Space and Launch Vehicles (replaces MIL-A-83577C), 30 June 2005
AIAA S-080-1998	Space Systems, Metallic Pressure Vessels, Pressurized Structures, and Pressure Components, 01 September 1998
AIAA S-081-2000	Space Systems – Composite Overwrapped Pressure Vessels (COPVs), 01 December 2000
Aerospace TOR-2003(8583)-2896	*Space Systems – Flight Pressurized Systems* (replaces MIL-STD-1522A), 31 August 2003
Aerospace TOR-2003(8583)-2895 Rev. 1	*Solid Rocket Motor Case Design and Test Requirements*, 22 December 2004
AIAA S-113-2005	Criteria for Explosive Subsystems and Devices Used on Space and Launch Vehicles, 30 June 2005
Aerospace TOR-2003(8583)-2894	*Space Systems – Structures Design and Test Requirements*, 02 August 2004
MIL-STD-1833	Test Requirements for Ground Equipment and Associated Computer Software Supporting Space Vehicles, 13 November 1989
DOD-W-83755A Rev. A Notice 1	Wiring Harness Space Vehicle Design and Testing, 04 September 1992

COE UIS	Common Operating Environment (COE) User Interface Specification (UIS), Version 4.3, (CM Reference: 59314), December 2003
MIL-STD-1367A	Packaging, Handling, Storage, and Transportability Program Requirements for Systems and Equipments, 02 October 1989
MIL-STD-470B	Maintainability Program for Systems and Equipment, 30 May 1989
Aerospace TOR-2004(3909)-3315 Rev. A	*Parts, Materials, and Process Control Program for Space Vehicles*, 12 August 2004 (replaces MIL-STD-1546)
Aerospace TOR-2004(3909)-3316 Rev. A	*Technical Requirements for Electronic Parts, Materials, and Processes Used in Space Vehicles*, 12 August 2004 (replaces MIL-STD-1547)
Aerospace TOR-98(1412)-1 Rev. A	*Parts, Materials, and Process Control Program for Expendable Launch Vehicles-Revision A*, 01 January 2004
Aerospace TOR-2004(3909)-3537 Rev. B	*Software Development Standard for Space Systems*, 11 March 2005
ISO/IES STD 15939	Software Engineering – Software Measurement Process, 11 July 2002
Aerospace TOR-2004(3909)-3405	*Metrics-Based Software Acquisition Management*, 05 May 2004
IEEE 1471	IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, 21 September 2000

Technical Handbooks

Aerospace TOR-2006(8506)-4494	*Space Vehicle Systems Engineering Handbook*, 31 January 2006
Aerospace TOR-2006(8546)-4591	*Space Vehicle Test and Evaluation Handbook*, 30 June 2006
ISBN 1-884989-11X	Spacecraft Thermal Control Handbook, Volume 1
ISBN 1-88-4989	Spacecraft Thermal Control Handbook, Volume 2, Cryogenics 14-4 (v.2)
ISBN 1-884989-15-2	Space Modeling and Simulation Roles and Applications Throughout the System Life Cycle
MIL-HDBK-5J	Metallic Materials and Elements for Aerospace Vehicle Structures
MIL-HDBK-17-2F	Composite Materials Handbook
MIL-HDBK-83575	General Handbook for Space Vehicle Wiring Harness Design and Testing
MIL-HDBK-241B	Design Guidance for EMI Reduction in Power Supplies
Aerospace TOR-2006(3904)-1	*Digital ASIC/PLD Development Handbook for Space Systems*, 30 November 2005

Best Practices

Aerospace TOR-2005 (8583)-4474	*Requirements for End-of-Life Disposal of Satellites Operating at Geosynchronous Altitude*
SMC-TR-98-35	*Tribology in the Space Environment*, 15 October 1997

Deliverables

DI-EMCS-80199B	Electromagnetic Interference Control 20 August 1999
DI-EMCS-80201B	Electromagnetic Interference Test Procedures, 20 August 1999
DI-IPSC-81430A	Operational Concept Description (OCD), 10 January 2000
DI-ILSS-81335	Design Review Data Package, 02 April 1993
DI-IPSC-81431A	System/Segment Interface Control Specification, 25 January 1993
DI-IPSC-81434A	Interface Requirements Specification (IRS), 15 December 1999
DI-IPSC-81432A	System/Subsystem Design Description (SSDD), 10 August 2002
DI-CMAN-81248A	Interface Control Document (ICD), 30 September 2000

Other

Critical Process Assessment Tool (CPAT),

Capturing Design and Manufacturing Knowledge Early Improves Acquisition Outcomes," GAO-02-701, July 2002

Chapter 6
Manufacturing Assurance

Steven R. Robertson
Parts, Materials and Processes Department
A.L. McClellan
Parts, Materials and Processes Department
Dan W. Hanifen
Baseline Systems/Payload

6.1 Introduction

The actual production of the finished item is where the "rubber meets the road." For the purposes here, hardware manufacturing is the focus of this chapter. It is recognized that in today's digital world, software and hardware are inexorably linked. However, this chapter will address hardware **manufacturing assurance**. Manufacturing engineering translates design documentation using available and certified materials, parts, and manufacturing processes to create products that meet user expectations and fulfill stated requirements. As one would expect, the manufacturing process is very complex and susceptible to errors introduced from many sources such as incorrect design information, material defects, tolerance errors, and calibration errors. Prudent and successful manufacturing processes use a system of checks (i.e., tests, inspections, and analysis) to validate that, at each stage of the manufacturing sequence, the end product is acceptable according to quality standards set for that stage in the sequence.

Beginning early in the concept development phase of a program, each developer examines the user needs, requirements (if adequately mature), existing construction, and test standards or specifications, and assesses existing manufacturing processes needed to implement potential solutions consistent with the mission's reliability, performance, and durability. Additionally, each developer identifies and assesses new and emerging manufacturing technologies to be considered for development and insertion, and assesses the environmental impact of manufacturing processes. All manufacturing processes are documented to include all aspects of manufacturing engineering; manufacturing methods; production and material control; minimization of scrap, rework and repair considerations; and requirements for facilities, materials, tooling, test equipment, equipment, personnel, training, government-furnished property, and

software (required to support the manufacturing process, not the final product).

To be successful and produce high-quality repeatable products, manufacturing practices and tasks require close teamwork and coordination between the systems engineering, design engineering, parts, materials and processes (PM&P) engineering, manufacturing engineering, test engineering, reliability engineering, safety engineering, quality assurance, and configuration management. This interaction occurs throughout the manufacturing process (starting before production begins) with producibility assessments to gain confidence that the manufacturing processes will provide needed items at the required performance, reliability, quality, and durability.

6.2 Definitions

Manufacturing[10] is the conversion of raw materials into products or components through a series of processes. It includes such major functions as manufacturing planning, tool design, scheduling, manufacturing engineering, material procurement, fabrication, assembly, test, packaging, installation and checkout, product assurance, and determination of resource requirements throughout systems acquisition.

Manufacturing engineering[11] is the specialty of professional engineering that requires such education and experience as is necessary to understand and apply engineering procedures in manufacturing processes and methods of production of industrial commodities and products. It requires the ability to plan the practices of manufacturing; to research and develop tools, processes, machines, and equipment; and to integrate the facilities and systems for producing quality products with optimal expenditure.

Producibility is a design accomplishment that enables manufacturing to repeatably fabricate hardware that satisfies both functional and physical objectives at an optimal cost. Producibility results from a coordinated effort by systems/design engineering and manufacturing/industrial engineering to create functional hardware designs that optimize the ease and economy of fabrication, assembly,

[10] MIL-STD-1528A, Manufacturing Management Program, para 3.4, 09 September 1986 (cancelled MIL-STD).
[11] IBID, para. 3.5.

inspection, test, and acceptance of hardware without sacrificing desired function, performance, or quality.

6.3 Objectives

The objectives for manufacturing assurance are two-fold. The first objective is to ensure that the manufacturing processes can produce the items and that they meet the specified requirements and design. The second objective is to accurately translate the design into a reliable, durable, manufactured item using manufacturing processes that are highly repeatable and error free.

6.4 Practices and Tasks

Manufacturing planning should be started early in the concept development phase of the program and produce a manufacturing management plan (MMP). The MMP has a broad scope and includes planning for make or buy decisions, tooling, special test equipment, receiving inspections, production yield thresholds, producibility studies, inspection requirements, fabrication plans, critical and strategic materials, production facility loading and capacity, sparing philosophy, machine loading, capital investment, subcontractor or vendor delivery schedules, and training. Additionally, early planning efforts should establish manufacturing process management metrics such as monthly manufacturing and production trends, manufacturing and testing yield rates, touch labor hours, hours for scrap, rework and repair, and out-of-station work.[12] As part of manufacturing source selection, vendor evaluation for capabilities should be included. Alternate suppliers should be developed or identified.

Manufacturing process mapping should be accomplished before production begins, to understand how work flows to assemble the item to be manufactured (e.g., flight components, assembly, subsystems, and system). A process map can help management determine the best method to complete work, identify areas that need improvement, identify resources needed in the key elements of manufacturing, define inspection points, and help identify critical processes. Considering production quantities and rate, process mapping provides insight into the amount of time required to compete each manufacturing task and sequence of tasks and thus provides input to program schedules.

[12] MIL-STD-1528A, para. 5.1.2, page 7.

Producibility assessments provide a producibility analysis and production feasibility early in the conceptual design process. A producibility analysis compares alternative materials, processes, and manufacturing methods to determine the most cost-effective method within the constraints of cost and schedule. Production feasibility determines the likelihood that the article can be produced with the given manufacturing technology, factory infrastructure, cost/schedule constraints, and likely competition with other programs for resources, such as floor space, test equipment, and personnel.

Evaluation of new manufacturing processes and/or facilities is particularly critical because NSS systems typically push the state-of-the-art and therefore manufacturing processes (and supporting infrastructure) continually evolve to meet the needs of NSS customers. New processes and facilities must be requalified to manufacture critical hardware. Producibility and manufacturing considerations include materials, tooling, test equipment, processes, facilities, skills, and in-process and receiving inspections, human engineering, subcontractor or vendor control, standardization requirements, safety requirements, corrosion and contamination, biomedical concerns, interface units, commercially available equipment, support equipment requirements, manufacturing and test software, considerations of process yield, process stability, and the impact of process variability on product quality.

Qualification of the manufacturing processes[13] provides confidence that new designs introduced to a contractor, subcontractor, or vendor's manufacturing process(es) can be accommodated without causing adverse impacts (i.e., introduce defects, schedule slips, rework, or cost increases). As such, consideration is given to the adequacy of manufacturing planning, tool design, manufacturing flow, assembly flow, long lead items, and personnel qualifications and training. Hardware and other resources (e.g., mockups) are allocated as "proof of design" and as "proof of manufacturing" for implementation prove-out and production equipment troubleshooting.

Manufacturing process monitoring/control is required to ensure that the launch or space vehicle hardware does not vary from appropriate qualified units. The criticality of space missions requires that manufacturers impose strict controls on each item. Contractor

[13] DOD 4245.7-M, "Transition from Development to Production," September 1985, pages 5-6.

processes for executing engineering changes should be carefully assessed to control the quality and pace of change and its impact on the manufacturing processes and end products. Items as seemingly insignificant as a threaded fastener must be verified to meet such design requirements as material properties, composition, dimensions, and installation requirements (e.g., lubrication, torque, etc.). This requires the use of in-process reviews, audits, and assessments of manufacturing process quality to detect and correct defects introduced during the manufacturing process. At each checkpoint, manufacturing records are examined and compared to design drawings to assure that the as-manufactured product is identical to the current design configuration; physical inspections are conducted (quality conformance), and item characteristics are compared to physical or functional models or other selection criteria established to judge design conformance. Item performance is also characterized as needed, failure analysis is conducted, and any discrepancies are recorded.

Periodic analyses are conducted of manufacturing methods, processes, techniques, equipment, and materials planned for use in production. State-of-the-art advances in manufacturing technology are reviewed to encourage the use of the latest and most efficient manufacturing technology.

Tools and methods to monitor the manufacturing process are selected and used. Inspection and test yields and hardware throughputs are monitored continuously and compared to predetermined thresholds. Periodic calibration of all measurement and sensor tools is performed to maintain the fidelity of manufacturing processes to avoid introducing errors in the unit qualification process.

- **Establish and maintain a production scheduling and control system** to plan all production activities including the identification of key production milestones, tracking production schedules for components and assemblies, tracking engineering change management for insertion into production, and analyzing lead-time for government and contractor furnish property.

- **Periodically review critical items, forms, and risk management** to ensure that all items that require a pedigree review are included, and to recommend changes if warranted. NSS systems require that special precautions be taken because item failures could seriously affect system operation or cause

the system to fail to achieve mission objectives (e.g., single-point failure or SPF) as there are items that have very stringent performance requirements relative to the state-of-the-art; therefore, state-of-the-art manufacturing techniques are required to produce those items.

- **Verify tolerances** are correct and use mock ups to check the fit of critical interfaces.

- **Assure that all participants (e.g. design, manufacturing, quality, PM&P engineering) participate in the design process early** so that all drawings, specifications, etc., are reviewed by all relevant disciplines. This helps prevent designers from selecting parts, materials, or designs that are difficult to qualify or integrate in the next level of assembly or difficult to manufacture.

- **Implement rigorous subcontractor and supplier management** to ensure that the system requirements have been successfully allocated and flowed to the appropriate subcontractors and/or suppliers. Institute informal and formal program reviews and audits of subcontractor and supplier development and production efforts. The contractor's quality organization should develop metrics and use audits to develop a list of approved suppliers to be used for critical subcontracted items.

- **Establish and track each item's pedigree** as it is manufactured to establish an as built vs. an as-designed configuration, and provide a means to find installed items in the event of a recall due to a generic problem. Lot numbers or date codes should be recorded along with any revision numbers of parts, materials, components, and assemblies used to build flight hardware. Special attention should be placed on any out-of-sequence operations to assure that the integrity of the product has not been compromised. In addition, Material Review Board actions should be reexamined to assure that "use as is" decisions are acceptable. Document links should be provided pertaining to resolution of manufacturing/test discrepancy reports and the identification numbers of critical tools (e.g., torque wrenches) and test equipment used on the flight hardware.

6.5 Strategies and Execution by Phase

Although manufacturing assurance tasks primarily occur in Phases C and D1, they begin in Phase 0 with increased emphasis in Phases A and B and decrease in emphasis in Phase D2.

The seven phases are as follows:

1. Phase 0: Pre-KDP A Concept Studies
2. Phase A: Concept Development
3. Phase B: Preliminary Design
4. Phase C: Complete Design
5. Phase D1: Fabrication and Integration
6. Phase D2: Fielding and Checkout
7. Phase D3: Operations and Disposal (Note: Disposal is not addressed, since is not applicable to space segment flight software, and not typically applied to ground systems hardware upgrades).

6.6 Organization of Tasks

Within each phase, the manufacturing assurance tasks are grouped either under program planning with respect to manufacturing or system engineering with respect to manufacturing. There's also an additional section called "system," which is an indentured structure to capture additional tasks at the space/ground segments, space vehicle bus/subsystems, and space vehicle payloads that an individual project can use to capture tasks at any level needed.

6.7 Key Tasks and Associated Objectives

Mission assurance objectives are accomplished by executing key manufacturing assurance tasks. Several objectives are accomplished by performing the manufacturing assurance on an NSS program:

- In Phase 0, manufacturing assurance assures that the request for proposal (RFP) adequately defines manufacturing planning needs for new manufacturing processes via the statement of work (SOW), contract data requirements list (CDRL), data item descriptions (DIDs), and manufacturing specifications and standards. This is critical to ensure that mission assurance has the necessary information to conduct independent assessments.

- In Phase A, manufacturing assurance assures that the program's manufacturing requirements are adequately defined and planned with an infrastructure that will support a reliable and repeatable manufacture of flight hardware. This is achieved by assessing the integrated management plan (IMP), CDRLs, make or buy process adequacy of resources, manufacturing plans, manufacturing processes qualification, and certification of critical manufacturing processes and the identification of risks.

- In Phase B, the tasks assure the completeness of producibility analysis, the make or buy decisions, design for manufacturing and assembly (DFMA), manufacturing methods, strategy for technology obsolescence and diminishing manufacturing resources, and the use of special test equipment, tooling, and support equipment.

- Phase C shares the same objectives as in Phase B, but at a more detailed level to also include an assurance of the completeness of manufacturing/production readiness reviews, configuration control of manufacturing process documentation, stability of the production process, ability to deliver the product on time, and the process for packaging, handling, storage, and transportation (PH&ST) of parts, units, and the final product.

- In Phase D1, the tasks assure that the contractor has an effective data retrieval system for determining the as-built configuration, variability reduction program, manufacturing process flow charts, manufacturing process qualification approach, inspection/process control methods, and Corrective Action Board (CAB) and hardware acceptance reviews (HARs).

- In Phase D2, the tasks assure that all open technical manufacturing and anomaly issues are closed and the space vehicle is ready for launch.

6.8 Government and Contractor Enabling Tasks and Products

Key government and contractor enabling tasks are as follows for each phase:

	Government Enabling Tasks	Contractor Enabling Tasks
Phase 0	SOW, CDRL/DIDs, RFP	
Phase A	Final contract	Integrated baseline review (IBR)/system requirements review/system design review (SRR/SDR), CDRLs, manufacturing plans
Phase B	Preliminary design review (PDR) entrance/exit criteria Attendance at preliminary design audits (PDAs)	Completion of PDR CDRLs Completion of PDAs
Phase C	Critical design review (CDR)/manufacturing readiness review (MRR) entrance/exit criteria Participation at critical design audits (CDAs)	Completion of CDR/MRR CDRLs Completion of CDAs
Phase D1	Participation at Phase D1 technical reviews (e.g., test readiness review (TRR), formal qualification review (FQR), production readiness review (PRR)) Completion of Phase D1 technical audits (e.g., physical configuration audit (PCA), functional configuration audit (FCA)) Independent readiness review team (IRRT) assessments	Completion of Phase D1 technical review CDRLs End item data packages HARs
Phase D2	Participation at technical reviews (e.g., system verification review (SVR), mission readiness review (MRR), launch readiness review (LRR), flight readiness review (FRR) IRRT assessments	Completion of technical reviews and CDRLs

6.9 References

Policy-related

NSS-03-01	National Security Space Acquisition Policy, Guidance for DOD Space System Acquisition Process, Number 03-01, 27 December 2004
SMCI 63-1201	Assurance of Operational Safety, Suitability, and Effectiveness for Space and Missile Systems, 16 January 2004
AFI 99-101	Developmental Test and Evaluation, 01 November 1996

Specification and Standards

MIL-STD-1528A	Manufacturing Management Program, 09 September 1986

Technical Handbooks

MIL-HDBK-727	Design Guidance for Producibility Provides Guidance for Producibility Assessments
Aerospace TOR-2006(8506)-4494	*Space Vehicle Systems Engineering Handbook*, 30 November 2005
Aerospace TOR-2006(8506)-4494	*Space Vehicle Systems Engineering Handbook*, (chapter 20), 30 November 2005
Aerospace TOR-(8583)-5235	*Parts, Materials, and Processes Control Program for Space and Launch Vehicles*, 08 November 2006
Aerospace TOR-(8583)-5236	*Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles*, 13 November 2006

Best Practices

MDG ASC/ENSM	Manufacturing Development Guide, January 2004, Wright-Patterson Air Force Base
DOD 4245.7-M	Transition from Development to Production, September 1985

Other

Critical Process Assessment Tool (CPAT), “Manufacturing”

Chapter 7
Integration, Test, and Evaluation

Dan W. Hanifen
Baseline Systems/Payload
William F. Tosney
Cross Programs Systems Engineering Office
Julia D. White
Cross Programs Systems Engineering Office

7.1 Introduction

Integration, test, and evaluation (IT&E) is a broad process whose purpose is to verify end item requirements satisfaction (e.g., functionality, performance, design/construction, interfaces, and environment) at all levels of assembly as those end items (e.g., units) form a system. This broad goal includes not only the obvious assembly and test of flight systems and supporting ground support equipment (GSE), but also through evaluation, the use of analytical methods to certify requirements satisfaction. Test, analysis, and demonstration are used throughout the design and manufacturing cycle to ensure that as-designed breadboards and prototypes meet the design intent and as each article is manufactured, quality, performance, and functionality are measured to ensure process and requirements compliance. At higher levels of assembly (subsystem and system) test, demonstration, simulation, and analysis are used in appropriate combination to provide discernable evidence of compliance. The final step for an NSS system is system validation, which again uses a combination of test, analysis (and in some cases, simulation), to certify that the user's needs were met under operational service conditions.

7.2 Definitions

Integration is a process whereby components, subassemblies, assemblies, units, and subsystems are combined functionally and physically to form and perform as a complete system.

Test is an activity performed to determine output characteristics of the unit under test (UUT) as a function of variable inputs. For the purpose of this guide, there are two categories of testing: formal testing and informal testing. Formal space vehicle hardware testing uses rigorous test planning and flight-like test articles to contractually verify

requirements and validate unit, subsystem, and system performance. Informal space vehicle hardware testing, such as development testing, uses engineering models, breadboards, or prototypes to assist in design decisions (e.g., first of a kind) or flight-like units (e.g., qualification unit) to investigate problems/anomalies in latter stages of development. Software assurance is addressed in section 7.8 of this chapter.

Evaluation is an activity to objectively determine the suitability of the product to perform its intended mission and satisfy requirements. Evaluation in the context of test is the set of tasks necessary to assess the suitability of a planned test program to provide adequate proof of performance; to compare analytical results and predictions with comparable test results; and to determine the adequacy of the test program as actually executed. In context of verification, evaluation includes the necessary tasks to plan and execute analysis, simulation, and inspection.

7.3 Objectives

The following are key mission assurance (MA) objectives with respect to the IT&E program.

For each level of assembly, properly execute and verify the functional performance, design and construction, and interface requirements:

- Evaluate contractor provided-evidence of completion (EOC) that the as-built system (including interfaces) satisfies the requirements and specification baseline.

- Identify issues with the proposed test, integration, and verification plans and procedures.

- Evaluate appropriateness and risk of verification by any method other than testing.

- Evaluate risks associated with deviations from environmental testing standards (e.g., MIL-STD 1540) and other applicable standards or best practices.

- Evaluate the fidelity to the “test like you fly” (TLYF) and “test what you fly” philosophies, especially at the system and higher levels of integration, and identify risks associated with

deviations from these philosophies. This includes implications to accurate modeling and simulation.

- Assess the degree to which the requirements are objectively verifiable and correct unverifiable requirements.

- Evaluate analysis, simulation, inspection, and test results to determine readiness to proceed to subsequent test or program activities.

7.4 Practices and Tasks

Most activities associated with the development, integration, validation and verification of space system components; units, subsystems and systems[14] are formally planned and performed by contractor personnel. Typical program office MA activities include making sure the appropriate testing, especially development, qualification, and acceptance testing, is appropriately planned, performed, witnessed, documented, and test results are independently evaluated to establish development, qualification, and acceptance status. Government program office, engineering group discipline specialists, and engineering group environmental test specialists should evaluate the formal test program and advise government and contractor personnel on appropriate test approaches and levels based on best practices, standards, Lessons Learned, and data-based experience. In addition, independent review teams, which can include personnel from The Aerospace Corporation, periodically review and assess the overall test program as well as specific test results and the resolutions of test failures.

Informal tests are done to clarify design decisions during the development phase or in response to problems discovered during planned formal testing and may be planned and executed less formally by contractor personnel. Aerospace technical discipline specialists should be involved in reviewing, witnessing, and evaluating the

[14] A system is defined as a composite of equipment, skills, and techniques capable of performing or supporting an operational role. A system includes all operational equipment, related facilities, materials, software, services, and personnel required for its operation. A government program office or the procurement agency responsible for its acquisition typically defines the scope of a system. In the context of this guide, “system” refers to the spacecraft and/or launch vehicle and associated ground command, control, and telemetry equipment, facilities, and personnel. The “system” can exclude mission data processing and distribution of mission products to the user.

planning and execution of key informal and ad hoc testing at each level of assembly. Aerospace monitors contractor activities to recognize when problems and issues arise and will contribute when Aerospace has specific design or testing expertise.

Under certain circumstances, Aerospace engineering laboratory personnel may perform specialized tests. These are usually done to demonstrate proof of concept, answer specific questions about certain technologies, or to assist with failure analysis.

"Test as you fly/fly as you test" is a key test philosophy for any NSS space or launch vehicle test program. It is derived from the earlier "fly before you buy" philosophy applied to other DOD weapons systems. TLYF is not formally defined in any existing or previously in-force government standard or handbook. It is generally used to mean that launch or space vehicles are exercised as they would be during flight or on-orbit mission, controlling the flight equipment and software (test what you fly) by ground equipment and software that will be used to operate it when fielded. This level and type of test may also be referred to as "day in the life" (DITL) or mission operations test. The philosophy may also be applied at lower levels of integration; e.g., launch or space vehicles controlled by test equipment, subsystems interacting with simulators, units exposed to flight level environments, slices subjected to mission-level data loads, or parts run in a mission-like way while immersed in an expected radiation field.

It is clearly not possible to test precisely as one would "fly" in a 1-g factory environment. A lesson learned from many mission ending in-flight failures is that it is both necessary to attempt to TLYF, and to acknowledge the inability to completely do so. TLYF may not be accomplished due to physics constraints (cannot be done), engineering limitations (doing things "like you fly" requires non-flight elements that may confuse or nullify the results of the test), or unwise use of resources (too much money or time for questionable data return). TLYF exceptions, therefore, must be assessed for risk. TLYF may force design choices to be more testable or to provide more useful *in situ* measurements. Adopting a TLYF philosophy may have profound effects on test facilities, test equipment, and test beds.

7.4.1 Integration

Successful space vehicle or launch vehicle hardware integration is a tightly controlled process that starts with a structural frame and uses a

hierarchical assembly and testing process to iteratively combine parts, components, subassemblies, and assemblies into units and subsystems, and finally into the finished system. Depending on the system requirements, contamination control/cleanliness requirements may place constraints at all levels of assembly and test to avoid potential mission impacts and/or loss of mission performance. Typical integration activities include receiving inspections, cleaning, calibration of support equipment, use of mock-ups and pathfinders, and rehearsals for fit checks, electrical grounding checks, mechanical and/or optical alignment measurements, tooling fabrication, completed integration procedures, an active record keeping process, electromagnetic interference (EMI) checks, mechanical, electrical, and thermal interface checks, and functional checks. Integration also includes examining integrated elements at all levels of assembly to detect flaws or problems that might surface at higher levels of assembly, potentially causing expensive rework or loss of mission.

A comprehensive and perceptive test program includes the following elements:

- **Test planning** begins during the early concept and requirements definition phase and continues through the qualification, production, and operational test phases of a program. Flight software and ground system test planning continues through operations and maintenance. Test planning requires that the system operational environments, modes, states, redundancies, risks, and failure modes are well understood, and focuses the test program in those areas to perceptively identify or validate the absence of defects and problems affecting mission success. Launch vehicle verification risk tradeoffs consist of even greater compromises, typically opting for flight demonstration testing to validate the final integrated design. Critical technical risks associated with implementing the test plan should be identified and tracked via the risk management process as appropriate.

- **Development testing** is used to collect and assess data in order to: validate that design concepts, processes, or techniques will achieve the desired results, reduce risk prior to the fabrication of qualification and flight hardware, validate test support equipment and that test procedures are correct, acquire data to verify system models and simulations, and

investigate problems found during testing in later stages of qualification and acceptance. Software test is addressed in Chapter 16.

- **Life testing** is a ground test program for satellites and launch vehicles designed to measure decreasing performance and failures as a function of time for assemblies/ units that may have a wear-out, drift, or fatigue failure modes by collecting engineering data as the assembly/unit is operated over extended periods of time.

- **Qualification testing** is conducted on those flight hardware units with insufficient history relative to the flight units, system application, or environment being addressed to demonstrate that the contactor's design, manufacturing process, and acceptance program produce hardware that meets the expected environmental requirements (transportation, launch, on-orbit operations, and repeated acceptance testing) as well as mission life requirements with margin.

- **Acceptance testing** is used to demonstrate that **each delivered flight item** meets performance requirements under maximum conditions expected during transportation, launch, and on-orbit operations, but not necessarily to demonstrate performance over mission life. Acceptance testing also acts as a control gate to ensure the flight item is free of workmanship, material, and quality defects.

- **Functional and performance testing** is used to verify electrical, mechanical, digital, signal, radio frequency, optical, and other mission performance parameters against the stated requirements under operational service conditions. Functional and performance tests, performed before, during, and after environmental tests, are used to verify performance under worst-case service conditions and to verify that the environmental stress testing did not change test article performance or mature latent defects into detectable flaws.

- **End to end (E2E) testing** is conducted at the full-up system level, including space, ground, and user segments. The testing includes signal or stimulus input to message, data, or signal output using all hardware, software, processes, people, and time/timing involved with flight and mission operations

between these inputs and outputs. Other common terms used to describe this type of test include inter-segment or multi-segment testing. E2E or inter-segment testing is first conducted at a single factory with simulations representing external interfaces and multi-segment functionality. Finally, factory-to-factory or factory-to-ground station testing is conducted to validate the reliability, operability, and performance of flight and ground systems to be delivered for launch and/or mission operations.

- **Launch base and/or ground station functional testing and rehearsals** are done during the launch processing timeframe. At the launch base, functional tests are conducted separately on the launch vehicle and the space vehicle after arrival from their respective factories, and then conducted again after the spacecraft is integrated to the launch vehicle. These tests not only demonstrate system interface compatibility between the space and launch vehicles, but re-verify compatibility between the vehicles and the launch base facilities as well as the early orbit and mission operational ground stations.

Rehearsals provide opportunities to demonstrate operator proficiency, system operability, and system reliability. Rehearsals can also provide the means to further demonstrate interface compatibility between the satellite and ground system before launch, and ensure that the encryption keys are valid. At ground stations, ground system rehearsals (computers, software, procedures, and personnel) should conduct operational demonstrations (ODs) of the as-built system to expose the new system to representative operational scenarios. ODs verify the correctness of operational documentation, the correctness of the operational databases, the efficacy of training, and uncover flaws in operational procedures. The OD is typically conducted for critical deployment and early orbit events and for DITL testing of the overall ground system. Following each round of tests, demonstrations, or rehearsals, results are evaluated and problems identified and assessed for impact and criticality, and corrective actions/workarounds are implemented prior to the formal flight readiness review (FRR) or launch readiness review (LRR).

- **On-orbit testing** is used to characterize overall mission performance and space vehicle subsystem performance, to verify requirements (if required), to characterize operating

limits, and to discover any problems affecting mission success resulting from the launch environment. Anomalies are identified, traced to root cause, and either corrected or workarounds established before turnover to mission operations. While conducting mission operations, periodic calibration tests are performed to maintain the space vehicle's performance according to specification (e.g., precision, accuracy, throughput, and timeliness). The frequency and extent of calibration testing is dependent on space vehicle performance and reliability trends.

- **System of systems (SoS) testing** is used to validate SoS performance and support the operational assessments of system suitability and effectiveness once all system elements have been deployed to their operational service locations and environments. NSS programs conduct a SoS-level test using operational space vehicles, ground systems (including mission data processing and operators), and external interfaces with other systems and customers. This type of test is often necessary in that it may be impossible to otherwise fully test and measure performance of a new space vehicle, system, or combination of systems on the ground during development, much less under simulated operational conditions.

- **Test and measurement systems** are required to exercise the hardware and acquire the experimental data necessary to allow clear and objective determination of whether development, qualification, and acceptance test objectives have been met. A formal measurement assurance plan and program (if successfully implemented) guarantee that measurements and test equipment operate in a fashion that assures the data quality can support the test objective assessment. This measurement assurance program, including the entire calibration/metrology and equipment recall functions, should be operated in accordance with applicable military specifications and verified by MA. Experimental uncertainty is a key issue in determining if the quality of the test data is appropriate for test success. In each case, where a test measurement is used to assure the quality of the product for the customer, the allowable experimental uncertainty of that data should be defined as a requirement in the relevant test plan.

7.4.2 Engineering Evaluation

Test and evaluation (T&E) engineering is responsible for developing and implementing a thorough and comprehensive system test plan based on defining a logical sequence of test events which will provide:

- Early evaluation of system concepts and feedback to the design function; the creation and evolution of test requirements through rigorous analysis
- Identification of performance parameters critical to operational effectiveness
- Establishment of validated linkages between operational requirements and test criteria
- Timely and credible test results to support milestone decision making
- Early identification of potential program risks

T&E engineering complements testing by using the data collected during testing to judge compliance with requirements, record failures, or improve simulations. The system test planning process establishes the test objectives, test fixtures/equipment, diagnostic instrumentation, and test points required for each test at each level of assembly, including regression testing. The verification process ties the test method and measurements to requirements in order to allow a judgment of requirements satisfaction. Typical activities include:

- **Pre-test reviews** are conducted to ensure the test article, test equipment, facilities, procedures, hardware, and software are ready for the event to proceed. Lessons Learned are also incorporated from previous test attempts and test programs.

- **Post-test reviews** are conducted following a critical test event to fully understand all test data before breaking configuration and moving on to the next test event. This joint contractor-government evaluation includes understanding the implications to mission success from data available through direct observations and the implications based on the results of data analysis (e.g., trending, out-of-family conditions, etc.). Data trends may indicate potential problems even if the direct measurements were consistent with and verified applicable specifications. Post-test reviews validate that the test results are also consistent with test objectives and include a rigorous review all test anomalies. Lessons Learned are formulated

and communicated within the test organization, the program office and, in some cases, with other NSS programs.

- **Test risk assessment** begins early in MAG Phases A and B of typical space programs. This assessment is primarily focused on resolving three issues. First, test risk assessment evaluates the key risks to mission success and determines if test is the best verification method to verify unit, subsystem, and system requirements. The assessment includes consideration of risk and confidence should another verification method (e.g., analysis, similarity, inspection, demonstration) be chosen due to program constraints. Second, test risk assessment examines the risk to the flight hardware undergoing the proposed test program to avoid overstressing the test article. Finally, test risk assessment evaluates each test for each proposed test article to ensure that the test program adequately exercises the combined software/hardware for nominal and off-nominal operating states, modes, potential redundancies, and failures in both nominal and off-nominal (worst case) operational environments[15].

- **MA** makes use of and participates in at least two contractor/subcontractor-led activities to discover and correct hardware and software test failures, the contractor/subcontractor Failure Reporting and Corrective Action System (FRACAS), and the failure review board (FRB) process. FRACAS is described in Chapter 11 and will not be repeated here. A successful test program includes interaction with FRACAS as an orderly method to capture and report test failures, associate failures with root cause(s), track the implementation of corrective actions to remediate failures, and track required retests to verify the causes of the failures have been corrected. A FRB is an established forum and may

[15] Aerospace uses a qualitative technique to subjectively assign values to testing as a means of evaluating the adequacy of typical test programs. This technique is known as Environment Test Thoroughness Index (ETTI). For each test at each level of assembly, a qualitative score is assigned based on test thoroughness when evaluated with respect to Aerospace SMC TR-04-17 TOR-2003 (8583)-1 (replaces MIL-STD 1540D), *Test Requirements for Launch, Upper Stage, and Space Vehicles*.

be composed of contractors, subcontractors or suppliers, the government program office, and consultants to coordinate the review of all significant failure reports, review failure trends, track and review the timely implementation of corrective actions, and provide closeout approval for reported failures (see also Chapter 11).

7.5 Strategies and Execution by Phase

While the IT&E process is active throughout a space system's life cycle, the majority of IT&E effort occurs during MAG Phases B, C, D1, and D2. As hardware and software mature through the design and development process, incremental testing at varying levels of assembly occurs. During MAG Phases B and C, the emphasis is on design validation. During MAG Phase D1, the emphasis is on validating test support equipment, establishing system performance baselines, and conducting unit/system qualification or acceptance. During MAG Phase D2 the emphasis is SoS functional testing in the operational environment, resulting in operational turnover of the new space system into mission operations.

Significant IT&E activities are described below for each phase:

MAG Phase 0: Consideration for perceptive and sufficient IT&E begins during MAG Phase 0 where potential technologies are considered for implementation in space systems. The technologies are evaluated for potential feasibility to advance future space program-unique applications. Considerations must be given to both ground and on-orbit testability to establish lifetime reliability and performance within predicted nominal and worst-case service environments. This includes considering testing impacts in 1-g environment, infrastructure requirements, needed GSE (e.g., handling, power, control) to include special test equipment for high-fidelity calibration and evaluation.

MAG Phase A: During concept development, IT&E evaluates the proposed concept space system concept alternatives to understand the interaction between mission requirements, system options, unit and system certification concepts and risks, and service environment alternatives and risks. As the space system concept alternatives are refined, the contractor's integration and test strategies and philosophy become clearer, and the needed ground test infrastructure, GSE, and special test equipment can be

considered. The overall system test program can be scoped considering applicable (and tailored) MA standards for test sufficiency/thoroughness and concept specific constraints driven by new technology. Pathfinder components/subassemblies and units considered as high risk are produced as brass board/ breadboard/prototype units. Brass board/breadboard/prototypes are evaluated by IT&E as part of a risk reduction effort to validate functionality, design, producibility, testability, and (in the best case) performance. This activity continues throughout MAG Phases B and C as well.

MAG Phase B: During preliminary design, IT&E supports risk reduction testing and developmental testing of prototype and engineering units to validate preliminary design and allocated performance. This includes evaluation of any environmental testing done as part of contractor risk reduction and/or developmental testing to validate design robustness. IT&E evaluates subsystem and system preliminary designs, preliminary I&T planning, and preliminary verification planning to identify issues and recommend correctives actions. IT&E also continues to examine the tailored MA test standards and the contractor's test strategy to ensure that test strategy adheres to acceptable environmental testing standards (i.e., MIL-STD 1540E), pyramid testing philosophy, and TLYF strategy. Finally, IT&E evaluates heritage component/assembly certification, if available, for use on the current program and application. During MAG Phase B, IT&E begins to also focus on test risks to the flight hardware over the course of the entire test sequence to avoid overstressing flight hardware. Finally, IT&E acts as an advocate for and evaluates the preliminary design of the GSE and test support equipment accompanying each subsystem design. Adequacy of IT&E schedule margin should include rework/retest in the event of test failures. Evaluate the allocation of on-orbit testing vs. ground testing.

MAG Phase C: During the final design phase, IT&E focuses on much the same areas as for the previous preliminary design phase. IT&E evaluates increased maturing of the final design of both the flight system and of the accompanying GSE/test support equipment and supports risk reduction by evaluating any ongoing developmental testing. Any planned certification testing at the component, subassembly, and unit level is evaluated for sufficiency. Any continuing environmental testing to validate

design and performance robustness is also evaluated. During MAG Phase C, the contractor submits the final system integration and test plan and the final verification plan for final approval before authorization to proceed to MAG Phase D1 (fabrication and integration). During MAG Phase C, final allocation of test as a verification method for system-level requirements is completed and assessed. Based on requirements flowdown to build to specification, test requirements are also flowed down to lower-level assemblies. IT&E continues to assess test risks to the flight hardware over the course of the entire planned test sequence to avoid overstressing flight hardware. IT&E evaluates heritage component/assembly certification, if available, for use on the current program and application. Finally, IT&E acts as an advocate for and evaluates the final design of the GSE and test support equipment accompanying each subsystem design. Adequacy of I&T schedule margin should include rework/retest in the event of test failures.

Phase MAG D1: During MAG Phase D1 (fabrication and integration), IT&E resources evaluate the execution of the flight system assembly/integration process from component fabrication to unit-level assembly and from unit-level certification to system-level integration and certification. This includes all unit-level, subsystem (if required), and system-level environmental certification to applicable (and current) specifications and standards. During system-level certification, IT&E evaluates the baseline integrated system test (BIST) and the final integrated systems test (FIST), which establish functional and performance baselines before and after environmental testing. In addition, IT&E resources evaluate the planning and execution of inter-segment compatibility testing beginning in a single factory with simulated interfaces, and extending to a factory-to-factory configuration using a dedicated test network, the flight space vehicle, the operational ground systems, and operations personnel/procedures. In preparation for system-level certification, IT&E resources evaluate the integration, validation and, if necessary, environmental certification of applicable GSE/special test equipment. During Phase D1, the bulk of the system specification is formally verified using “test” as the preferred verification method. IT&E evaluates contractor provided formal sell-off packages containing adequate engineering evidence (usually in the form of engineering memoranda) to demonstrate in detail how the requirements were satisfied. Throughout the test

program, IT&E identifies any deviations from the TLYF philosophy that may increase risk to the program. IT&E evaluates the planning for and execution of factory confidence/pre-ship testing in preparation for deploying the space vehicle to the launch site.

MAG Phase D2: During the fielding and checkout phase, IT&E focuses on the planning for and execution of space system and segment-level launch base and on-orbit testing, and the final operational test and evaluation (OT&E). At the system level, IT&E resources evaluate satellite initialization immediately after launch. This initialization establishes the spacecraft subsystem and system performance baseline after surviving the harsh environment of launch and the deployment of critical satellite assemblies (e.g., solar panels, communication antennas). At the segment level, the satellite and associated ground control and mission data processing are demonstrated as part of a space segment test to validate inter-segment interfaces are functional. Finally, IT&E evaluates the planning and results of OT&E. OT&E is a transition phase that validates user/operator expectations for operability and utility of the new space system while exercising all ground control, communications connectivity, mission data processing, and user interaction procedures and processes.

MAG Phase D3: During operations and disposal, IT&E resources evaluate the planning and execution of routine mission operations performance, routine satellite and supporting ground system calibrations, all proposed software, hardware, and data configuration changes, and all spacecraft and ground system anomaly recovery activities, including diagnosis of root cause and the validation of corrective actions (including software/data corrections and procedural workarounds). In the case of disposal of on-orbit satellites, IT&E ensures that adequate planning (including simulation), procedure development, and rehearsals have occurred so that all disposal activity occurs error free.

MAG Generic Tasks: IT&E evaluates the government program planning prior to each development phase and for major contract modifications to ensure that the test program is sufficient and perceptive at all levels of assembly. In doing so, IT&E evaluates the request for proposal (RFP) (with associated statement of work (SOW), contract data requirements list (CDRL), data item descriptions (DIDs), and design/construction specifications and

standards, including system test) and the contractor's proposal response. In preparation for each new phase, IT&E assures adherence to recommended integration, test, and certification standards consistent with the objective to enhance MA or participates in joint efforts with the government and contractors to tailor those standards to meet program unique circumstances. IT&E ensures that the necessary data to evaluate I&T readiness and completion is readily available and stored over the long term by contract mandate. Finally, IT&E ensures that the contractor has been tasked to have a comprehensive software, data, and hardware configuration management process that will support test configuration definitions throughout the system life cycle.

7.6 Organization of Tasks

The Mission Assurance Verification Matrix (MAVM) task database for the IT&E process is organized in a hierarchy by life cycle phase discussed above. For each life cycle phase, the process is further organized into the following categories: Program planning, systems engineering, space systems integration, and testing.

Program planning includes an evaluation of the contract mechanisms defining the scope and tasks for the work performed by the contractor to assure that the information required to plan, execute, and evaluate a comprehensive system test program is in place and accessible by the system program office (SPO) technical team.

Systems engineering includes a series of tasks to ensure that the requirements allocation process traces to the test process both ways and that there is adequate schedule and resources for both system integration activities and a system test program. Assessment of testing schedules, test risks, verification process, and allocation of test as a method are addressed in systems engineering.

Space systems integration tasks are required to evaluate whether the contractor's process, sequencing, and schedules successfully build up the space vehicle from the lowest level of assembly to a fully integrated system. Space system testing tasks include evaluation of contractor tasks to successfully demonstrate system functionality, interface compatibility, and performance and/or certify unit, subsystem (if applicable), and system for the service environment (e.g., factory, transportation, launch base, launch, on-

orbit). Also included are the activities to validate and certify as required all supporting GSE and/or test equipment.

Within each category described above, activities are further organized by level of assembly (unit, subsystem, system, and segment). Inter-segment and SoS testing is organized with the systems engineering functions.

7.7 Key Tasks and Associated Objectives

Sufficient testing is the key to increased mission success. This section is intended to highlight those key tasks that are deemed more important to the goal of achieving mission success. This discussion is organized by key tasks, rather than MA phase. The tasks will generally run across several phases and evolve as the system evolves.

During program start-up, IT&E evaluates the program acquisition strategy, government RFPs, and contractor/subcontractor proposals, to ensure that consistent direction has been given and adequate resources have been set aside to provide for a robust test program. An independent analysis of potential MA test standards compared to historical test programs, costs, and mission success trends will provide valuable insight in order to optimize a test program within given funding and schedule constraints. This MA activity will have to be repeated at each major development milestone to ensure that schedule and budget pressures do not result in a dilution of the contractor's test program.

IT&E MA activities assess the system concept and the new technology that will be introduced with that concept. Consideration will be given to mission utility, performance, material composition, structure size, stiffness, etc., that may impact the way the ground testing should and can simulate the service environments (e.g. "0" gravity, vacuum, etc.). Or, are themselves affected by the integration and test environment (e.g. humidity, contamination, debris, temperature, etc.). Additionally, IT&E evaluates any existing technology or delivered flight hardware that will be potentially considered. While the designers worry whether existing technology and/or flight units can satisfy requirements, IT&E MA is concerned with understanding any prior test history to optimize the test program and avoid over-testing potential flight hardware, thereby decreasing predicted mission life and reducing mission success.

During Phase 0 through final design, IT&E is concerned with the scope, rigor, and sufficiency of the overall test program. The proper test program scope is critical to ensure that all required component, unit, subsystem, and system-level development and certification testing is defined and that margin is available. Test scope includes adequate resources and schedule margin for retest in the event of failures/rework that inevitably occur in a development program. Test rigor refers to ensuring that contractor processes are in place to rationally approach test milestones with key pretest reviews, clear entrance criteria and procedures, and also ensure that all test failures are documented, chased to root cause, and that all rework is adequately tested without shortcuts. Sufficient testing includes the establishment of the right test conditions at the right level of assembly to perceptively measure performance, or force latent defects into failures. Testing must also provide the means to measure the right data for models and simulations that will be used during system-level verification to provide the basis of predicted performance for on-orbit testing from beginning-of-life initialization to end-of-life disposal. Where needed, MA can also provide capabilities for independent testing to assess test failure root causes and recommend mitigation steps prior to retesting.

While this chapter promotes testing as the preferred verification method, IT&E MA must also evaluate the test program to ensure that test risks are considered. These risks fall into three categories. First, IT&E must ensure that testing is capable of providing the information needed to verify key requirements and validate system E2E performance. This point emphasizes the need for the test program to be perceptive, both to measure performance and drive out latent defects due to shortfalls in the manufacturing/assembly processes. Second, IT&E must ensure that, if another verification method (e.g., analysis, similarity, inspection) is chosen instead of test, the risk of such a choice including potential impacts is identified. Without testing allocated requirements at appropriate levels of assembly there is no way to provide rigorous evidence of requirements satisfaction. Third, IT&E must also address the risk of testing too much. All flight hardware is evaluated to ensure that the combination of certification testing, retesting in the event of rework, and the launch itself does not result in flight hardware with limited mission life once on orbit.

Throughout all the MAG phases, IT&E MA also provides an independent assessment of the concept of operations (CONOPS), the integration and test program, test plans, test procedures, schedules, and training to ensure that, at every level possible, the TLYF philosophy is

followed. This philosophy emphasizes the need to test each level of assembly as it would be flown including environments (in order during launch phase), operational scenarios (including nominal and off-nominal cases), all operational software logic paths, all hardware states (e.g. on, standby, off), hardware modes (e.g., 100%, 50%, 25% capacity/capability), all hardware redundant capabilities, all hardware and software fault detection and housekeeping functions, and all external interfaces.

7.8 Government and Contractor Processes and Products

Enabling Government Processes and Products

The government processes should provide access to any contractor data stored in government databases. The government should also provide routine and secure communications access with the contractors. Access for information exchange includes regularly scheduled management and systems engineering reviews, telecommunications, development, and test-related milestones (e.g., SRR, PDR, CDR, TRR) and integrated product teams (IPTs) or working groups (WGs). To facilitate IT&E, the government program office should provide the following products for MA use: draft and final RFP for each acquisition phase; the contractor/subcontractor proposals for each acquisition phase, including proposed program and test schedules; the negotiated contracts for each phase; the acquisition plan; all high-level operations concepts documents; the initial and final capabilities description document; the test and evaluation master plan (TEMP); the integration and test plan; conservatively tailored MA test standards; system CONOPS and companion design reference cases; and all CDRLs and DIDs. Government provisions for independent test and evaluation may also be required early in the life cycle to ensure the capability exists for independent testing.

Enabling Contractor Processes and Products

To enable the MA IT&E tasks, the contractor must provide access to and cooperation in the following contractor processes: Management, systems engineering, and test engineering processes; integration and test planning and execution processes; verification planning and execution processes; CONOPS WGs; and configuration management, risk management, and test failure review/corrective action processes. To facilitate MA IT&E, the contractor should be required to provide

timely access to all requirements allocated to build to specifications, design information (including engineering memos), and test results/test failure data for all flight units and special test equipment. This includes preliminary and final unit, subsystem, and system design presentations and data, integration and test requirements, plans and procedures; detailed integrated master schedules (prime and subcontractor); verification plans; verification ledgers (map requirements to verification methods to verification evidence); test reports; and test/engineering memos documenting verification evidence.

7.9 References

Policy-related

NSS-03-01	National Security Space Acquisition Policy, Guidance for DOD Space System Acquisition Process, Number 03-01, 27 December 2004
SMCI 63-1201	Assurance of Operational Safety, Suitability, & Effectiveness for Space & Missile Systems, 16 January 2004
AFI 99-101	Developmental Test and Evaluation, 01 November 1996
AFI 99-102	Operational Test and Evaluation, 01 July 1998
AFPD 99-1	Test and Evaluation Process
AFI 99-106	Joint Test and Evaluation
AFI 99-109	Test Resource Planning

Specifications and Standards

Aerospace TR-2004(8583)-1 Rev. A	*Test Requirements for Launch, Upper-Stage, and Space Vehicles* (aka SMC TR-06-11)

Aerospace TOR-2003(8583)-1	*Electromagnetic Compatibility Requirements for Space Equipment Systems*, August 2005
Aerospace TOR-2004(3901)-3242	*General Guideline for Space Vehicle (SV) Verification Plan Development and Execution*, 15 March 2004
MIL-STD-810F Notice 3	Environmental Engineering Considerations and Laboratory Tests, 05 May 2003
MIL-STD-1833	Test Requirements for Ground Equipment and Associated Computer Software Supporting Space Vehicles, 13 November 1989
ISO/IEC 17025:1911	General Requirements for the Competency of Testing and Calibration Laboratories
Aerospace TOR-2003(8583)-2895	*Solid Rocket Motor Case Design and Test Requirements*, 22 December 2004
Aerospace TOR-2004 (8583)-3291	*Criteria for Explosive System and Devices Used on Space Systems Vehicles*, 09 August 2004, (replaces MIL-A-83578A and MIL-STD-1576)
DOD-W-83755 Rev. A, Notice 1	General Handbook for Space Vehicle Wiring Harness Design and Testing, 04 September 1992
ANSI/NCSL Z540-1	Calibration Laboratories and Measuring and Test Equipment—General Requirements
IEEE12207	Information Technology—Software Life Cycle Processes Software Verification
MIL-STD-45662	Calibration Systems Requirements

MIL-STD 1543B	Reliability Program Requirements for Space and Launch Vehicles, 25 October 1988
MIL-STD-785B Notice 2	Reliability Program for Systems and Equipment Development and Production, 05 August 1988

Technical Handbooks

Aerospace TOR-2006 (8506)-4494	*Space Vehicle Systems Engineering Handbook*, 31 January 2006
Aerospace TOR-2006 (8546)-4591	*Space Vehicle Test and Evaluation Handbook*, 06 November 2006
ISBN 1-884989-11X	Spacecraft Thermal Control Handbook, Volume 1, 200
ISBN 1-88-4989	Spacecraft Thermal Control Handbook, Volume 2, Cryogenics 14-4 (v.2)
IBSN 1-884989-15-2	Space Modeling and Simulation Roles and Applications Throughout the System Life Cycle, 2004
IBSN 1-884989-13-6	Nickel-Hydrogen Life Cycle Testing Reviews and Analysis, 2003
MIL-HDBK-340A Vol. II, 1	Test Requirements for Launch, Upper-stage, and Space Vehicles, April 1999
MIL-HDBK-334A	Environmental Stress Screening (ESS) of Electronic Equipment, 16 August 1993
MIL-HDBK-781A	Handbook for Reliability Test Methods, Plans, and Environments for Engineering, Development Qualification, and Production, 01 April 1996

MIL-HDBK-1811	Mass Properties Control for Space Vehicles, 11 August 1998
MIL-HDBK-2164A	Environmental Stress Screening Process for Electronic Equipment 19 June 1996
MIL-HDBK-83575	General Handbook for Space Vehicle Wiring Harness Design and Testing, 04 June 2005
NASA Technical Memorandum 110172	Pyrotechnic Design, Development and Qualification June 1995
Aerospace TOR-2001(1465)-0934	*Software Independent Verification & Validation (IV&V)* 28 February 2001
Aerospace TOR-2006(3904)-1	*Digital ASIC/PLD Development Handbook for Space Systems*, 30 November 2005

Best Practices

Aerospace Briefing	Satellite Acceptance Test-Updated Study on Acoustic Test Effectiveness, June 2001
AIAA-91-1302	Thermal Testing Explained, June 1991
Aerospace ATM 2003(3907-62)-1	*Recommended Sequence for Thermal Vacuum and Dynamics System Testing*, 10 September 2003
Aerospace ATM 2002(3130-12)-1	*Design and Verification of Launch and Space Vehicle Structure Briefing*, 1 May 2002

Data Deliverables

DI-EMCS-80200B	Electromagnetic Interference Test, 20 August 1999

DI-EMCS-81540A	Electromagnetic Environmental Effects (E3) Integration and Analysis Report, 19 December 2002
DI-EMCS-81541A	Electromagnetic Environmental Effects Verification, 19 December 2002
DI-QCIC-80553	Acceptance Test Plan, 25 March 1998
DI-NDTI-80809B	Test/Inspection Report, 24 January 1997
DI-NDTI-81284	Test and Evaluation Program Plan, 11 September 1992
DI-NDTI-80566	Test Plan, 13 April 1988

Other

Critical Process Assessment Tool (CPAT), 14 August 1998

Tosney, William F. and Pavlica, Steve. June 2003. "Satellite Verification Planning Best Practices and Pitfalls Related To Testing." *Proceedings of the 5th International Symposium for the Environmental Testing of Space Programmes.*

White, J, Wright, C. October 2006. "End-to-End Testing in a Test Like You Fly Context." *23rd Aerospace Testing Seminar.*

Chapter 8
Operations Readiness Assurance

Dan W. Hanifen
Baseline Systems/Payload
James B. Gin
AWTR Systems Engineering
John G. Gebhard, III
Retired

8.1 Introduction

For the purposes of this guide, **operational readiness assurance (ORA)** will be divided into three general categories for discussion: readiness planning, activation, and mission operations.

8.2 Definitions

The term **readiness** refers to all the activities required to transport, receive, accept, store, handle, test, deploy, and control space vehicle, launch vehicle, and supporting ground systems such that associated flight or mission operations can be conducted safely while maintaining vehicle integrity.

Activation is a set of activities whereby newly acquired capabilities and/or systems are operationally checked out by a government program office/engineering development team before they are released for mission operations. For the purposes of this guide, activation include space vehicle activation on orbit, launch vehicle “activation” after successfully completing launch base processing when judged ready to perform flight operations, and ground system “activation” after it has been deployed, the crews proficient and ready for mission operation.

Mission operations is the program stage after launch vehicle processing and/or satellite activation where operators and users control the intended mission for the launch vehicle or satellite until completion end-of-life.

8.3 Objectives

The objectives of readiness planning as carried out by the government program office-development contractor-launch base team are to guarantee that the material handling of the elements of a system and the interaction of personnel and external equipment with the system itself can be, and are, executed safely and without causing damage to the system or to the handling equipment.

The objectives of activation are to ensure that the space vehicle and launch vehicle are configured and ready to perform mission and flight operations, respectively.

The objectives of mission operations are successfully executed when a launch vehicle reliably completes flight operations and places its payload in its intended orbit. For space vehicles, mission operations are successful executed when both the bus and payload perform as intended over their design life and reliably produce and deliver mission data to operators, users, and customers.

In practical terms, the ORA objectives address on one hand the verification of operations procedures, following their definition, in order to make sure that they are consistent with overall system integrity and safety goals, and, on the other hand, the validation that the operational execution of these procedures meets their intent and preserves actual system integrity and safety.

8.4 Practices and Tasks

ORA begins early in development and continues through the system operational life. ORA is normally implemented via a combination of process/procedure planning, control, and verification activities, which are described in the following subsections.

8.4.1 Readiness Planning

Readiness planning is a continuous activity over the life cycle of the system and contains critical mission assurance elements. Key operations necessary for the handling of major system components and elements should be identified relatively early in every program, i.e., as soon as the system processing is sufficiently well defined. At that point, planning for major assembly, test, integration, and deployment operations begins. Launch system, transportation, and launch base

infrastructure requirements and operations concepts are developed for the resources needed to successfully process and launch the space vehicle. Physical, functional, environmental, operations, performance, and safety requirements are documented. Testability, launch base processing, and space vehicle pathfinder activities also are considered.

The responsible government program office works with the launch base/deployment site and range operations personnel to ensure that all operations planning is completed and in place for receiving the hardware, utilizing needed facilities, security, safety, launch processing, environmental impacts, communications for administration and telemetry receipt/processing, and radar tracking and optical observation to support launch and mission requirements. If new facilities or modifications to existing facilities are required, the program will review the system specifications and design drawings to ensure that handling and storage of the system and its components is adequate.

Human factors engineering considers what functions have been allocated to system operators and users, how much time is allocated for the tasks, what information is required and level of proficiency is needed, and how the system operators, maintainers, and users will interact with and utilize the new system. Implicit in readiness planning are a series of analyses and simulations to capture requirements decompositions and allocation for human activity, conduct work flow analyses and simulations, conduct throughput analyses and simulations, determine the number, location, proficiency and certification required of operators and users, determine system provided status and product information formats, content and timeliness, assess and document decisions made by the system operator and user, and evaluate the maintenance and calibration operations concept in light of availability requirements.

Contingency planning is a necessary element in the overall space vehicle readiness planning process. Fault conditions as indicated by the contractor's failure mode and effects analyses are addressed with associated contingency operations developed to assure that the space vehicle can be recovered in a timely manner such that the vehicle integrity is maintained and services restored as soon as possible. Where appropriate, planning should identify specific procedure development required and plan for testing and rehearsing their execution along with an associated certification approach.

A key element in both normal and contingency operation is the development of simulators, analysis tools, and databases, as well as their certification for use in both procedure verification and operator training. In most instances, it is impractical to utilize pathfinder or flight vehicles to support this activity, thus requiring the development of simulators. Planning should address the development of simulator requirements, including human-machine interaction requirements, possible reuse of contractor's software test tools, and approach in certifying the resultant simulator's use.

8.4.2 Monitoring of Development and Test Operations

A program must have a thorough and timely understanding of development and test activities for the hardware and software to begin operations planning, identify changes required in that planning, and assure such changes are implemented expeditiously. To this effect, operations personnel monitor ongoing system development to fully understand capabilities and limitations of the hardware, software, interfaces, and procedures to be delivered and the potential workarounds in place. This task also includes reviewing development testing results as part of the design review process that characterizes functional performance.

8.4.3 Review of Factory Acceptance Test Operations

Ideally, factory acceptance testing would use the procedures, simulators, and test equipment developed for the launch and operations phase. The program operations personnel review the detailed factory acceptance test procedure produced by the system development contractor and the post-test report for each system or subsystem that is to be shipped as a completed configuration end item. A thorough review of the test procedure, simulators, and test equipment is completed prior to testing. Test report results are reviewed and accepted prior to shipment to an operational deployment site. This review includes hardware buildup and acceptance test pedigree data for flight hardware and ground support equipment, including reports on any ground test anomalies.

8.4.4 Pre-ship Reviews

The program conducts hardware pre-ship reviews to assure that flight hardware and components, software, ground support equipment, and procedural documentation are ready to ship to the deployment site.

Operations personnel participate in this review. This type of review is meant to identify any open issues affecting deployment and subsequent operations, verify that planning is in place to closeout these issues in a timely manner, and verify supportability of the program's ensuing activities. Operations personnel ensure sufficient coordination between the system contractor and Range/launch site, and/or any other receiving site, to assure that the latter is ready to receive program hardware, that receiving support has been appropriately scheduled, and receiving facilities are prepared to support hardware arrival and post-shipping inspection activities.

8.4.5 Launch/Deployment Base Operations

After the arrival of a system or major element at the launch base (or operational deployment site in the case of ground equipment), program office personnel participate in all ground support operations required to activate and validate the system(s) readiness for launch and/or deployment. In many instances, The Aerospace Corporation is required to certify that the operations were satisfactorily executed as part of the launch certification process.

8.4.6 System Activation Operations

System activation includes a review of ground system test (GST) and integrated system test (IST) procedures to ensure their adequacy to provide verification of stated system operational requirements. The government program office and operations personnel participate in the GSTs and ISTs per approved roles and responsibilities and test procedures, to:

- Evaluate the data generated from the tests and review system nonconformance conditions and anomalies
- Participate in the decision process to approve the repair, removal, and/or replacement of system elements that caused a nonconformance or anomaly
- Request or perform more in-depth data analyses and system operation risk assessments, as required

Where operations crews are required, an additional operational test and evaluation phase occurs to ensure the crews are trained and proficient, and that any deficiencies in crew setup are documented and assessed as not mission critical, with workarounds established.

8.4.7 Pre-flight Review of Flight Operations

A flight operations reviews (FOR) is conducted before each launch. The system contractor joins the government program office and operations personnel to assess the adequacy of final operations planning and compatibility of flight components with ground support equipment and the launch support network (e.g. the Range), including results of network compatibility tests. Specifically, the purpose of the FOR is to:

- Examine demonstrations, tests, analyses, and audits to determine system readiness for a safe and successful launch and subsequent flight operations
- Ensure that all flight and ground hardware, software, personnel, and procedures are ready and that all interface and cross-compatibility issues have been identified and resolved

In the case of the deployment of a space vehicle system, or placement in operations of a ground system only, the equivalent of the FOR can be referred to as a "deployment operations review." It involves a corresponding set of review actions, as applicable to the elements and operations included in the deployment of the space vehicle or ground system.

8.4.8 Post-flight Analysis

The program conducts, in coordination with the system contractor and the Range/launch site operator, post-flight review of all operations. From a mission assurance (MA) perspective, the post-flight review of launch operations and processes has the primary objective of assessing system performance, identifying Lessons Learned, and developing implementation plans to incorporate those lessons learned in the next launch cycle. A "post deployment review" can be similarly conducted for space vehicle systems once on orbit and/or for supporting ground control stations or systems.

8.4.9 On-orbit Mission Operations

Mission operations includes critical MA tasks to validate that space vehicle safety is considered while minimizing system unavailability during the performance of required mission operations. Detailed table-top peer reviews of routine and contingency procedures, on-orbit handbooks, and databases are used as part of MA. Additionally,

subsystem performance analysis and trending are used to forecast system outages and to support replenishment planning. These assessments can also extend to supporting ground systems and help identify needed maintenance. On-orbit anomaly resolution is normally a time-critical, crucial effort requiring a dedicated on-site team to provide real time assessments and recommendations.

8.5 Strategies and Execution by Phase

The operational readiness MA process is active in all program phases, but with emphasis on later phases when the system is being deployed to the field for launch preparations or in the case of ground systems, for installation into the operational sites and higher-level system integration tests. While operational readiness is a key MA issue in these phases, the necessary supporting planning and engineering must take place in the earlier phases to enable a successful readiness assessment in the later phase.

In MAG Phase 0, the proposed system operational suitability is assessed along with assuring consistency of the operation concepts that are captured in pre-Milestone A program summaries, including capabilities development document, initial concept of operations, system architecture, operational views, and test and evaluation stratagems. As in the other MA processes, the request for proposal (RFP) for the follow-on Phase A effort is assessed, but in this case relative to the operational requirements. Assuring that the appropriate human engineering standards (such as Standards for Human Computer Interface found in the International Organization for Standardization) are being required in the RFP is a typical MA task. It is also appropriate to closely examine operational performance requirements such as operational timelines, operational manning and skill levels, operational dependability, and other key performance parameters (KPPs) contained in the technical requirement document or following system specifications developed in MAG Phase A for feasibility and consistency with the program documentation.

During MAG Phase A, operational personnel should be represented at the system design review and participate in the detailed review of the system operational aspects. Trade study results are reviewed relative to allocation of functions between the different segments and impact on operations. Assessments are made of the resulting operational concept refinements and system design relative to their feasibility and supportability. In addition to scrutinizing flight equipment

supportability, the supportability of ground simulators, ground support equipment, and as in the case of ground systems, the sustainment viability of the relative hardware and software elements, are assessed.

The operational readiness process will also examine the related operational infrastructure. If the required infrastructure is not available, then the MA process should assure that those infrastructure requirements are identified and a determination made as to whether they can be acquired in time with programmed resources to support the program. During MAG Phase A, MA will also assure that the system operational modes and states have been clearly identified. A preliminary "day in the life" of the system will be evaluated to assess its logical sequence and associated manning and equipment loading profiles.

As the design progresses through MAG Phases B and C, the operational readiness MA process examines the detailed design to assure that it is suitable and satisfies operational requirements. The degree of autonomy in the detailed design is assessed with regard to the ability of the ground command and control system to intervene in time to support recovery from on-orbit anomalies. Telemetry and other diagnostic aids afforded by the detailed design are evaluated to assure that they are sufficient to assess system and subsystem performance and to take the proper course of action to restore the system to operational capability after experiencing on-orbit anomalies. Also confirmed is the ability of the ground system to functionally verify command execution. As the mission design matures in these phases, MA personnel will assess the resulting system flexibility and ground control functions to permit necessary refinement and evolution of mission functions and performance.

Ground site activation plans for both the ground system and the launch site are formalized during the later part of the design phase and in some cases development is started to enable delivery of the segment vehicles and ground system to the field at the end of MAG Phase D1. During the MAG Phase D1 fabrication and integration, launch site personnel and ground segment operators and support personnel participate in factory acceptance and qualification testing activities to assure the operational suitability of the product being delivered. It also serves as a familiarization of equipment being delivered to the field. The certification of rehearsal and training devices, ground support equipment, which handles service and test flight equipment—is completed during this phase. MA operational readiness would assess

the readiness level of these items demonstrated during these certification activities. The operator is also actively engaged in assessing the graphic user interfaces and often requests refinements during this phase.

At the end of MAG Phase D1, launch base planning and procedural development are completed. MA planning would address the MAG Phase D2 verification tasks that are required to support launch preparation and government's launch certification process. Launch "commit" and abort criteria are developed and refined in MAG Phase D2 and verified under the operational readiness MA process. Launch site procedures are also verified during MAG Phase D2 and placed under configuration management along with associated scripts and test software. Prior to the actual delivery of the flight equipment to the field, MA would assure the readiness of the ground system, procedures, and personnel to receive flight vehicles and ground equipment. At the ground site, mission planning continues with command plans being developed and rehearsals being conducted. As the launch site processing continues, incremental operational reviews are conducted to verify readiness to proceed with the next activity. In support of the test and evaluation master plan, development testing and evaluation would continue at the launch and ground system sites with each new step addressing higher levels of system integration. Finally, at the end of MAG Phase D2, launch preparation operations are conducted. Specific targeted mission parameters are verified along with day of launch placards.

During MAG Phase D3, the actual launch and mission operations are conducted. The operational readiness process would assess operational performance, reconstruct flight system performance, support satellite vehicle checkout and calibration, support anomaly identification and resolution, support post launch reviews and provide continuing support to on-orbit operations.

8.6 Organization of Tasks

The basic task structure, under the operational readiness MA process, is identical to the other process and consists of three parts: program planning, system engineering products and processes, and system segments. The basic organization is shown in Appendix A3. The program planning tasks are in turn subdivided into tasks that assess, from an ORA prospective, current program executability, readiness for associated KDPs, and the adequacy of follow-on RFP. System

engineering product and processes address the system concept of operation, system suitability and effectiveness as well as the identifying specialty engineering task that support the ORA process. The third part, system segments, is organized by the system segment and addresses the allocated operation requirements, the operational design solution, the segment operational suitability and effectiveness, operational planning and supporting equipment, procedure, training and personnel requirements, and final operations.

At the lowest level, specific MA task examples are given. These examples are considered valid MA tasks, but identified as examples as they represent an incomplete set. As the MA task database (Appendix A3) matures, more detailed examples will be added until a complete set is developed. Additionally, the reference guidance and associated checklist will be expanded and provided to govern the execution of the MA tasks. As such, the database should be considered a living document that will mature over time.

8.7 Key Tasks and Associated Objectives

The readiness tasks encompass all the activities required to plan, transport, receive, accept, store, handle, test, deploy, configure, and conduct launch and space vehicles and supporting ground systems. The associated MA tasks include tasks that assess the feasibility of operation requirements, design adequacy relative to operational needs, site activation planning and execution, personnel proficiency and operations. The ORA process tasks directly support SMC's operational safety, suitability, and effectiveness process.

As discussed earlier, the objectives of the ORA process is to guarantee that the material handling of the elements of a system and the interaction of personnel and external equipment with the system itself can be, and are, executed safely and without causing damage to the system or to the handling equipment. In the case of mission control and processing ground systems, the objective is extended to ensure that the integrated system (including hardware and software elements, training and rehearsal devices, procedures, and personnel) can and do conduct successful operations while maintaining vehicle safety and delivering the required services to users. In a broader sense, ORA ensures the overall operability of the system and its operational execution. In practical terms, the ORA execution addresses on one hand the verification of operations procedures in order to make sure that they are consistent with overall system integrity and safety goals,

and, on the other, the validation that the operational execution of these procedures meets their mission intent and preserves actual system integrity and safety.

A number of key tasks are identified, including initial planning activities to assure that infrastructure requirements are clearly identified with specific plans to acquire capability when that capability is not readily available. In this early effort, certification of training devices, rehearsal tools, and simulators should also be addressed. Additionally, the launch site personnel need to become familiar with not only the flight equipment, but also the ground support equipment and associated software being fielded, and if possible, participate in their certification with a valid testing device that will adequately verify flight equipment readiness. Similarly, transport, handling, and servicing equipment need to be verified with regard to maintaining vehicle integrity while performing their intended function.

For ground systems, site activation and transition planning are early operational readiness tasks that need to be accomplished in order to accommodate lengthy installation, checkout, and system development testing cycles. Operational personnel need to become familiar with ground equipment and software, and help to develop training material and operational procedures, command plans, and contingency and backup operations. Operations management and operators need to assess personnel manning levels and the information content of graphic displays in terms of visibility into the flight vehicles performance and status. To support this assessment, early operational assessments should be encouraged and include, if appropriate, the independent operational test and evaluation organization. Before initiating these early tasks, it is important that management roles and responsibilities are clearly defined, especially among the supporting government team (which can involve numerous organizations and agencies). Clear channels of communications need to be established and maintained over the lengthy development cycle with avenues provided to raise and resolve issues.

As the operational processes and procedures are defined, MA operational readiness should identify associated verification points that will eventually become the basis of the government's flight worthiness certification. Combined system-level launch and operation rehearsals should include injection of faults and unforeseen countdown delays to provide opportunities to demonstrate the operational teams' proficiency. The ORA process as identified in Appendix A3 (the MA

verification matrix task database), provides independent assessments based on these rehearsals. At the launch site, the final readiness assessment takes place through pre-launch reviews.

8.8 Government and Contractor Enabling Processes and Products

In order to successfully execute the identified operational readiness MA tasks identified within the database, enabling government and contractor processes and products are required. As discussed in other processes, a basic MA need common to all MAG phases is access to the government's draft and final RFP, the negotiated contract, the capabilities description document, concept of operations (CONOPS), and test and evaluation master plan (TEMP). Operational personnel need to participate in all the stages in requirement and design development as well as during the vehicle qualification and acceptance testing. Access to pre-ship reviews is critical in that the operational community needs to assured that all anomalies and reach-back issues have been resolved and the vehicle is ready to be transported to the launch site.

Similarly, for ground systems, operational and support personnel need to participate in requirements and design development, the formal qualification testing, system-level integration, and site activations. When the system segments are deployed to the field, operational readiness assessments require access to the procedural development, training materials, and operational rehearsal findings, as well as documentation identifying operational-related anomalies and correction actions.

The program integrated master plan (IMP), factory, launch base and system test plans, pre-launch and operation procedures, and the TEMP are important baseline documents to enable the development of detailed operational readiness verification plans. The specific tasks identified in Appendix A3 are general as to be applicable to all space programs. However, in developing operational verification plans for a specific program, the required MA verification tasks are normally specified at a detailed execution level and can be derived from the accomplishment criteria found in the IMP, inspection of the launch base test plans, and the detailed operational procedures.

8.9 References

The policies governing operational readiness assessments can be found in SMC instructions *SMCI 63-1201* and *SMCI 63-1202*, which define the overall operational safety, suitability, and effectiveness process and the space flight worthiness certification, respectively. Additional guidance on operational assessments can be found in USAF instructions AFI 99-102, *Operational Test and Evaluation* and AFI 16-1001, *Verification, Validation and Accreditation*. Aerospace report TR-2004(8583)-1 Rev. A (aka SMC-TR-06-11), *Test Requirements for Launch, Upper-Stage and Space Vehicles*, identifies testing best practices and includes discussion of launch base testing activities. MIL-STD-1833, *Test Requirements for Ground Equipment and Associated Computer Software Supporting Space Vehicles*, is a similar testing on document directed ground support equipment and software. MIL-STD-1472F, *Design Criteria, Human Engineering Standard*, is applicable to ground command and control equipment and ground support equipment. It should be supplemented by software standards found in International Organization for Standardization (ISO).

Policy-related

AFI 99-102	Operational Test and Evaluation, 01 July 1998
AFI 16-1001	Verification, Validation and Accreditation, 01 June 1996
AFI 10-1211	Space Launch Operations, 17 July 2006
AFI 10-1201	Space Operations, 25 July 1994
AFSPCI 10-1208	Spacelift Operations, 01 November 2005

Chapter 9
Mission Assurance Reviews and Audits

Paul Cheng
Mission Assurance Subdivision
Andrew Y. Hsu
Acquisition and Risk Management Office
Dan W. Hanifen
Baseline Systems/Payload
Joseph Statsinger
Retired

9.1 Introduction

The **mission assurance (MA) reviews and audits** process, with the associated process of Lessons Learned, is the most visible manifestations of MA independent technical analysis applied to NSS programs. Table 9.1-1 lists major reviews and audits in the time order in which they are typically conducted in programs. For typically small quantity (e.g., fewer than 10 space vehicles or launch vehicles) NSS programs, and per NSS 03-01[16], the reviews begin during MAG Phase A (concept/architecture development), and continue until the system is operational.

[16] National Security Space Acquisition Policy (NSS) 03-01, "Guidance for DOD Space System Acquisition Process," 12 December 2005. Phase A includes SRR. Phase B includes SDR, PDR, and (optionally) CDR. Phase C includes CDR and all reviews to transport the system from the factory to the launch base, to launch the system, and finally to successfully transition the system into mission operations.

Table 9.1-1, Reviews and Audits

Review or Audit	Phase	Key References	Secondary References
Manufacturing Management/Production Capability Review (MM/PCR)	A	AFMCP 844	
Integrated Baseline Review (IBR)	A	DOD Program Managers' Guide to the Integrated Baseline Review Process	DOD 5000.2-R
		SAF/AQ Policy 94A-015, Sept 94	
Systems Requirements Review (SRR)	A	MIL STD 1521C	Aerospace TOR-2004(3909)-3360
			MIL STD 499B
		NSS 03-01	
		SMCI 63-1202	
System Design Review (SDR)	A	MIL STD 1521C	Aerospace TOR-2004(3909)-3360
		NSS 03-01	
		SMCI 63-1202	
System Design Review (SDR)	A	MIL STD 1521C	Aerospace TOR-2004(3909)-3360
		NSS 03-01	
		SMCI 63-1202	
Preliminary Design Audit (PDA)	B	Aerospace TOR-2004(3909)-3360	Aerospace TOR-2005(8617)-4204
Preliminary Design Review (PDR)	B	MIL STD 1521C	Aerospace TOR-2004(3909)-3360
			Aerospace TOR-2005(8617)-4204
		NSS 03-01	
Critical Design Audit (CDA)	C	Aerospace TOR-2004(3909)-3360	Aerospace TOR-2005(8617)-4204
Critical Design Review (CDR)	C	MIL STD 1521C	Aerospace TOR-2004(3909)-3360
			Aerospace TOR-2005(8617)-4204
		NSS 03-01	
Manufacturing/Production Readiness Review (PRR)	D1	MIL STD 1521A	MIL STD 1521C
			SMCI 63-1202
Test Readiness Review (TRR)	D1	MIL STD 1521C	MIL STD 1540

Review or Audit	Phase	Key References	Secondary References
		SMCI 63-1201	MIL Hdbk 340
		SMCI 63-1202	MIL STD 810
			Aerospace TOR-2003(8583)-1
Formal Qualification Review (FQR)	D1	MIL STD 1521C	MIL STD 1540
		SMCI 63-1202	MIL Hdbk 340
			MIL STD 810
			Aerospace TOR-2003(8583)-1
System Verification Review (SVR)	D1	MDA-QS-001-MAP	
Hardware Acceptance Review (HAR)	D1	SMCI 63-1203	Aerospace Pedigree Reviews, briefing by K. Ganz and D. Helgevold, 19 September 2000
Functional Configuration Audit (FCA)	D1	MIL STD 1521C	
Physical Configuration Audit (PCA)	D1	MIL STD 1521C	Aerospace TOR-2004(3909)-3360
Pre-Ship Review (PSR)	D1	MIL STD 1521C	SMCI 63-1204
Independent Readiness Review Team (IRRT)/ Mission Assurance Team (MAT)	D2	SMCI 63-1201	SMCI 63-1203
		SMCI 63-1204	
Mission Readiness Review (MRR)	D2	SMCI 63-1201	SMCI 63-1203
		SMCI 63-1202	
		SMCI 63-1204	
Aerospace President's Readiness Review (APR)	D2	SMCI 63-1201	SMCI 63-1203
		SMCI 63-1202	
		SMCI 63-1204	
Flight Readiness Review (FRR)	D2	SMCI 63-1204	SMCI 63-1201
			SMCI 63-1202
			SMCI 63-1203
Launch Readiness Review (LRR)	D2	SMCI 63-1204	
Post Flight Review (PFR)	D3	SMCI 63-1204	SMCI 63-1203
		SMCI 63-1201	
		SMCI 63-1202	

Program reviews entail a tremendous amount of detailed engineering and programmatic efforts. Not only do the reviews make it possible for the interfaces and composite performance to be understood, they also establish a schedule imperative with entrance and exit criteria that synchronizes the government and contractor expectations. The reviews permit the MA experts to work in concert with program development resources and within the program's chain of command to fulfill their roles.

The review process also entails lesson learning. A Lesson Learned is understanding gained by experience—either positive (as in a successful test or mission), or negative (as in a mishap or failure). Sharing lessons from the NSS program—i.e., to identify, communicate, and record good practices and adverse experiences with implications broader than localized corrective actions—is an important MA mechanism that benefits the future work of the organization, especially in the prevention of recurrence of accidents.

Relevant experiences can be drawn both vertically and horizontally: at each stage of the program, the system program office (SPO) needs to extract experiences from legacy programs and earlier phases of the current program, as well as to seek cross-program wisdom. Senior NSS leadership has emphasized the importance of cross-program learning lessons, and demanded the creation of a formal system to facilitate lesson learning and sharing across the NSS enterprise, as a part of the Launch Vehicle Board Area Review (BAR) actions. Formal lesson learning is also required as a part of the SMC OSSE process (SMCI 63-1201).

In response to the BAR and SMC tasking, The Aerospace Corporation has developed a process to collect and validate lessons from a wide variety of sources. Aerospace has prepared numerous *Lessons Learned* volumes that, together with numerous validated lessons from other sources such as NASA, are made available to program office and engineering personnel who are supporting any potentially affected program activities. The process by which Aerospace cross-references, validates, and configurationally manages lessons is outside the scope of this chapter, but lesson sharing across the NSS enterprise can be sustainable only if all programs diligently collect, assess, document, and infuse pertinent lessons at every phase (Figure 9.1-1).

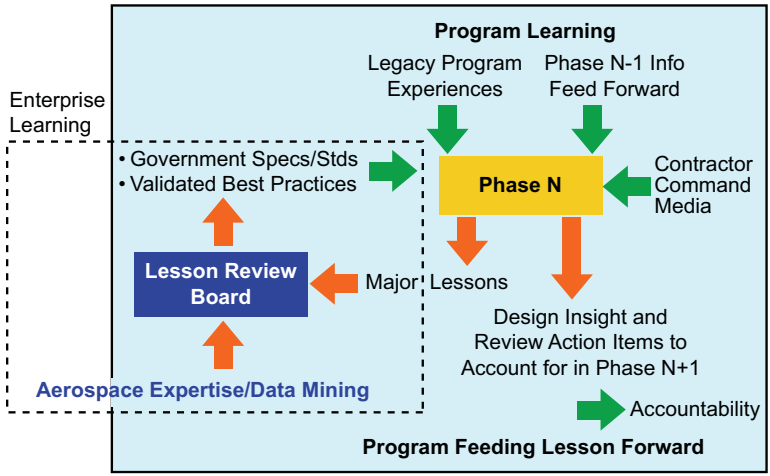


Figure 9.1-1, A Closed-loop Learning Process

9.2 Definitions

Three categories of MA reviews are considered in this guide: technical reviews, audits, and mission and launch readiness reviews. **Technical reviews** are activities accomplished by technical experts established to exhaustively investigate the state, status, and performance of units, subsystems, and systems throughout the design, development, production, and test phases to uncover risks and issues, and to recommend steps to resolve risks/issues affecting mission success. **Audits** are independent inspections of each configuration item (CI) or process conducted by discipline or subsystem experts within a system to ensure that functional characteristics and physical attributes comply with relevant specifications, standards, and concepts of operations (CONOPS). **Readiness reviews** are used as formal gates to approve transition to operational status (flight or mission) of the space vehicle or launch vehicle once system integration is completed and the government program office and launch/mission operations personnel are satisfied that all requirements that can be verified prior to launch have been (including documentation), and that personnel have been trained, certified and available to support the operation.

Lessons Learned are typically concise storytelling reflecting on "what we did wrong" (e.g., this satellite failed because its grounding scheme had a hidden flaw) and "what should have been done differently." Lessons Learned also encompasses "**best practices**" and "**best-of-the-**

breeds." The term "best practice" usually refers to a process that has worked well and is therefore recommended (e.g., spacecraft grounding should be set up and executed in a specific fashion), especially if the NSS enterprise has validated it. "Best-of-the-breed" are processes that have been used before (for example, a Milstar bus grounding policy) and are presented with the expectation that the users will carefully scrub them before adaptation. All three items can have a wide scope, but only those associated with MA—particularly those involving correction of deficiencies and improvement of performance—are discussed here.

9.3 Objectives

Technical reviews ensure that:

- The requirements are properly defined and allocated to configuration items
- The CONOPS is acceptable and meets the needs of the users
- The design(s) is (are) capable of being built in the projected time and satisfies stated requirements
- All internal and external interfaces are clearly defined, complete, and verifiable
- A program baseline is established whose requirements can be verified in the projected time
- Contractor risk assessments are complete and proposed corrective actions adequate and doable
- The contractor's design, risk, cost, schedule, and/or resource information is visible and available
- Test planning supports the "pyramid test philosophy," "test as you fly," and system-level testing and test flows
- The end of line unit to unit deviations are acceptable

Audits assure that:

- The CI as-built version is according to the specifications, physical layouts in drawings, and manufacturing processes and procedures
- The tests were adequately defined, scoped, and executed to verify that the test article's performance and interfaces comply with requirements and specifications

- The specifications, technical data, engineering drawings, design documentation, quality control records, and manuals adequately describe the product baseline

Readiness reviews assure that:

- The flight system and/or facilities, procedures, and personnel are ready to conduct mission operations and the risks, liens, and workarounds are acceptable
- The system may be operated in an operationally safe, suitable, and effective manner
- The baseline has been maintained throughout its operational life
- The system has been verified and the residual risk is acceptable to commence launch processing and final launch preparations
- The vehicle is flight worthy

Lesson learning ensures that:

- Retention and dissemination of critical knowledge gained from diverse sources are accomplished
- Mistakes are not repeated and wheels are not reinvented
- Proper MA policies and practices are established and highlighted

9.4 Practices and Tasks

The following reviews are generally followed[17] but the scope and focus may vary. For example, depending on the size of the contract and risk, the systems requirements review (SRR) and the systems design review (SDR) may be held together following contract award. The design-oriented reviews (e.g., preliminary design review (PDR) and critical design review (CDR)) are primarily unit and subsystem oriented while the mission and launch readiness reviews are system oriented.

[17] MIL-STD-1521, "Technical Reviews and Audits for Systems, Equipments, and Computer Software," 04 June 1996 and Aerospace TOR-2002(3105)-1668, *Acquisition Strategy Considerations*, 31 March 2002.

9.4.1 Technical Reviews[18]

9.4.1.1 Manufacturing Management/Production Capability Review (MM/PCR)[19]

An MM/PCR is conducted during source selection by the government program office at the prospective contractors' facilities to evaluate competing contractors' capability to meet all immediate and future production requirements of proposed systems.

9.4.1.2 Integrated Baseline Review (IBR)

The IBR provides a mutual (government, contractor program manager) understanding of the inherent technical and programmatic risks in the contractor's plans, the underlying management control systems, and the required resources to reduce risks to an acceptable level. An IBR also examines consistency among technical, schedule, cost, resource and management risks. IBRs are generally conducted within three months after every program key decision point (KDP) and called for by the government program manager as part of his/her risk management approach. Those risks identified during the IBR should be reviewed and mitigation plans incorporated into risk management planning.

9.4.1.3 SRR

The SRR determines if the contractor's efforts to understand and translate mission requirements into system requirements and operations concept was adequate, and establishes a formal system requirements baseline down to the element level. This includes summarizing significant potential and known program risks and potential risk mitigation strategies, identifying interfaces with and impact to other systems, describing development and operational test approaches, and addressing the producibility of the proposed design concept. The SRR is generally conducted once per program after a significant number of systems functional requirements have been defined and allocated to appropriate CIs and a significant amount of requirements analysis has been completed. This activity is conducted by the contractor and is

[18] MIL-STD-1521B, "Technical Reviews and Audits for Systems, Equipments and Computer Software," 04 June 1996, Appendices A, B, D, E, I, K. Note that the schedule for software reviews may lag that for hardware reviews to allow hardware design to stabilize before the start of software development.
[19] MIL-STD-1528A, "Manufacturing Management Program," 09 September 1986, page 4.

generally completed within MAG Phase A (concept exploration) or, at the latest, soon after development contract award (MAG Phase C).

9.4.1.4 SDR

The SDR evaluates the contractor's approach for optimization, correlation, completeness, and risk mitigation associated with the allocated technical requirements of the identified CIs and the established system design specification baseline. The SDR also includes examinations of the system functional requirements, external interface control requirements, and preliminary system verification plan. A review of the systems engineering process that allocated the technical requirements and the engineering plan for the design and development phase is also conducted. Basic manufacturing considerations and the production-engineering plan will also be reviewed as consideration of design producibility. Careful examination is conducted of all medium- and high-priority risks from assembly level to segment level, and their reflection to the system level along with companion mitigation strategies.

9.4.1.5 PDR

The PDR evaluates the contractor's technical adequacy, progress, and risk resolution for the selected design-to approach for all CIs, and establishes a CI design baseline down to the assembly level. The PDR demonstrates design compatibility with the performance and engineering specialty requirements of the hardware development specifications. Included is an evaluation of technical risks associated with the manufacturing process/methods and the establishment of the compatibility of the physical and functional interfaces among and between CIs (e.g., units, subsystems, or system), facilities, computer software configuration items (CSCIs),[20] and personnel. The PDR processes allow for an engineering assessment of the technical adequacy of top-level design, testing approach, and CONOPS. PDRs are normally conducted once per program for each CI at the assembly level, subsystem, element, and segment building to the system level as appropriate.

[20] Computer software configuration item (CSCI).

9.4.1.6 CDR

The CDR evaluates the contractor's detailed system design and the detailed build-to design for each CI (e.g., CSCIs, units, subsystems, or system) to determine if each design meets the allocated functional, performance, and engineering specialty requirements. The CDR also is used to evaluate whether the design can be produced and verified[21], has interface compatibility between CI/CSCIs, facilities, and personnel, and that all risks have been identified, rated, and satisfactory mitigation plans established. CDRs are normally held once per program during MAG Phase C for each CI (assembly level), subsystem, element, and segment building to a system level, as appropriate.

9.4.1.7 Test Readiness Review (TRR)[22]

The TRR examines the contractor's progress and status for each CI/CSCI to determine whether hardware and software procedures are complete and the contractor is prepared to start testing. The results of any informal testing and changes to the CONOPS are also reviewed.

9.4.1.8 Formal Qualification Reviews (FQR)

An FQR evaluates the test, inspection, or analytical results by which a group of hardware configuration items (HWCIs)/CSCIs comprising a system is verified to have met specific performance requirements (specifications or the equivalent). This review does not apply to hardware or software verified at functional configuration audit (FCA) for individual CIs.

9.4.1.9 Production Readiness Review (PRR)

The PRR evaluates the contractor and the contractor's design readiness to begin manufacturing.[23] The PRR is conducted by the government

---

[21] The system level is usually validated by simulation due to verification limitations.

[22] TRR as documented in MIL-STD-1521B (page 5) is for formal software testing of CSCI. The definition here has been generically expanded to include both hardware and software since it is felt the description was generically written and could be extended to hardware with minor changes. FQR also expands the definition of FCA to include both hardware and software.

[23] Per MIL-STD-1528A, "Manufacturing Management Program," 09 September 1986, "Manufacturing is the conversion of raw materials into products or components through a series of processes. Manufacturing includes manufacturing planning, tool design, scheduling, manufacturing engineering, material procurement, fabrication, assembly, test,

program office and supported by the contractor. The PRR is held incrementally (generally three sessions–two preliminary and one final) during full-scale development. This review is intended to determine if the issues, risks, and corrective actions for manufacturing have been satisfactorily resolved prior to a production go-ahead decision. As the design matures, the review become more focused and refined dealing with production planning, facilities, allocation, identification and fabrication of tools/test equipment, long lead acquisitions, and the incorporation of producibility-oriented changes.

9.4.1.10 System Verification Review[24](SVR)

The SVR incrementally demonstrates that the total system (personnel, products, and processes) is verified to satisfy requirements in the functional and allocated configuration documentation and to confirm readiness for production, support, training, operations, subsequent verifications, additional development, and disposal. The SVR determines if the system produced is capable of meeting the technical performance requirements established in the specifications and test plans.

9.4.1.11 Hardware Reviews

Acceptance reviews can be informal or formal reviews chaired and presented by the contractor. Formal reviews are sometimes called hardware acceptance reviews or buy-off reviews with the objective of verifying that all hardware, parts, materials, and components have been manufactured and tested in accordance with current design documentation, test procedures, and related documentation prior to government acceptance via a DD-250 and/or delivery to the next highest level assembly or to the launch site. The manufacturing, inspection, and acceptance verifications plus hardware pedigree status are the principal inputs to this review. The team reviews all acceptance test data, and any perceived shortcomings are investigated. The responsible test engineers are available to explain how the test was conducted and anomalies were resolved.

Independent pedigree reviews by a government team often supplement contractor-led acceptance reviews and focus on individual critical

---

packaging, installation and checkout, product assurance and determination of resource requirements throughout systems acquisition."

[24] The definition is documented in the Missile Defense Agency Mission Assurance Plan (MAP), MDA-QS-001-MAP, 09 January 2004, para. 3.4.1.8, page 53.

components and subsystems to establish that the as-built hardware agrees with its design and manufacturing requirements and is not "out-of-family" with predecessors. The pedigree includes a review of manufacturing and quality assurance documentation to verify documented procedures and processes were followed, that any out-of-sequence work maintained the product's integrity, engineering changes were proper, deviations and "use as is" material review board decisions were adequately justified, and whether new processes, materials, or design changes were made that did not violate the product's qualification status. The pedigree also includes an assessment of acceptance testing to ensure procedures were followed, deviations were justified and the root cause of noted test discrepancies was identified with the appropriate corrective action taken.

9.4.2 Audits[25]

Formal development and manufacturing audits are described below. Informal, planned or ad hoc, audits are covered in Chapter 5.

9.4.2.1 Functional Configuration Audit (FCA)

The FCA is a formal audit conducted by the government program office and supported by the contractor to demonstrate that hardware and/or software CIs have been achieved. This audit examines the CONOPS, test plans, analysis and inspection reports, as-used qualification test procedures, test data, test reports, drawings, and other supporting documentation. An FCA is conducted on either the first production unit or a pre-production representative of the configuration to be released as an operational production unit. The final FCA occurs at the completion of CI qualification testing.

9.4.2.2 Physical Configuration Audit (PCA)

The PCA is a formal audit conducted by the government program office and supported by the contractor. The PCA technically examines subject CIs to verify that each CI "as-built" conforms to the technical documentation defining the CI in order to establish the product baseline. A complete PCA is done on the first production unit and is not repeated unless significant engineering changes and resulting

[25] PCA and FCA definitions are found in MIL-STD 1521B, "Technical Reviews and Audits for Systems, Equipments, and Computer Systems," 04 June 1996, Appendices G and H, pp. 71-82.

modifications to the CI have occurred. Customer formal acceptance of product specification and successful completion of the PCA results in the establishment of the product baseline. The PCA includes a detailed examination of engineering drawings, specifications, technical data, acceptance test procedures and test data, design documentation, and all operational support documentation (e.g., user manuals, diagnostic manuals, and firmware support manuals).

9.4.2.3 Preliminary Design Audit (PDA)

PDAs are working-level meetings between the government program office team and the contractor prior to the program's formal PDR milestone. PDAs address design thoroughness (ability to meet all functional, performance, and interface requirements from the system to the CI level) in specific functional areas, units, or subsystems, and are milestones on the program's detailed schedule. For complex NSS systems, successful PDAs represent entrance gates to the formal PDR. A series of detailed technical meetings between the contractor, subcontractors, suppliers, and government program office constitutes a single PDA. PDAs are held for each CI (assembly level), subsystem, element, and segment building to the system level, as appropriate. The PDA process allows for very detailed design investigations to ensure requirements can be satisfied, identifies faults/failure modes and plausible mitigation approaches, examines relevant risk mitigation plans and progress, and identifies issues that need to be resolved before the formal PDR. PDAs are normally held once per program prior to the formal PDR in MAG Phase C.

9.4.2.4 Critical Design Audit (CDA)

CDAs are detailed technical working-level meetings between the government program office, the contractor, the subcontractors, and the suppliers prior to the program's formal CDR milestone. For complex NSS systems, CDAs are held for each CI (assembly level), subsystem, element, and segment build to the system level, as appropriate. CDAs address design thoroughness (the ability to meet all functional, performance, and interface requirements from the system to the CI level), risk reduction, and verification and test planning for each level of assembly under examination. During detailed CDA engineering interactions, confidence is gained that the design trades are completed, the final design is complete and producible, and the design has been documented for manufacturing or procurement to begin. Successful completion of each CDA will ensure that all outstanding problems,

issues, and risks have appropriate work-off plans. Successful completion of each CDA is an entrance criterion for the program's formal CDR milestone. CDAs are normally held once per program prior to the formal CDR during MAG Phase C.

9.4.3 Readiness Reviews

Readiness reviews provide a formal mechanism that supports the decision-making process by forcing a careful examination of all elements of the system at key maturity milestones relative to final integration, testing, and operator proficiency, including outstanding problems or liens, in preparation for launch. Key decision points (KDPs) include the decision to ship the launch and/or space vehicle to the launch site from the factory; the decision to proceed with vehicle erection on the launch pad; and the decision to proceed with the launch after successfully completing launch integration and processing, successfully demonstrating end-to-end mission connectivity, and successfully demonstrating personnel proficiency through rehearsals. Post-launch reviews are also included to assess flight performance and gather lessons learned.

9.4.3.1 Independent Readiness Review Team (IRRT)

IRRT reviews are independent, technical examinations of space vehicle and/or launch vehicle risks beginning approximately one to two years prior to launch. These reviews are conducted by a core team, augmented as needed to provide a complete set of discipline and subsystem experts from Aerospace, system engineering and technical assistance (SETA), government, and contractor personnel.

The reviews provide technical assessments of the space vehicle or launch vehicle, identify increased risks beyond the established mission baseline to safety or mission success, recommend risk mitigation or confidence-enhancing steps, and evaluate all open issues and the acceptability of all indicated closure paths. The reviews are done incrementally with the final review occurring before launch. As such, the extent of each review is negotiable depending on the hardware/software design and development stage of the program, hardware/software performance history, and resources available for the review, changes since the last review and the scope of the last review. The timing of final IRRT activity should provide sufficient time for a complete review and for any corrective actions to take place and critical recommendations implemented.

9.4.3.2 Mission Readiness Review[26] (MRR)

The MRR is a formal review organized by the spacecraft single manager (SM) to evaluate the readiness of the spacecraft before final launch integration activities are initiated. The mission director, launch program SM, and appropriate launch base detachment commander may choose to attend. Program and support organization personnel conduct the MRR, which is supported by the appropriate contractors. Findings and deficiencies should be corrected or disposed of before the flight readiness review (FRR) one to two days before launch. The MRR addresses all system components of mission readiness, including status of flight hardware (spacecraft, launch vehicle, upper stage), launch and support facilities, range and orbital operations, ground station operations, and the readiness and training of all personnel, including customer elements processing mission data. Successful completion of the MRR results in a decision to ship the launch vehicle or space vehicle to the launch base to begin launch processing (i.e., "consent to ship").

9.4.3.3 Aerospace President's Readiness Review

In support of the SMC commander's FRR (see the following paragraph), the president of The Aerospace Corporation conducts his own objective review of the space and launch vehicles' readiness to support the designated mission. Both the Aerospace program offices and the IRRT present their findings during this review and support more detailed technical discussions on specific issues, as required by, prior to, during, or subsequent to the president's formal review. Aerospace corporate vice presidents of the appropriate Space Launch Operations, Space Program Operations or National Systems Group, or Engineering Technology Group support the president's review. In accordance with SMCI 63-1201, the president presents his findings to the SMC commander during the FRR and participates in the readiness poll.

9.4.3.4 Pre-ship Review (PSR)

The program conducts hardware PSR to assure that flight hardware and components, software, ground support equipment, and procedural documentation are ready to ship to the deployment site. Operations

[26] SMCI 63-1201, "Assurance of Operational Safety, Suitability, & Effectiveness for Space and Missile Systems," para 3.4.4.3, page 14, 21 May 2001.

personnel participate in this review. This type of review is meant to identify any open issues affecting deployment and subsequent operations, verify that planning is in place to close-out these issues in a timely manner, and verify supportability of the program's ensuing activities. Operations personnel ensure sufficient coordination between the system contractor and Range/launch site (and/or any other receiving site), to assure that the latter is ready to receive program hardware, receiving support has been appropriately scheduled, and receiving facilities are prepared to support hardware arrival and post-shipping inspection activities.

9.4.3.5 FRR[27]

The FRR is a formal review organized and coordinated with applicable government program offices and presented to the SMC commander (or designated representative) by the mission director and supported by the launch base and appropriate contractors. The FRR evaluates the space flight worthiness of the integrated flight hardware (space vehicle, upper stage and launch vehicle) approximately one to three weeks before launch. It also addresses the readiness of launch and support facilities (ground systems), range and orbital operations, and the readiness and training of the operating personnel. The review includes a safety verification of the integrated system.

The objective is to ensure the prime contractors, The Aerospace Corporation, the spacecraft program office, launch programs, and the SMC commander agree that the launch vehicle is flight worthy and ready to begin final launch operations. Other inputs to the FRR include the IRRT reviews, the contractor and Aerospace president's reviews, and detailed briefings by both the spacecraft and launch program teams. At completion of the FRR, the SMC commander will assess and may certify space flight worthiness of the integrated system for USAF space missions. For USAF-managed space and launch vehicles in support of non-USAF customers, the SMC commander will be responsible for approving the SM's certification. For selected critical missions, the SMC commander will follow-up with an executive mission readiness report (EMRR) to Air Force senior leadership. The FRR is conducted after the launch vehicle and spacecraft are integrated, approximately one to two weeks before launch.

[27] SMCI 63-1201, "Assurance of Operational Safety, Suitability, & Effectiveness for Space and Missile Systems," Appendix D, pp. 13-14, 21 May 2001.

9.4.3.6 Launch Readiness Review (LRR)

A LRR is an operations readiness review organized by the Launch Decision Authority (i.e., launch base wing commander, or the Launch Processing Agency when a non-Air Force Space Command launch site is used) and supported by the appropriate contractors. It is conducted following the integrated launch and space vehicle systems test one or two days before launch. The LRR process provides a summary pre-launch assessment of the readiness status of the total system (space and launch vehicle), the launch facility, range safety and instrumentation, the Air Force Satellite Control Network, the operational mission control station, operations personnel, and other launch or on-orbit support. Launch Decision Authority also verifies the closure of issues and items and determines the readiness status of safety, training, weather, and recovery teams.

9.4.3.7 Post-flight Review (PFR)

A PFR is conducted for all missions requiring a MRR and the results are presented to the single manager who chaired the MRR. It is intended as a top-level summary predicated on post-launch, in-depth assessments conducted by the space vehicle program manager, launch vehicle program manager, and appropriate payload mission managers. The PFR typically covers the time from the MRR through early on-orbit operations. The PFR addresses pre-launch ground operations, launch operations, mission and space vehicle operations, the launch vehicle, the space vehicle, critical ground systems and interfaces, and the payload user's ground interface to receive and process mission data. The PFR captures all Lessons Learned from the mission and provides both feedback and schedule imperative to the government program office to implement Lessons Learned before the program office's next mission. PRRs are held approximately 60 days after launch and early on-orbit testing is completed.

9.5 Strategies and Execution by Phase

The major reviews and audits described in the Mission Assurance Verification (MAVM) task database include those called for in NSS 03-01 (Figure 9.5-1); SMC policies (Horejsi, 2004), (Horejsi, SMCI 63-1202 Space Flight Worthiness, 2004), (Horejsi, SMCI 63-1203 Independent Readiness Review Team, 2004), (Horejsi, SMCI 63-1204 SMC Readiness Review Process, 2004); and MIL-STD-1521. Not all

the reviews and audits are necessary for every program: the program manager decides which are appropriate.

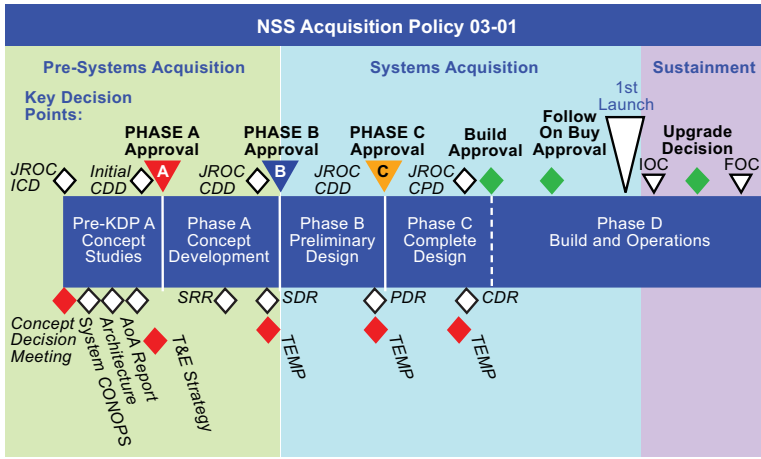


Figure 9.5-1, NSS 03-01 Program Phases and Key Events

9.6 Organization of Tasks

The tasks in the MAG database are organized by phases according to program planning and systems engineering tasks. The complexity and heritage of the program dictate to what extent design reviews for lower-level subassemblies (for example, whether the solar array should be reviewed separately from the EPS review) are warranted.

9.6.1 Objectives Associated with Reviews and Audits

Several objectives are accomplished by performing the needed reviews and audits of an NSS program:

- In Phase 0, assure that the program concept and timeline are adequately defined to issue a draft capabilities development document (CDD) and independent program summary (IPS) as well as a draft request for proposal (RFP), (statement of work (SOW), contract data requirements list (CDRL), data item descriptions (DIDs), etc. to prospective contractors. This is critical to ensure that MA has the necessary information to conduct independent assessments.

- In Phase A, it assures that the program's architecture and requirements are adequately defined to proceed to preliminary design work. This is achieved by verifying that, among others, the IBR, SRR, and SDR are adequately passed.
- In Phase B, the tasks assure that the requirements have been properly flowed down to all levels of the work breakdown structure (WBS) and that they will be met by the design by verifying the PDAs and reviews. Entrance gates for future major reviews are defined to prevent reviews if the contractor is ill-prepared.
- Phase C reviews share the same objectives as in Phase B, but at a more detailed level. CDAs, the system design and manufacturing readiness incremental spaceflight worthiness review, and the CDR work to assure that the design will meet requirements.
- In Phase D1, the tasks assure that the hardware is fabricated as designed, testing is properly planned and executed, and the hardware actually performs as intended under testing. Major objectives that must be verified include TRRS, FQRs, PRRs, FCAs, and PCAs.
- In Phase D2, the tasks assure that all open technical issues are closed and the space vehicle is ready for launch. Reviews that must be passed include the SVR, MRR, LRR, and several Aerospace independent reviews.

9.6.2 Objectives Associated with the Lessons Learning Process

Lesson learning itself is a continuous process. Detailed instructions for lessons learning activities required of a program at each phase and review are described, for example, in the SMCI 63-1201. Each MA-supporting discipline requires specific lesson learning, as set forth below.

The tasks related to the Lessons Learned process are largely to ensure that lesson learning is conducted in all phases:

In Phase Pre-KDP A, the objective of lesson learning is to ensure that the new program fully understands the challenges involved in setting requirements, matching resources, developing architecture, and formulating acquisition strategy. Programs typically exhibit excessive optimism in early planning, and a study of legacy program execution experiences provides a reality check.

The specific lesson learning tasks include collecting legacy program schedule, budget, and technical performance; analyzing discrepancies in cost/schedule performance vs. goals; and incorporating applicable insights in defining acquisition strategy. Planning for the new program should make provision for all known hurdles such as risks in developing certain technology and major testing snafus.

Lessons Learned implementation in early program phases emphasizes learning of existing lessons. Nevertheless, programs should begin lesson generation activities by documenting issues, successes, and other findings useful to the project's subsequent phases and preventing nonconformances from recurring. In particular, the program needs to extract lessons pertaining to systemic issues worthy of communicating to the customer agency. Support is available from Aerospace in making the submissions interesting, technically sound, and obvious to an outside reader.

In Phase A, the objective of lesson learning is to ensure that the program's architecture and requirements are properly set, and that adequate contractor assessment has been performed. Numerous on-orbit anomalies have been traced to requirements not set forth during early program formulation. Unrealistically set technical requirements have also resulted in excessive, sometimes unnecessary, cost.

The path to lesson learning involves analyzing the legacy program's requirements, key performance parameters (KPPs), designed-to specifications, and flight performance, and incorporating applicable insights in defining KPP and designed-to specifications. The MA process needs to ensure that the new program has scrutinized top-level legacy specifications (in particular, waivers to the legacy program's requirement should not be granted just because the need was not apparent). Planning should include lessons on ground segment capability, development history, and reusability; "heritage equipment" issues, organizational issues (for example, government-furnished equipment or convoluted teaming), and any other legacy program's lessons, if documented.

The program should:

- Review lessons from Pre-Phase A activities
- Require contractors to develop Lessons Learned programs, incorporating appropriate lessons from the contractor's

Lessons Learned system (since the contractors are already involved in Phase A)
- Assess past technical and acquisition performance of the contractor (in particular, all flight anomalies of a "standard bus" proposed for the program)
- Understand applicable specifications, standards (including tailoring methodology), best practices, and validated lessons, particularly as documented in the *Space Vehicle Systems Engineering Handbook*, TOR-2006(8506)-4494

The program should also document issues, successes, and other findings, particularly those useful to the customer agency and to the project's subsequent phases.

In Phase B, the objective of lesson learning is to ensure that the requirements have been flown down and will be satisfied at the preliminary design level. Many anomalies had occurred because the requirements were improperly stated, the supposedly heritage design did not work as expected, and the interface was not properly handled.

Lessons learning activities in Phase B amount to making sure proper functional analysis practices are used and good technical baseline housekeeping rules are followed.

The program should:

- Review lessons from Phase A activities and appropriate lessons from the contractor's Lessons Learned system
- Assess applicable specifications, standards (including tailoring methodology), best practices, and validated lessons,, particularly as documented in the *Space Vehicle Systems Engineering Handbook*, TOR-2006(8506)-4494, and sections 1, 2, 3, and 6 of *100 Questions for Technical Review*, TOR-2005(8617)-4204
- Oversee the contractor's implementation of Lessons Learned programs
- Ensure that an occurrence reporting system is developed, maintained, and implemented
- Participate in NSS-wide sharing of Lessons Learned activities by systematically documenting issues, successes, and other findings useful to the customer agency and to the project's subsequent phases

In Phase C, the objective of lessons learning is to ensure the detailed design is appropriate. Most detailed design activities are discipline-specific. However, engineering mistakes not only cause most flight failures, but also tend to recur. MA activities should strive to use past failures as lessons to catch engineering mistakes.

The program should review:

- Lessons from Phase B activities
- Appropriate lessons from the contractor's Lessons Learned system
- Applicable specifications, standards (including tailoring methodology), best practices, and validated lessons,, particularly as documented in the *Space Vehicle Systems Engineering Handbook*, TOR-2006(8506)-4494, and section 3, 4, and 5 of *100 Questions for Technical Review*, TOR-2005(8617)-4204
- Discipline-specific lessons, such as NASA Mechanism lessons and Electronic Systems Branch Design lessons (both available online).

As in earlier phases, the program should also document issues, successes, and other findings, particularly those useful to the customer agency and to the project's subsequent phases.

In Phase D1, the objective of lesson learning is to ensure the equipment will be produced as designers intended, verified properly, and meet requirements. Many failures have occurred because equipment developed latent defects during manufacturing, was tested in an incorrect configuration, suffered damage due to an excessive test environment, or passed verification with design errors undetected.

Lesson learning activities in Phase D1 involve making sure the manufacturing process matches the design requirements and is compatible with the flight environment (e.g., certain items such as cadmium plated parts cannot be use in space); eliminating mishandling and contamination; catching latent deficiencies; conducting the test in a perceptive and safe manner, and reviewing the test results carefully.

The program should:

- Study lessons through Phase C and appropriate lessons from the contractor's Lessons Learned system

- Review manufacturing- and test-related lessons in sections 7 and 8 of *100 Questions for Technical Review*, TOR-2005(8617)-4204, and in the *Space Vehicle Test and Evaluation Handbook*, TOR-2006(8546)-4591
- Evaluate major factory problems and flight anomalies in the legacy program (described in the failure review board (FRB) minutes, flight readiness review packages, and post-flight reports) to preclude running into similar trouble
- Ensure lessons from earlier phases are followed by addressing all previously booked technical concerns
- Document material review board (MRB) and FRB anomalies and address corrective actions
- Feed lessons forward to space vehicle/launch vehicle integration, and operation, including information to ensure proper rework and retest, that the flight configuration is properly verified, and that the Orbit Operational Handbook documents necessary workarounds
- Provide lessons to government as candidates for future specifications and standards by presenting issues, successes, and other findings to the customer agency including FRB trend analysis and annotation on all important FRB items

In Phase D2, the objectives of lesson learning are to make sure the space is ready for launch, and to improve follow-on vehicles by completing the learning loop. Space programs are expensive in part because the community is deficient in knowledge reuse. Launches have also failed because anomalies that did not compromise a mission were ignored, even though in retrospect the mission success was purely a matter of luck and the next mission could easily fail.

Lesson learning activities in Phase D2 primarily involves analyzing and documenting launch preparation and flight experiences. Most importantly, post-flight reviews must be thorough—anomalies cannot be dismissed simply on the basis of “in-family” or “no flight impact.”

The program should:

- Compile comprehensive program lessons to be incorporated in the contractor’s command media and in the government’s knowledge base
- Determine the root cause of all flight anomalies
- Feedback lessons to design and functional areas and ensure correct reachback, reachforward, design change, test

procedure change, and other corrective actions are taken (SMCI 63-1201 prescribes lesson activities associated with each review)

9.7 Government and Contractor Tasks and Products

See the MAVM task database for the associated enabling tasks for each task. Key government and contractor enabling tasks are as follows for each phase:

	Government Enabling Tasks	Contractor Enabling Tasks
Phase 0	SOW, CDRL, integrated program summary (IPS), draft acquisition decision memorandum (ADM) Common criteria, measures of effectiveness to evaluate concept studies	
Phase A	IBR IPS, ADM	IBR, SRR, SDR
Phase B	PDR entrance criteria Completion of PDAs	Completion of PDRs Completion of PDAs
Phase C	CDR entrance criteria Completion of CDAs	Completion of CDRs Completion of CDAs
Phase D1	Completion of Phase D1 Technical Reviews (e.g., TRR, FQR, PRR) Completion of Phase D1 technical audits (e.g., PCA, FCA) IRRT assessments	Completion of Phase D1 technical reviews Completion of Phase D1 technical audits
Phase D2	Completion of technical reviews (e.g., SVR, MRR, LRR, FRR, PSR, IRRT assessments)	Completion of technical reviews

9.8 References

Policy-related

SAF/AQ Policy 94A-015

SMCI 63-1201	Assurance of Operational Safety, Suitability, and Effectiveness for Space and Missile Systems, 21 May 2001
SMCI 63-1202	Space Flight Worthiness
SMCI 63-1203	Independent Readiness Review Team

SMCI 63-1204	SMC Readiness Review Process
NSS 03-01	National Security Space Acquisition Policy, 12 December 2005

Specifications and Standards

MIL-STD 1521C	Technical Reviews and Audits for Systems, Equipments, and Computers

Handbooks

DOD Program Manager's Guide to the Integrated Baseline Review Process, April 2003

Best Practices

Aerospace TOR-2004 (3909)-3360 Rev. 1	*Systems Engineer's Major Reviews for National Security Space System Programs*, 02 February 2005
MIL-STD-499B	Systems Engineering, draft dated 06 May 1994
Aerospace TOR-2002 (3105)-1668	*Acquisition Strategy Consideration,* 31 March 2003
Aerospace TOR-2004 (8617)-4204	*100 Questions for Technical Review*

Other:

Critical Process Assessment Tool (CPAT), 14 August 1998

"From Data Collection to Lessons Learned—Space Failure Information Exploitation at The Aerospace Corporation," Proceedings of the First International Forum on Integrated System Health Engineering and Management in Aerospace, November 07-10, 2005, Napa, California, and references cited therein.

Chapter 10
Risk Management

Sergio B. Guarro
Systems Engineering Division

10.1 Introduction

Risk management (RM) is a structured process that has as its objective the identification and evaluation of risk across the board within a program or mission, including the identification and evaluation of specific risk reduction and risk control measures. Within this structured framework, RM provides the means of organizing, assessing, controlling, and tracking risks that may be related to any of the other disciplines and processes that are crucial components of mission assurance (MA). RM has a key program function in identifying and communicating threats to mission success to all decision makers and program stakeholders at all levels.

10.2 Definitions

Risk is the term used to refer to events that are possible, but not yet realized, and that carry adverse consequences for a program or mission. Risk is usually characterized by the identification of the risk events that pertain to a specific program or mission, by their probability of occurrence, and by the magnitude of the possible impacts as measured in some appropriate scale of assessable consequences.

Risk assessment refers to the technical activities that are applied to identify risk, to understand its nature in terms of possible sources, mechanisms, and consequences, and to evaluate its magnitude, in relation to a specific program or mission.

Also in the context of an entire program or mission, RM refers to the entire engineering process associated with the organized and systematic handling of risk, which includes not only the risk assessment practices and tasks, but also the decisions and actions intended to mitigate or minimize risk.

10.3 Objectives

RM provides assurance that program and system risks have been thoroughly analyzed (and impacts allocated to lower-tier subsystems, components, interfaces, etc.) and impacts identified, mitigation plans developed, and as the mitigation plans are executed, tangible evidence is produced that demonstrates risks have been effectively controlled.

Within the context of a program, risk is normally assessed with respect to technical performance, cost, and schedule. The MA aspects of RM, i.e., the assessment and handling of conditions or events that pose a threat to the successful execution of a mission, are directly related to the technical performance. SMCI 63-1201 (Assurance of Operational Safety, Suitability, & Effectiveness for Space and Missile Systems) states that it is a part of the program single manager's key responsibilities for system design and qualification to see that "a rigorous risk management process [must] be in place, all known technical issues resolved, residual risks satisfactorily assessed and accepted or mitigated, and confidence in mission success [must] be established at an acceptable level."

As an element of MA, RM must maintain a vigilant focus on system technical performance and, at least in this dimension, must be executed as an independent assessment function. In this capacity, it supports all other MA functions by providing an overarching framework under which mission risk issues can be evaluated and dealt with. MA objectives covered under this framework are:

- Systematic identification of issues that have potential impact on successful mission execution
- Formulation and use of explicit criteria and means of evaluation to decide whether mission assurance actions are necessary with respect to any identified risk issues
- Selection and execution of mission assurance interventions that are most effective in terms of risk reduction impact and efficient in terms of use of program resources

Besides its MA dimension and in the general context of space systems programs, RM is applied as a process to support program management functions. As such, it is concerned with events that also may have

adverse impacts on program execution in terms of program schedule and cost objectives.

10.4 Practices and Tasks

In the context of a program or project, RM is normally articulated as an organized process that is documented in a formal plan. This is a document, endorsed by the program manager or director, which defines the flow of RM activities and assigns basic responsibilities for their execution. General guidance for the definition of a risk management plan (RMP) and for the organization of a RM process is provided by ISO Standard 17666, Space Systems – Risk Management, 10 April 2003 and by the Department of Defense Risk Management Guide (see also section 10.5).

Many applications of RM are relatively unstructured and qualitative. However, several formal technical tools can be used to support RM key processes. Most of these have been proven and validated in the related discipline of probabilistic risk assessment (PRA), which is itself a standard framework and process to execute in-depth risk analyses of complex technological systems and missions. These techniques and their contextual use are individually discussed in the following sections. An overview of the PRA framework as an integrated risk assessment tool is given in 10.4.4. The reader can find more detailed technical discussion of the techniques introduced below listed as reference documents in section 10.9.

10.4.1 Techniques for Risk Identification

Master logic diagrams (MLDs) are basic classification/categorization-tree structures that can be used to organize and assist the process of risk-item identification and definition. An MLD is a deductively derived logic tree that identifies categories and subcategories of the domains of interest, which in the case at hand are risk initiators (initiating conditions or events) and impact areas (assets). MLD risk models are used to make sure the organization of risk source (or risk-initiator) and the program-asset impact categories is complete, traceable, and balanced. The MLD also is one of the basic tools for execution of mission PRAs, as discussed in paragraph 10.4.4.

10.4.2 Models for Risk Scenario Development

Risk items of concern for a program or mission can be analyzed and assessed in varying degrees of depth. Inductive logic models, such as event trees (ETs) or event-sequence diagrams (ESDs), constitute a class of formal models that are generally well suited to developing logically organized representations of risk items and risk scenarios. Inductively derived event trees and event-sequence diagrams are routinely used also in conjunction with deductive MLD and fault-tree models in PRA frameworks that are specifically executed to assess operational risk for space missions (see section 10.4.4). The degree of detail in the ET or ESD modeling of individual risk-items and scenarios can vary greatly, mostly depending on the complexity of the risk scenario represented and on the availability of data that may be used to assess the associated risk in quantitative terms.

10.4.3 System Failure Models

In most situations, program-risk evaluations need to cover a broad variety of risk items. Usually, top-level scenario models will provide enough information and insight for risk control trades and other program decisions. Sometimes, however, certain risk items may emerge as particularly significant and technically intricate. This is especially true whenever analysts are considering whether a system or subsystem design can meet quantitative risk/reliability goals or requirements for mission success or safety performance (e.g., in consideration of potentially defective parts and their impact on the launch success probability for a launch vehicle where they may be embedded in one or more critical subsystems). For these situations, detailed failure models are better suited to represent system or subsystem performance. Often such detailed system failure models are used for the purpose of enabling the quantification of branch probabilities in ET or ESD risk scenario models as introduced above.

A typical system/subsystem modeling choice is to use deductively derived fault trees and execute the associated analytical procedures to obtain quantitative estimates of system failure probability. Models borrowed from the reliability engineering domain, such as reliability block diagrams, are also sometimes used for the same purpose. Other models are also available and recommended for special modeling needs. For example, influence diagrams and Bayesian belief networks are well suited to model situations involving multiple influences and conditional probabilities.

10.4.4 Integrated Mission Risk Models

There exist situations where, to meet specific mission risk goals or to obtain quantitative indications on how to achieve a risk-balanced system design, it is desirable to develop an operational risk model for an entire mission. The term PRA is used to indicate a specific type of analytical framework that has been developed and matured over time for this specific type of risk analytical application. A PRA framework has as its objective the identification and analysis of all key risk scenarios that can result in mission failure and in a set of undesirable consequences. The framework is developed and quantified in steps, using the types of risk models that were discussed earlier in an integrated fashion:

1. MLDs are used to systematically identify initiating events and end-states that constitute, respectively, the sets of start and end points for all risk scenarios of interest.
2. ET or ESD models are developed to identify specific risk scenario sequences leading from initiating events to consequence end-states.
3. ET (or ESD) branch points depict the successful or unsuccessful operation of a specific subsystem. They are developed using fault-tree subsystems failure models to identify the sets of possible root causes for the corresponding ET branch-point event.
4. Risk scenario sequences are quantified, using the results of the fault-tree analyses to determine ET branch point conditional probabilities, and the ET conditional probability chains to quantify entire sequences.
5. Overall, scenario sequence probabilities, obtained as described above, are combined to obtain the probabilities of specific consequence end-states of interest (this is necessary when a specific end-state may result from different sequences that may occur independently).

PRA models for complex systems can be very extensive and several additional sub-processes and considerations beyond the overview process outline given above do apply.

10.4.5 Risk-Reduction Models

The risk assessment process can be extended to compare the risk reduction effect that a system or mission design modification has with

respect to an initial design baseline, within the cost (in time and resources) of the execution and implementation of that design modification. Any combination of the risk reduction models discussed in the preceding sections can be used to estimate the risk-reduction worth of a specific design modification. When multiple risk-reduction measures are possible to address a specific risk, the combined consideration of risk-reduction worth vs. cost for each of these permits the identification of a mission-optimal or program-optimal risk-reduction solution. For a given amount of available resources this approach permits, within the limits of the analytical techniques employed, the identification of the design improvements that provide the greatest possible risk reduction, i.e., the greatest possible mission success/MA benefit.

10.5 Strategies and Execution by Phase

This section describes the organization of tasks that constitute the implementation of the risk assessment and management supporting discipline.

Like all the other supporting MA disciplines, RM can technically be viewed as having its own self-contained process of execution. The RM portion of the MA task database represents and documents a form of comprehensive implementation of such a process from the viewpoint of tasks that can be executed by The Aerospace Corporation.

Program risk encompasses a space system life cycle, from acquisition activities such as concept definition, contract award, system design and development, manufacturing, and testing, to activities that need to be executed to complete the system mission. Thus, while a program progresses through the various phases of the acquisition process, it can be expected that the nature of the risk items that may be identified and managed will change. For example, in the pre-key decision point (KDP-A) phase, when a system to be acquired is not even fully defined at the most general of levels, the risk items that can be identified probably concern broad issues of acquisition strategy and technology maturity, whereas at the manufacturing stages of Phase D most risk items can be expected to concern production quality and test or system integration issues.

While the inner characteristics of the risk items that are the subject matter of the RM process change from one program acquisition phase to the next, the blueprint of application of the process itself does not.

Thus, in each phase the process repeats its standard application steps, which are grouped into four basic groups of activity or "subprocesses:"

- Risk planning
- Risk assessment
- Risk handling
- Risk monitoring

10.6 Organization of Tasks

Besides the standard partitioning of tasks according to acquisition phases, the RM tasks to be executed in each phase are organized around the RM subprocesses listed at the end of the preceding section, as further explained below.

10.6.1 Risk Planning Verification and Support Tasks

Risk planning consists of the upfront activities necessary to execute a successful RM program. It is an integral part of normal program planning and management. The planning addresses each of the other RM functions, resulting in the definition of an organized and thorough approach to assess, handle, monitor and document risks, and in the identification of the associated activities and responsibilities.

In a large program, RM planning activities resulting in the production of formal "RM plan" documentation will be normally carried out by the government and its direct FFRDC/SETA support, as well as by the prime contractor(s) and major subcontractors. Accordingly, the MA task database includes groups of tasks aimed at the direct support of government RM planning activities, as well as groups of tasks aimed at the validation and verification of contractor/subcontractor RM planning tasks and associated products (such as contractor RM plan documents).

10.6.2 Risk Assessment Verification and Support Tasks

The risk assessment process includes the identification of critical risk events and conditions, which could have an adverse impact on the program, and the analyses of these events and conditions to determine their likelihood of occurrence, consequences, and impact timeframe. The applicable guidance and reference documents indeed subdivide the assessment activities into the two further subprocesses of "risk

identification" and "risk analysis." The former includes examining all significant facets of the program to identify potential risks involving requirements, technical execution, schedule, cost, and management factors. The latter concerns the determination of the two characterizing components of the risk, for each of the risk items that have been previously identified, i.e.: the likelihood that the risk will occur and the severity of the consequences to the program should it occur.

Similarly to the basic organization of RM planning-related tasks, the MA task database tasks related to risk assessment are roughly subdivided into tasks concerning the support of risk identification and analysis tasks to be conducted by the government area of a program, and validation and verification tasks executed by contractors and subcontractors.

10.6.3 Risk Handling Verification and Support Tasks

Risk handling is the process that identifies, evaluates, selects, and implements actions and interventions that are designed to drive all risk items of significant concern to acceptable levels, in line with the existing program constraints and objectives.

The subprocesses for execution of a risk handling plan for a specific risk item are:

1. Identification of handling options
2. Evaluation and selection of executable options
3. Development and implementation of selected handling plans

In accordance with the above, the MA task database includes groups of tasks that are in support of government activities in the above three subprocess areas, as well as groups of tasks that are meant for the validation and verification of contractor activities in the same three subprocess categories.

10.6.4 Risk Monitoring and Updating Tasks

In addition to the basic risk planning, assessment, and handling-related activities addressed above, the MA task database includes tasks that are intended for the tracking of progress in the implementation and execution of risk handling actions, and the updating of planning and assessment activities executed in earlier program and/or acquisition phases. Independent review of the program risks at milestone reviews

and other major program decision points may be included in these groups of tasks as well. Tasks involving the monitoring of risk handling plans include not only monitoring the completion of the steps that have been outlined in the plan, but also monitoring the success of each step and the level to which the predicted risk reduction was achieved.

10.6.5 Plan Update and Risk Reassessment Tasks

The MA task database includes specific groups of updating tasks that are particularly relevant at the beginning or in the early stages of each new acquisition phase for a given program. These are those tasks that concern:

- The updating of government RM plans to make them current for a new acquisition phase
- The review and reassessment of "residual" risk items inherited from an earlier acquisition phase
- The review and validation of contractor RM plans generated for a new acquisition phase

10.6.6 RM Lessons Learned Tasks

The MA task database concludes each phase of acquisition with a task specifically intended for the assembly, review, and documentation of RM-related Lessons Learned.

10.7 Core MA Processes (CMPs) Supported by Risk Management

RM addresses the whole spectrum of potential risks that may affect a program, thus each of the associated tasks, as executed, may be related to one or more CMP tasks, depending on the program phase and the particular risk topic being addressed.

Given the forward-looking nature of the risk identification and assessment activities, RM tasks executed in a given program phase may relate not only to CMP tasks pertaining to that same phase, but even to CMP tasks that are associated with a later phase. For example, during the concept development phase it can be expected that many risk issues be related to tasks belonging to the requirement analysis and verification CMP and that are executed in that phase. However, it can

also be expected that several risk issues be identified that relate to tasks of the design assurance CMP that are to be executed in the following preliminary design phase (MAG Phase B).

In general, because RM addresses both “programmatic” (i.e., cost and schedule) and “technical” (i.e., mission success and safety) issues, the execution of RM tasks will cut across the entire spectrum of acquisition phases and will entail information input and output relations with a full range of CMP tasks listed in the MA task database associated with this guide (Appendix A3). In addition, RM tasks will have close links and interfaces with a number of government and contractor enabling tasks, as discussed in the following section.

10.8 Government and Contractor Enabling Tasks and Products

RM tasks executed by Aerospace or by any other responsible organization will always require a considerable amount of data and input information from the government organization responsible for program management and decision-making, and from the prime contractor, which in turn may be required to also serve as the primary conduit of information concerning second-tier contractor processes and tasks that may also be needed. The amount and level of detail of the information required as input will depend on the breadth and depth of scope of the RM process planned for execution by a specific program, but in general shall at a minimum include the key elements discussed below in sections 10.8.1 and 10.8.2.

10.8.1 Government Enabling Tasks

The nature of the interface between the RM process carried out by the MA and the corresponding government RM process may vary greatly, depending on the assignment of roles and accountabilities chosen by the government acquisition authority. In many cases, there may not be any distinction between the two, so that the MA organization will operate as an entity that directly assists and participates in the government RM plan formulation and execution. In other cases, the government RM plan may have a more programmatic focus, while the MA aspects of RM may be addressed by a parallel process carried out jointly by the Government program management cadres and by the MA organization.

In the first type of RM process setup, i.e., in cases where there may exist a partial distinction between "programmatic" government RM activities and MA RM activities, the following key elements of information from the former will be required by the latter:

1. Scope and objectives of government RM plan for the program of interest.
2. Nature and characteristics of the principal government-side risks identified by the government program and/or the acquisition authority.
3. Nature, characteristics and execution plans for risk handling measures and tasks chosen by the government to address risks referred to above in item 2.

All of the above elements of information usually require the execution of specific tasks in order to be produced and made available as program documentation in the form of reports or data items. These tasks are identified in the MA task database as "government enabling tasks" and the associated data items as "government enabling products."

As a more common alternative, the program RM process may be established according to the second of the two paradigms mentioned above. In this case the MA organization will itself participate in the generation of the government RM information and results listed in 1 through 3 above. Thus, the corresponding tasks will no longer be "government enabling tasks," but will become tasks executed by the MA RM organization jointly with government personnel.

10.8.2 Contractor Enabling Tasks

Ideally, the program RM process should be fully integrated across the interfaces between the acquisition authority, the MA organization, and the program contractors. Even though in practice it is impossible to communicate all potentially RM-relevant information both horizontally and up and down the management structures of all involved organizations, it remains in all cases true that much of the MA RM process foundation lies upon program execution information and data that is generated and managed by the prime contractor and its subcontractors. For this reason, this guide and the associated MA task database identify a number of contractor enabling tasks and products that must be made available in order to make possible the execution of the RM tasks for which the MA organization is responsible and accountable. Some of the enabling data and documentation produced

by the contractors must in fact be reviewed for concurrence by the MA organization to assure its accuracy and validity.

In general, in each acquisition phase the contractor enabling tasks of interest are those that result in the generation and communication to the MA organization of the following basic types of "enabling products":

1. Contractor RM plan documentation – Must be reviewed to make sure it defines an RM process, a risk assessment technical framework, and risk information data formats that are compatible with those selected for the government and MA RM process(es).
2. Summary documentation of definitions and assessment classifications for all risk items identified by the contractor(s) – Some level of review by the MA organization is generally recommended for validation of and concurrence with risk levels assigned by contractor(s) to risk items of potential government concern.
3. Detailed documentation of those risk items identified by the contractor(s) which, if the risk handling measures planned and executable by the contractor(s) with contractor resources only were not to be successful, could impact the execution of the government program and/or mission in a material way because of their potential severity – Must be reviewed for validation of and concurrence with the contractor(s)' assessment.
4. Detailed documentation of risk items identified by the contractor(s) that cannot be handled by the contractor(s) with contractor resources only, i.e., without the likely need to deploy government and/or MA organization resources beyond the negotiated program contractual baseline – Must be reviewed for validation and concurrence with the contractor(s)' assessment.
5. Detailed handling plans formulated by the contractor(s) for all risk items of the type defined in 1 and 2 above – Must be reviewed for validation of and concurrence with the contractor(s)' selection of handling measures and related execution plans.
6. Detailed documentation of results produced by the execution of risk handling measures for all risk items of the type defined in 1 and 2 above – Must be reviewed for validation of and concurrence with the contractor(s)' assessment of level of success, i.e., risk reduction, achieved by implementation of risk handling plans and risk handling measures.

10.9 References

The following report contains information that is of direct significance and assistance for the execution of tasks associated with the RM discipline as defined in this guide:

Aerospace TOR-2005(8583)-4019	*Risk Management Plan Guide for Space Acquisition Programs*, 29 April 2005

The following additional references contain general procedural guidelines and technical information pertaining to the execution of a complex RM process in a generic space system and DOD acquisition program, respectively:

1. ISO 17666, Space Systems Risk Management, 01 April 2003 (included in the Aerospace-recommended list of specifications and standards).
2. DOD Risk Management Guide Risk Management Guide for DOD Acquisition, Defense Systems Management College, Fifth Edition, v.2, June 2003.

Additional guidance can be found in the following references:

Policy-related

SMCI 63-1201	"Assurance of Operational Safety, Suitability, & Effectiveness for Space and Missile Systems," 21 May 2001

Technical Handbooks

DOD Risk Management Guide Risk Management Guide for DOD Acquisition, Sixth Edition, v.1.0, August 2006

Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, Office of Safety and Mission Assurance, NASA Headquarters, Washington, DC 20546, August 2002

Fault Tree Handbook with Aerospace Applications, Version 1.1, Office of Safety and Mission Assurance, NASA Headquarters, Washington, DC 20546, August 2002

Chapter 11
Reliability Engineering

Roland J. Duphily
Acquisition and Risk Management Office

11.1 Introductions

Reliability engineering encompasses a set of analytical activities that include the development of probabilistic system reliability requirements, the analysis of failure modes and effects, the identification and control of critical/limited life items, the development of probabilistic reliability models, the determination of component/part failure rates, the use of worst-case and parts stress analyses, the analysis of accelerated life test data, and the implementation of a failure recurrence prevention system which ensures that all failures are adequately driven to closure. Reliability plans (MIL-STD-1543 tailored) that define the process are prepared and submitted as a program contract data requirements list (CDRL) with periodic updates. Software reliability is not discussed here, but is addressed in Chapter 16.

To enhance effectiveness of the reliability engineering process, it needs to be organizationally separate from the design engineering organization with independent reporting to a mission assurance function outside of the programs. While independent, it needs to work closely with system engineering and the design team to accomplish its tasks. The process begins during conceptual design and continues through the remaining program life cycle, which includes detail design, assembly, integration and test (I&T), and on-orbit problem resolution.

11.2 Definitions

- System or device **reliability** is defined as the probability that the system or device will perform its intended functions for a specified period of time, under specified operating conditions.

- **Reliability engineering** is a combination of engineering techniques and practices aimed at assuring the reliability level specified (numeric value) for a system or device will be achieved in its actual operation by the user.

11.3 Objectives

The objective of reliability engineering is to define and support the implementation of the program/project reliability assurance activities such that the design risks are balanced within project objectives and constraints. Reliability engineering is integral to the system design process and works closely with the subsystem designers, risk management, parts, materials, and processes (PM&P), system safety, subcontractors, quality assurance (QA), I&T engineering, and configuration management. Reliability engineering also tracks the design's ability to meet or exceed the product's reliability requirements. System reliability requirements are developed and included in system requirements documents. Reliability assessments of the hardware design characteristics against allocated requirements are performed by contractors to detect design deficiencies and functional performance risks, as well as ways to mitigate them early in the design process.

11.4 Practices and Tasks

Key practices and tasks include reliability requirements definition and allocation, design architecture reliability prediction, tradeoffs, failure modes and effects analysis (FMEA), reliability critical and limited life item control, parts reliability analysis, worst case analysis, parts stress analysis, and failure reporting and corrective action. Early planning of an adequate reliability assurance process will benefit the program/project by contributing to a robust design, with an optimal balance between design verification tasks, cost, and schedule constraints, and minimize the probability of very late and costly detection of problems which could threaten mission launch schedules or mission objectives. The results of reliability analysis identify potential risk items that are managed by the risk management process. During the design development process, reliability engineering assists with design tradeoff studies, the implementation of accelerated life testing of new hardware, and the assessment of failures during I&T.

11.4.1 Numerical Reliability Requirements Determination

Figures of merit, such as, mean time to failure (MTTF), probability of failure (PoF), reliability (1-PoF), mean mission duration (MMD), and mean life estimate (MLE), provide guidance to the design team. Figures of merit help to determine the necessary part quality,

redundancy, and part stress levels needed to meet expected mission success criteria. Through analytical and empirical methods, the intended uses, mission profile, success criteria, and environments of the system are translated into realistic system-level reliability performance parameters for system development specifications and requirements documents. The most important thing to remember is to state reliability performance requirements in terms of the required results and provide the criteria for verifying compliance.

11.4.2 Reliability Predictions and Tradeoff Studies

Reliability block diagrams (RBDs) graphically represent the hardware and software needed for success, operating duty cycles, redundancy types, and any available work-arounds. When comparing competing designs, quantification of RBDs helps to determine which design concept is the most reliable or has the lowest PoF. Results of these analyses are CDRLs and part of design review packages.

Probabilistic reliability models and failure data sources need to be independently reviewed for adequacy of assumptions, completeness, and accuracy. RBDs or fault trees used to model the system also are reviewed, as are failure rates deemed reasonable for active and standby conditions are reviewed. Numerical results are reviewed for reasonableness when compared to similar systems.

11.4.3 FMEA/Failure Modes Effects and Criticality Analysis (FMECA)

The FMEA or FMECA process is an effective tool in the decision making process, provided it is a timely iterative activity. A FMECA is identical to a FMEA except for the additional consideration of criticality, and is typically called a bottom-up analysis that looks at each hardware element, its failure modes, the effects on higher levels, and associated criticality. Late implementation or restricted application of the FMEA/FMECA dramatically limits its use as an active tool for improving the design or process. Initiation of the FMEA/FMECA starts as soon as preliminary information is available at a high level and then is extended to lower levels as more details become available.

The design FMEA/FMECA of complex systems usually begins with a functional modeling approach, which is later expanded into a detailed hardware modeling process, for major system components. When any design or process changes are made, the FMEA/FMECA is updated and

the effects of new failure modes introduced by the changes are carefully assessed. Although the FMEA/FMECA is primarily a reliability task, it provides information and support to safety, maintainability, logistics, test, and maintenance planning, and failure detection, isolation, and recovery (FDIR) design. The use of FMEA/FMECA results by several disciplines assures consistency and avoids the proliferation of requirements and the duplication of effort within the same program. Results of these analyses are CDRLs with periodic updates and summarized within critical design review (CDR) packages.

The FMEA/FMECA process needs to be independently reviewed to evaluate its effectiveness in identifying and controlling credible single-point failures. The failure modes analyses should be used to identify credible single-point failure modes and feed into the critical items controls process to eliminate or control their effects.

11.4.4 Critical/Limited Life Item Control

Mission and safety critical items are those items whose failure would directly affect system or personnel safety, mission success, or operational readiness. Limited life items are those items whose expected life is less than two times the mission design life.

The early identification, tracking, and control of critical items through the preparation, implementation, and maintenance of a critical items list (CIL) and limited life items list (LLIL) will provide valuable inputs to a design, development, and production program. From the CIL activity, critical design features, tests, inspection points, and procedures can be identified and implemented that will minimize the probability of failure of a mission or loss of life. The LLIL activity identifies those limited life items and the required documentation needed to ensure that the items are successfully tracked during I&T to minimize stressing before launch. Results of these analyses are typically CDRLs with periodic updates and part of design review packages.

An independent evaluation of the critical/limited life item identification process and critical/limited life item control plans for completeness should be completed as part of mission assurance.

11.4.5 Worst-case and Parts Stress Analysis

A worst-case analysis is performed where failure results in a Category I or II degree of severity. The most sensitive design parameters are analyzed, including those subject to variations that could degrade performance. The adequacy of design margins in electronic circuits, optics, electro-mechanical and mechanical items are demonstrated by analyses, test, or both. The analyses consider all parameters set at worst-case limits and worst-case environmental stresses. Part parameter values for analyses include manufacturing, temperature and cumulative radiation variability, and aging effects of environment. The analyses are updated with design changes. The analysis results are presented at design reviews.

Electrical/electronic stress analysis is performed on all new designs including designs incorporating commercial off-the-shelf/non-development item (COTS/NDI) and design modifications to determine, from the circuit and the operating conditions of a given application, the actual stresses induced on each part. The stress analysis is conducted using worst-case environmental and load conditions. Unacceptable stress conditions based on derating criteria are eliminated.

11.4.6 Parts Reliability Analysis

Electrical, electronic, optical, and mechanical part failure rates are the basic building blocks of probabilistic reliability predictions. Therefore, confidence in the predictions is very much dependent on having failure rates (MIL-HBK-217, etc.) derived from credible sources or test data with appropriate adjustments for quality, end use environment, stress levels, and temperature levels. To help validate reliability predictions, an independent evaluation is performed on part quality level, available accelerated part life test data, derating criteria (MIL-STD-1547), parts stress analysis, participation in government industry data exchange program (GIDEP) alerts, and junction temperature limits (< 105C). For new parts (e.g., heterojunction bipolar transistors (HBTs), field programmable gate arrays (FPGAs), etc.) it is especially important that the part qualification process be independently reviewed by a team consisting of experts from PM&P and reliability to validate the design.

11.4.7 Accelerated Life Testing

The contractor establishes and maintains an accelerated life testing (ALT) program to detect and correct any inherent design and

manufacturing flaws and to determine product robustness of mission-critical items. Selection criteria are established to identify ALT candidates. Criteria and candidates are made available for technical review. ALT is used during development in an iterative fashion beginning at lower levels of assembly and progressing to higher levels of assembly until sufficient margins have been verified. Test methods include a series of individual and combined stresses applied in steps of increasing intensity (well beyond the expected field environments) until failure or a malfunction is obtained. Failure modes are analyzed for root cause and corrective action.

11.4.8 Environmental Stress Screening

An effective environmental stress screening (ESS) program is created and maintained so that workmanship failures can be identified early and removed from equipment. The program includes development of ESS profiles based on thermal and vibration surveys and equipment response analyses. As a minimum, power on and performance monitoring are performed at two levels of assembly. The ESS program considers equipment design, part/component technology, and production fabrication techniques. Effectiveness is tracked for each level of screening and metrics established to support appropriate tailoring of existing screening profiles. To determine the most effective screening profiles, the ESS program includes feedback of latent and intermittent failures, previously undetected design defects, previously undetected failure modes, and workmanship defects into Failure Reporting Analysis and Corrective Action System (FRACAS). ALT results may be used as a baseline for determining initial ESS profiles.

11.4.9 FRACAS

A closed loop failure analysis and corrective action system is established to ensure that all failures are documented, analyzed for root cause, and that timely corrective actions are taken to reduce or prevent recurrence. It serves as a management tool to identify, correct, and prevent further recurrence of all failures occurring in hardware and software during system debugging, engineering tests, qualification tests, ESS, receiving I&T, fabrication, acceptance tests, flight tests, and on-orbit failures. The program office needs to be an active participant in the contractor and subcontractor failure review board (FRB) process to ensure that the root cause is adequately identified and prevented from occurring in the future. The failure analysis and corrective action

results need to be well documented and easily retrievable for use in future on- orbit failure investigations.

Most contractors have an automated FRACAS database, which includes their subcontractor failures. Preliminary copies of each failure report are typically CDRLs submitted within a week or earlier of the failure. FRB data packages may also be submitted by the contractor to the program office for review prior to the FRB's. Summaries of open failure report status are generally presented at regular contractor program reviews. In addition, delivered hardware typically includes completed test failure reports as part of its end-item data packages.

11.4.10 High-level System of Systems Reliability Model

For complex architectures with multiple space segment, launch segment, and ground segment elements, it is imperative to develop a high-level system of systems reliability and/or availability model to ensure that the appropriate reliability and/or availability requirements are flowed to the elements. It is a living model that evolves with the design and assists with making decisions during trade studies of how to operate various element combinations and meet overall mission success probabilities.

11.5 Strategies and Execution by Phase

To maximize mission probability of success and minimize single-point failures, reliability tasks begin in pre-phase A to ensure that the request for proposal (RFP) adequately addresses needed reliability activities in the statement of work (SOW), CDRLs, data item descriptions (DIDs), and specifications. Reliability engineering's primary focus during Phases A-C is to ensure CDRLs are completed accurately and that reliability is adequately addressed at system requirements review (SRR), system design review (SDR), preliminary design review (PDR), and CDR at the system, subsystem, unit, and part levels. Updating of Phases A-C reliability analysis occurs during Phase D as a result of design and part changes that have been driven by corrective actions associated with mitigating failures that have occurred during qualification, acceptance, and integration tests at the part, unit, subsystem, and system level. The proper definition and administration of a preventative closed loop FRACAS are the primary reliability engineering tasks during Phases D1-D2. The contractors FRACAS is reviewed along with participation as needed at material review boards

(MRBs) and FRBs. Testing failure reports are reviewed for completeness and verification that all has been done to determine the root cause with adequate corrective action. Participation at pedigree reviews, hardware acceptance reviews, and physical configuration audits (PCAs) are also accomplished to assure that all documentation is adequately closed. During Phase D3, on-orbit failures are analyzed to determine the root cause and the space vehicle reliability model/prediction updates are reviewed after redundancy losses in support of mission life estimates (MLE).

11.6 Organization of Tasks

Within the mission assurance task data base (MAVM) reliability engineering tasks are assigned to one of the following seven MAG phases first:

1. Phase 0: Pre-KDP A Concept Studies
2. Phase A: Concept Development
3. Phase B: Preliminary Design
4. Phase C: Complete Design
5. Phase D1: Fabrication and Integration
6. Phase D2: Fielding and Checkout
7. Phase D3: Operations and Disposal

11.7 Core Mission Assurance Processes Supported by Reliability Engineering

During requirement analysis and validation, reliability engineering assists with the development of reliability, availability, and maintainability requirements for inclusion in the RFP, the assessment of allocated requirements conducted by the prime contractor, and assessment of the flow-down of reliability requirements down to subcontractors.

During design assurance, reliability engineering assists with the assessment of reliability trade studies, and the assessment of reliability analysis conducted for reliability requirements validation and verification—namely, an assessment of reliability models, FMEA, fault tree analysis (FTA), parts accelerated life testing models, parts stress analysis, worst-case analysis, critical items analysis, and limited life items analysis.

During manufacturing assurance, reliability engineering assists with a review of process FMEAs for high-volume lines such as solar arrays, and new parts qualification reliability criteria such as HBTs and FPGAs.

During integration test and evaluation, reliability engineering assists with the definition of accelerated life test requirements, analysis of life test data results, and the FRACAS process definition and implementation.

During operations readiness assurance, reliability engineering assists with the collection, review, and analysis of launch and on-orbit anomalies.

During mission assurance reviews and audits, reliability engineering is an agenda item at SRR, PDR, CDR, and flight readiness review (FRR), and participates in FCAs and PCAs.

11.8 Government and Contractor Task and Products

In addition to requiring access to the government's draft and final RFP and the negotiated contract, the reliability engineering team needs access to the contractor's reliability policy and guidance documentation across the prime and subcontractors. The reliability engineering team will also need unfettered access to the contractors' design teams at all levels of the program through the active design period and testing activities. Contractor CDRLs for SDR, PDR, CDR, reliability plans, life testing, predictions, FMEA/FMECAs, FRB packages, and end item data packages are also needed.

11.9 References

Specifications and Standards

MIL-STD-1543B	Reliability Program Requirements for Space and Missile Systems, 25 October 1988
MIL-STD-756B	Reliability Modeling and Prediction, November 1981

MIL-STD-1629A	Procedures for Performing a Failure Modes, Effects & Criticality Analysis, November 1980
IEEE STD 1413.1-2002	IEEE Guide for Selecting and Using Reliability Predictions Based on IEEE 1413

Technical Handbooks

Aerospace TOR-2006(8506)-4494	*Space Vehicle Systems Engineering Handbook*, Chapter 21, 30 November 2005
MIL-HBK-338B	Electronic Reliability Design Handbook
MIL-HBK-217F	Reliability Prediction of Electronic Equipment

Best Practices

NASA Technical Memorandum 4322: NASA Reliability Preferred Practices for Design and Test

Deliverables

DI-RELI-80685	Critical Items List, 30 September 1998
DI-SESS-81613	Reliability & Maintainability (R&M) Program Plan, October 2001
DI-RELI-81497	Reliability Prediction, April 1989
DI-RELI-81496	Reliability Block Diagrams, April 1989
DI-RELI-80687	Failure Modes Effects & Criticality Analysis (FMECA), June 1986
DI-RELI-81315	Failure Reporting and Corrective Action System (FRACAS), 1989
DI-RELI-80255	Failure Summary Report, June 1986

Other

Critical Process Assessment Tool (CPAT), Reliability Engineering (contains guidance on RFP preparations)

Air Force Instruction 10-602 Determining Mission Capability and Supportability Requirements, 20 September 2000 (contains reliability metrics definitions)

Chapter 12
Configuration Management

Roland J. Duphily
Acquisition and Risk Management Office

12.1 Introduction

The primary purpose for **configuration management (CM)** is to establish and maintain control over a program's technical hardware and software baselines consisting of requirements, specifications, designs, interfaces, data, and supporting documentation. The CM discipline provides a structured systems engineering approach to controlling baseline changes and conducting impact (e.g. performance, cost, and schedule) analysis to maximize mission success and minimize unwanted performance degradations during and after the changes are implemented. Finally, configuration management provides a mean to coordinate change and achieve consensus among the system stakeholders (e.g., contractors, government program office(s), and operations) in order to successfully implement those changes (e.g., databases, hardware, software, interfaces, drawings, requirements, supporting documentation, etc.) to maintain or evolve the system. CM plays a prominent role during a program's physical configuration audit and functional configuration audit as described in Chapter 6 of this guide.

12.2 Definitions

During system development, CM[28] is a rigorous approach that is designed to technically and administratively document, control, and maintain status of the functional, physical, developmental, allocated, test, and product baselines of a program's system, including hardware, software, data, interfaces, procedures, and processes throughout a system's entire life cycle. CM of systems is based on the concept of configuration items (CIs).

[28] Definition consistent with INCOSE SE Handbook, INCOSE-TP-2003-016-02, Version 2a, 1 June 2004, Section 5.3.1, p 46 and Goddard Space Flight Center (draft) SE Directive, GPG 7120.5, 4/8/2002, p.3.

A **CI**[29] may be defined as an individual item (e.g., hardware component, software module, a procedure, or a process), or may be a significant part of a system or part of a higher-level CI with physical and functional characteristics that make it unique. CIs are designated at appropriate levels of assembly for baseline documentation and management based on program-unique circumstances.

12.3 Objectives

The objective of CM is to ensure that the software and hardware functional, allocated, developmental (software), test, and product baselines are consistent, accurate, and repeatable throughout the system's life cycle and that any changes to those baselines maintain the same accuracy, consistency, and repeatability. Accurate information as a basis for design, development, and test decisions reduces risk and thereby improves mission success. The CI level is where configuration management really begins; the process encompasses, to some degree, every item of hardware and software down to the lowest bolt, nut, and screw, or lowest software unit. This does not mean that the acquiring activity, the prime contractor, or even subcontractors have visibility or configuration control authority over every part. Rather, it means that some organization within either the supply chain or the standardization process has configuration documentation and change control responsibility for each part.

12.4 Practices and Tasks

The following are key CM practices and tasks:

- *Establish a CM program and plan for each program and system under development.* The CM plan is contractually mandated as a contract deliverable for the development contractors. A complementary plan is also developed for government program office use and eventually each system stakeholder will develop and use similar plans as its operational baselines accommodate newly delivered systems.

- *Define attributes and measurable performance parameters at all needed levels of assembly.* These become benchmarks for the stakeholders and the development contractors to use as a

[29] IBID INCOSE SE Handbook, p.48.

known basis for acquisition and use of each item produced as part of system development.

- *Identify, document, and verify each CI's physical and functional characteristics or attributes to establish that description as a known basis for change.* CIs should be uniquely identified and verified to make sure they conform to, and perform as defined in, the configuration documentation.

- *Correlate manufactured items with their associated requirements, design, and product information.* Ensure a consistent reliable process is used to label each configuration item.

- *Capture configuration information during the product definition, change management, product build, distribution, operation, and disposal processes. Store and organize the information for retrieval and use across the program.* Make applicable data (i.e., procurement, design, supportability) easily accessible for making design, procurement, or supportability trades and decisions over a system's life cycle. Also collect change status as activities associated with the CM process occur. This configuration status accounting information should be correlated, maintained, and provided in useable form as required.

- *Evaluate proposed change and identify and further assess performance and cost; schedule impacts prior to making change decisions.* Specifically, whenever a change to a CI is contemplated, evaluate the effect of that change on other CIs and associated documents. If done correctly, the impact of any change can be minimized, avoiding costly downstream surprises.

- *Establish and use a systematic change management process.* Change activity is managed and costly errors due to ad hoc erratic change management are avoided.

12.5 Strategies and Execution by Phase

Within the Mission Assurance Verification Matrix (MAVM) task database, CM tasks are first assigned to one of the following seven MAG phases:

1. Phase 0: Pre-KDP A Concept Studies
2. Phase A: Concept Development
3. Phase B: Preliminary Design
4. Phase C: Complete Design
5. Phase D1: Fabrication and Integration
6. Phase D2: Fielding and Checkout
7. Phase D3: Operations and Disposal

To ensure that spacecraft configuration baselines are well defined with a good change management and status accounting process, CM tasks begin in pre-Phase A to ensure that the request for proposal (RFP) adequately addresses needed CM activities in the statement of work (SOW), contract data requirements list (CDRL), data item descriptions (DIDs), and specifications. The primary focus of CM during Phases A-C is to ensure baselines are properly established, CDRLs are completed accurately, and CM is adequately addressed at system requirements review (SRR), system design review (SDR), preliminary data review (PDR), and critical design review (CDR) at the system, subsystem, and unit levels, with well-defined hardware and software configured items and change control boards (CCBs). Updating of Phases A-C baselines occurs during Phases D1 and D2 as a result of design and part changes that have been driven by corrective actions associated with mitigating failures that have occurred during qualification, acceptance, and integration tests at the configured item, unit, subsystem, and system level. Verification of baselines occurs via functional configuration audits (FCAs) and physical configuration audits (PCAs).

12.6 Organization of Tasks

The MAVM task database for CM is organized in a hierarchy by life cycle phase as discussed above. For each life cycle phase, the process is further organized into the following categories: program planning, systems engineering, and space systems CM.

Program planning includes an evaluation of the contractor's CM plan, CI identification process and release plans, and CCB procedures to ensure that a good CM process is in place and accessible by the system program office technical team.

Systems engineering includes a series of tasks to ensure that the CM process traces to all interfacing processes and that there is adequate participation, as well as product data management (PDM) tools and resources for controlling all baselines. Ongoing

assessment of CCB processes throughout all the team players are also addressed in systems engineering.

Space systems CM tasks are required to evaluate whether the contractor's CM process at lower levels successfully flow up possible impact of lower-level configuration changes to the space vehicle.

Within each category described above, CM tasks are further organized by level of assembly: unit, subsystem, system, and segment.

12.7 CM Programs Supported by CM

During requirement analysis and validation, CM assists with the development of CM requirements for inclusion in the RFP, the assessment of baseline and change management requirements conducted by the prime contractor, and assessment of the flow-down of CM requirements to subcontractors.

During design assurance, CM assists with the assessment of CM plans, release plans, class of change, CCB procedures, baselines, hardware and software configuration items (hardware configuration items (HWCIs) and computer software configuration items (CSCIs)), engineering change proposals (ECPs), engineering review board, configuration control boards, and status accounting process

During manufacturing assurance, CM assists with a review of the methods controlling manufacturing processes/procedures, changes to processes/procedures, quality assurance (QA) support to CM, and as-built configuration reporting processes.

During integration test and evaluation, CM assists with the review of methods for controlling integration and test processes/procedures, changes to integration and test (I&T) processes/procedures, and as-integrated configuration reporting processes.

During operations readiness assurance, CM assist with the management of configuration changes driven by launch and on-orbit anomalies that can change future builds.

During mission assurance reviews and audits, configuration management is an agenda item at SRR, PDR, CDR, flight readiness review (FRR), and supports FCAs and PCAs.

12.8 Government and Contractor Task and Products

In addition to requiring access to the government's draft and final RFP, and the negotiated contract, the CM team needs access to the contractor's CM policy, guidance documentation, and change documentation across the prime and subcontractors. The CM team will also need unfettered access to the contractors' engineering team at all levels of the program through the active design period and testing activities. Contractor CDRLs for SDR, PDR, CDR, CM plans, release plans, engineering review board (ERB)/CCB procedures, configured items lists, configuration control board minutes, ECPs, and end item data packages are also needed.

12.9 References

Specifications and Standards

Aerospace TOR-2006(8583)-1	*Configuration Management*, August 2005, replaces MIL-STD-973, Configuration Management, 17 April 1992

Technical Handbooks

MIL-HDBK-61A(SE)	Configuration Management Guide, 7 February 2001
Aerospace TOR-2006(8506)-4494	*Space Vehicle Systems Engineering Handbook*, Chapter 23, 30 November 2005

INCOSE SE Handbook, INCOSE-TP-2003-016-02, Version 2a, 1 June 2004

Best Practices

Deliverables

DI-CMAN-80858B	Contractors CM Plan, 30 September 2000

DI-CMAN-80556A	Configuration Audit Plan, 17 April 1992
DI-CMAN-81516	As Built Configuration List, 15 July 1996
DI-CMAN-80639C	Engineering Change Proposal, 30 September 2000
DI-CMAN-80641B	Request for Waiver, 13 January 1995
DI-CMAN-80640C	Request for Deviation, 30 September 2000
DI-CMAN-80642C	Notice of Revision, 30 September 2000

Other

Critical Process Assessment Tool (CPAT) on Configuration Management from SMC/AXM, 14 August 1998

Chapter 13
Parts, Materials, and Processes

Howard D. Wishner
Navigation Division
George G. Cuevas
Parts, Materials, and Processes Department
Steven R. Robertson
Parts, Materials, and Processes Department

13.1 Introduction

The consequences of mission failure or inability to deploy the system on time due to **parts, materials, and processes (PM&P)** issues need to be clearly understood by the mission assurance (MA) team, as these elements are fundamental to the overall mission reliability and program success. Reliable and dependable operation means that the equipment must operate continuously with high availability in service, resulting in considerable design redundancy to meet reliability and service life requirements. These requirements drive the need for robust designs that are dependent on robust PM&P that have been fully qualified in terms of demonstrated long life and tolerance to the harsh environmental conditions of space. The characteristics and performance of the program's PM&P must also be clearly understood by the design team so that they can be applied in a manner to preserve their inherent robust capabilities.

PM&P engineering has distinct MA elements that start with independently verifying that proposed contractual PM&P requirements are consistent with the overall national program priority and risk management approaches identified in the acquisition strategy. This is crucial to program success as all too often, attempts to backfill for the lack of adequate requirements have led to significant cost overruns and delays and/or the procuring agency accepting degraded mission reliability. The requirement definition phase is followed by a planning phase in which the MA tasks verify that adequate PM&P controls and procedures have been developed and applied seamlessly across the program. In the implementation phase, MA focuses on assuring that these controls and procedures are rigorously followed and that the program has indeed acquired the required robust PM&P.

13.2 Definitions

PM&P are those basic elements that are required to manufacture the desired end product.

A **part** is defined as one piece, or two or more pieces joined together, which are not normally subjected to disassembly without destruction or impairment of its designed use.

A **material** is a metallic or nonmetallic element, alloy, mixture, or compound used in a manufacturing operation, which becomes either a temporary or a permanent portion of the manufactured item.

A **process** is an operation, treatment, or procedure used during a step in the manufacture of a material, part, or assembly.

PM&P engineering is a critical engineering discipline comprising of a set of skills and knowledge used to select, apply, design, and manage PM&P used to manufacture an end product.

13.2.1 Objectives

The objective of PM&P engineering is to provide a standardized set of qualified parts, material, and processes to enable the manufacture of a reliable end product at a minimum life cycle cost and program risk that meets its system performance requirements. The overall PM&P objectives achieve the required system performance through an efficient PM&P program-wide policy that utilizes the best practices from prior or current military standards and existing supplier processes.

13.3 Practices and Tasks

The PM&P engineering activity is a critical system engineering process, and as discussed previously, applicable to all phases of an acquisition and produces the number of critical products as outlined in the following subparagraphs. In many cases, preliminary versions can be developed in earlier phases and then finalized and maintained in the phases described below.

13.3.1 Concept Development Products

PM&P engineering activities during MAG Phase A (concept development) establish:

- A comprehensive PM&P program policy from the derived system engineering constraints and performance needs
- A cross-functional PM&P management plan for efficient and uniform implementation of PM&P policy
- A rating system with judging supplier's performance and development of an approved suppliers list

13.3.2 Design and Development Products

PM&P engineering activities during MAG Phases B and C (preliminary design and complete design) provide for:

- The documented individual part, material, or process needs consistent with PM&P program requirements
- The development, maintenance, and control of a database/system documenting design requirements, design baseline, control, and use of life-limited and lot control items, the basis for decisions made, and control of evolving requirements so impact of change can be effectively determined prior to implementation
- The development, maintenance, and control of approved selection, as-designed, and as-built program-compliant PM&P lists and methodology for approval of new PM&P
- The development of a methodology for generation of temperature, radiation, and aging derating to meet system performance at end-of-life (EOL)
- The development of part selection criteria, including the development of design manuals to assure parts application does not exceed performance boundaries
- The demonstration of critical manufacturing processes
- Audits of critical manufacturing processes, along with performance of part and material risk reduction tasks that address new technologies and verify readiness to enter production
- An approved suppliers list

13.3.3 Manufacturing and Test Products

PM&P engineering activities during MAG Phase D1 (fabrication and integration) provide for:

- The development of a closed-loop system to efficiently feed back necessary changes derived from system-level performance results and industry data interchange
- The development of an in-process or EOL validation process for a "*g*ood known part, material, and process"
- The development of a list of long lead items and methodology for assuring "on-time" delivery
- The development of new technology insertion criteria and obsolescence management;
- Addressing the uniformity of which PM&P requirements are imposed across the program
- The monitoring PM&P qualification and lot acceptance test results, with emphasis on assessing any deviation from the initial requirement set and/or appropriate corrective actions

13.3.4 Deployment and Operations Products

During MAG Phase D2 (fielding and checkout), PM&P engineering activities and processes continue to assure that performance expectations are being met, provide a continuing identification of technology and performance upgrade opportunities, and resolve and implement corrective actions/Lessons Learned for any system anomalies that are traceable to PM&P.

13.3.5 MA PM&P Engineering Practices and Considerations

The life cycle costs of PM&P as well as availability are integral parts of PM&P management. It is essential that PM&P engineering works closely with design engineering to prevent selection of parts and materials that are not readily available at the quality and reliability levels required for the mission as specified in the qualified product list (QPL) and qualified manufacturing line (QML). Designers' choice of technology (parts and materials) during this phase determines subsequent cost, schedule, and reliability of the end system. The program approved selection and as-designed PM&P lists should be independently reviewed with respect to available databases of past

performance of similar PM&P items. Similarly, selected suppliers' past performance should also be independently reviewed utilizing available databases with issues being identified to the MA and program management organizations.

During production planning and PM&P procurement, emphasis is placed on supplier selection and supply chain management, where technical requirements/performance, cost, and schedule are monitored on a continuing basis. Communication is essential to assure requirements are being met at both the supplier and subcontractor level and to provide a means of assessing technical and schedule performance. MA should assure a seamless operation.

While it is recognized that developers' current procurement practices tend to select many of their parts and materials from the QPL and QML certified by Defense Supply Center Columbus (DSCC), it remains the responsibility of the developers and procuring agency to assure that the requirements of the program have been imposed and are being met. Where QPL/QML-specified parts are not available or where parts do not meet program requirements, the developer must either upgrade the devices or prepare a procurement source control drawing to impose those specific requirements. The MA processes include independent verification of parts selection, and source control drawings reflect that program requirements (including qualification) and the as-executed part qualification program and quality conformance inspections (QCI) were successful. All PM&P-related failures during production and test, starting at the QCI and lot destructive physical analysis (DPA), are independently assessed for reach back and appropriate corrective actions. The common MA theme during these activities is based on the adage, "trust, but verify."

A PM&P control board (PM&PCB) or designated integrated product team (IPT) is established to address numerous workaround plans and minor waivers, allowing the program to go forward while attempting to maintain product integrity. MA augments this activity by providing independent assessments through audits and continuing peer reviews. As a goal, PM&PCB activities should appear seamless across developers and vendors, with common format and requirements being imposed on all.

A wide range of skills and knowledge bases is required to support these activities. These include an in-depth understanding of applicable military standards for various types of PM&P and their associated

standard testing methods, such as MIL-STD-883. A thorough understanding of the underlying technologies and their application (including hardness assurance requirements), along with a comprehensive understanding of the related industrial base, is also required to assure the lowest risk part or material is selected which meets system performance needs. Similarly, manufacturing engineers are required to select low-risk, qualified, reliable processes. Because of the diversity of required skills and knowledge, a team of technical specialists is normally required. MA should assess depth and breadth of the government/contractor PM&P engineering team.

13.4 Strategies and Execution by Phase

MAG Phase 0

During this phase (requirements and concept definition/acquisition planning), government PM&P provides support to concept studies and provides input to the request for proposal (RFP) that goes out to contractors to bid on.

MAG Phase A

During this phase (system definition/concept development), the government PM&P verifies the contractor's PM&P control program plan accomplishes the following: 1) defines all tasks and subtasks that apply to the selection, application, procurement and testing, etc. of PM&P; and 2) assures the PM&P control program is consistent with operational requirements and mission needs.

MAG Phase B

During this phase (preliminary design), as the design and development are initialized, the PM&P process is refined. The government evaluates contractor and subcontractor PM&P control plans for adequacy and adherence to the tailored PM&P requirements documents and verifies their PM&P process is in accordance with program requirements. Government participates in PM&PCBs. Government access assures consistency of PM&P requirements across all subcontracts.

MAG Phase C

PM&P management is evaluated during MAG Phase C (complete design). As-designed parts lists are reviewed for early identification of risky items to facilitate replacement and minimize cost and schedule impact.

MAG Phase D1

During MAG Phase D1 (fabrication and integration) PM&P documents are updated and verification is to be provided, indicating that the contractor maintained and updated the PM&P control program plan, the program-approved parts list (PAPL), and other PM&P documents. Documentation is verified to realistically reflect the "as-built" configuration. During this phase, functional configuration audits (FCAs) and physical configuration audits (PCAs) are reviewed to assure thoroughness, completeness, and traceability requirements are met. This phase assures that all noted PM&P discrepancies/nonconformances and issues have been dispositioned in accordance with material review board or PM&PCB procedures. This phase also verifies that the functional and product baselines have been established.

During this phase, PM&P verifies that PM&P engineering performed failure analysis of failed electrical-electronics parts; verifies that analyses were carried out to the extent necessary to establish root cause and identify corrective action; assures extensive characterization and, if necessary, performs independent characterization; and verifies that the PM&PCB reviewed the results of the failure analysis and ruled on the validity of the cause and corrective action.

MAG Phases D2 and D3

During MAG Phase D2 (fielding and checkout) and MAG Phase D3 (operations and disposal), PM&P expertise is provided in support of on-orbit anomaly investigations.

13.5 Organization of Tasks

Within the Mission Assurance Verification Matrix (MAVM) task database, PM&P tasks are first assigned to one of the following seven MAG phases:

1. Phase 0: Pre-KDP A Concept Studies
2. Phase A: Concept Development
3. Phase B: Preliminary Design
4. Phase C: Complete Design
5. Phase D1: Fabrication and Integration
6. Phase D2: Fielding and Checkout
7. Phase D3: Operations and Disposal

Within each phase the task may then be either incorporated within one of the core MA processes, as illustrated in general terms in Figure 1.4-3, or directly associated with a program work breakdown structure (WBS) element within the general structure illustrated by Table 2.2-3.

13.6 Core MA Processes Supported by PM&P

During requirement analysis and validation, PM&P assists with the development of PM&P requirements for inclusion in the RFP, the assessment of PM&P policy, requirements, and plans conducted by the prime contractor, and assessment of the flow-down of PM&P requirements to subcontractors.

During design assurance, PM&P assists with assessments of the implementation of PM&P policy, plans, the documentation of individual part, material, or process needs consistent with PM&P program requirements, and participation in PM&PCB activities related to nonapproved parts selection, derating criteria, and new part qualification process assessment.

During manufacturing assurance, PM&P assists with audits of critical manufacturing processes, monitoring of PM&P qualification, and lot acceptance test results, with emphasis on assessing any deviation from the initial requirement set and/or appropriate corrective actions.

During integration, test, and evaluation, PM&P assists with the definition of accelerated life test requirements, analysis of life test data results, failure analysis of failed suspect parts and to resolve and implement corrective actions/Lessons Learned for any system anomalies that are traceable to PM&P.

During operations readiness assurance, PM&P assists with the review and analysis of launch and on-orbit anomalies.

During MA reviews and audits, PM&P is an agenda item at system requirements review (SRR), preliminary design review (PDR), critical design review (CDR), and flight readiness review (FRR), and participates in FCAs and PCAs.

13.7 Government and Contractor Enabling Tasks and Products

MAG Phase 0

Key Government Enabling Tasks:

- The system program office (SPO) requests The Aerospace Corporation to provide PM&P inputs to the RFP or statement of objectives (SOO).
- The government PM&P tailors the PM&P control program for space vehicles specified in Aerospace TOR-2004(3909)-3315 Rev. A, *Part, Material and Process Control for Space Vehicles* (replaces MIL-STD-1546). In this way, the project's unique and special requirements are incorporated into a project-specific tailored PM&P control plan.
- During this phase, government PM&P also tailors the technical PM&P requirements for space vehicles specified in Aerospace TOR-2004 (3909)-3316 Rev. A, *Technical Requirements for Electronic Parts, Materials, and Processes Used in Space Vehicles* (replaces MIL-STD-1547). In this way, the project's unique and special requirements are incorporated into a project-specific tailored PM&P technical requirements document.
- The primary PM&P objective of this phase is to assure the PM&P requirements in the RFP will result in the use of available, qualified, and reliable PM&P consistent with program objectives.
- The government typically requires contractors to have a document detailing the contractor's PM&P control program and technical requirements for PM&P for space vehicles.
- The SPO requests Aerospace to evaluate a contractor-generated proposal or statement of work (SOW).
- During source selection, government PM&P will evaluate contractors' proposals to assure they implement PM&P requirements in the RFP.

MAG Phase A

Key Government Enabling Tasks:

- The SPO requests Aerospace to provide PM&P inputs to the systems requirements document (SRD).
- The PM&P requirements are presented during the SRR, so that there can be agreement between the SPO and the contractor as to precisely what PM&P requirements are and how they relate to overall system and mission requirements.
- The SPO requests Aerospace to evaluate the contractor's system specification.
- The government verifies the contractor has organized, chartered, and empowered a PM&PCB to assure consistency of PM&P requirements set to required policy and directives.
- The government provides input at the system design review (SDR), defining top-level PM&P requirements for the contract, and verifies that assurance characteristics and control features are documented as part of the initial concept baseline. Assure that selected characteristics and associated assurances levels fully meet system requirements and mission needs.
- The government verifies the prime contractor has flowed-down PM&P requirements to the subcontractor to the extent necessary to meet system-level requirements. Assure consistency of PM&P requirements across all subcontracts. May participate in subcontractor selection.

MAG Phase B

Key Government Enabling Task:

- The SPO requests Aerospace to evaluate the contractor preliminary design PM&P process.

Key Contractor Enabling Tasks:

- Contractor is to prepare PM&P data products in accordance with the PM&P control plan commensurate with the maturity level of engineering data.
- During the preliminary design phase, the contractor generates data products in accordance with the requirements in the PM&P control plan. Such products include PM&P characterization data, PAPL, PM&P selection list (PMPSL),

preliminary parts list (PPL), PM&P approval requests (PARs), etc.

- Government PM&P evaluates these data products to assure they are of a maturity level commensurate with available engineering data, and to see that they accomplish what is required by the PM&P control plan.
- It is during this phase that there is verification of allocation and flow-down of PM&P requirements to include life-limiting material, aging, storage/environment, radiation effects, etc. The resulting design constraints on PM&P form a part of PM&P selection criteria and are outlined in the PM&P control plan.
- During MAG Phase B, the contractor's derating of PM&P is reviewed for compliance with requirements for long-term reliability in accordance with program requirements. Implementation of PM&PCB-approved policy for stress-derating across the program is verified at this phase. Stress deratings of parameter values needed to achieve lower failure rates of PM&P. EOL deratings are necessary to demonstrate circuits perform intended functions at EOL.
- Early identification of PM&P derating issues allows mitigation such as replacement, life testing, analysis, etc. that can minimize additional costs and schedule delays.
- The SPO requests Aerospace to evaluate the contractor's parts test plans.
- MAG Phase B is when the contractor's test plans are evaluated to assure parts tests will meet the PM&PCP objectives and will not damage the parts.
- A PDR is held during Phase B, at which time the preliminary design is presented. The contractor's PM&P process is presented as part of this PDR. After the contractor has satisfactorily presented the data products identified in this section, and they are found to be in compliance with requirements, the design and development proceeds next to MAG Phase C.

MAG Phase C

Key Government Enabling Task:

- The SPO requests Aerospace to evaluate the contractor's detailed design PM&P process.

Key Contractor Enabling Task:

- During MAG Phase C, the contractor is to generate data products for the PM&P control plan tasks to the maturity level commensurate with the maturity level of available engineering data.
- MAG Phase C PM&P data products and Aerospace/government PM&P review activities include:
- Evaluating procured parts quality levels and specifications.
- Evaluating final part stress analyses.
- Evaluating PM&PCB operations.
- Evaluating final parts radiation analyses.

These activities provide insight into the contractor's ability and progress toward meeting the flowed-down PM&P requirements.

During MAG Phase C the following is to be accomplished:

- Verify that PM&P engineering monitored all subcontractors' performance to assure that delivered products satisfy contractually flowed-down PM&P requirements and allocated PM&P design constraints.
- Verify the PM&P processes have been properly implemented to include review of PAPLs, as-designed part lists (ADPLs), derating analyses, non-standard part approval requests (NSPARs), PM&PCB minutes, etc.
- Verify the contractor's single event effects (SEE) analysis report. Certify the piece part SEE rate used in calculation of equipment outage rates is consistent with published (validated by parts engineering) SEE rates.
- Assure validity of piece part SEE rates used in SEE analysis. Verify the frequency of system outage (requiring ground assistance) satisfies specified system availability and dependability requirements.

- Verify that the contractor held regularly scheduled PM&PCB meetings for resolution/disposition of PM&P issues. Verify all PM&P issues were promptly resolved and effectively documented.
- Verify the contractor's worst-case circuit analysis (WCCA) is completed by CDR. WCCA is to be reviewed and certification given that parameter EOL limits used in node calculations are consistent with EOL deratings (radiation and aging deratings) issued by PM&P engineering and specified in the program EOL derating document. WCCA is to be reviewed and certification given that the electronic/electrical/ electromagnetic (EEE) parts' electrical and temperature stress derating factors in the report comply with the mandated stress derating factors for the program.
- Assure validity of piece part failure rates used in reliability analyses, based on stress derating factors mandated for the program.
- Verify degradation limits of critical parameters for use in worst-case design. Verify that radiation degradation limits are derived from radiation test data. Verify that aging degradation deltas are derived from burn-in and life test deltas. Assure that degradation limits information is made available to designers in a timely fashion to allow assessment as to whether or not piece part has the required EOL margin.
- Verify characterization data (including radiation characterization) and qualification testing of new PM&P. Assure timely assessment of PM&P capabilities. Assure timely generation of radiation degradation limits for use in RLAT and worst-case design.

All of the PM&P products listed above are to be successfully completed, evaluated and approved prior to CDR. When CDR is successfully completed, MAG Phase C can be considered completed and will advance to MAG Phase D (build/operations).

13.8 References

Policy-related

Specifications and Standards

Aerospace TOR-2006(8583)-5235	*Parts, Materials, and Processes Control Program for Space and Launch Vehicles*, 08 November 2006
Aerospace TOR-2006(8583)-5236	*Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles*, 13 November 2006
Aerospace TOR-98(1412)-1, Rev. A	*Electronic Parts, Materials, and Processes Control Program for Expendable Launch Vehicles*, 01 January 2004
MIL-STD-1556B	Government/Industry Data Exchange Program (GIDEP) Contractor Participation Requirements, 24 February 1986

Technical Handbooks

MIL-HDBK-965	Acquisition Practices for Parts Management (for GIDEP Application Guidance Manual), 30 September 1996
Aerospace TOR-2006(8506)-4494	*Space Vehicle Systems Engineering Handbook*, 31 January 2006
Aerospace TOR-2006 (8546)-4591	*Space Vehicle Test and Evaluation Handbook*, 06 November 2006

Deliverables

DI-MISC-80526D	Parts Management Plan, 05 August 1998

DI-MISC-80071E	Parts Approval Request, 05 August 1998
DI-MISC-81277	Parts, Materials, and Processes Selection List, 27 July 1992
DI-RELI-80255	Failure Summary and Analysis Report, 17 October 1996
DI-RELI-80253	Failed Item Analysis Report, 17 October 17 1986
DI-QCIC-80125B	Government Industry Data Exchange Program (GIDEP) Alert/Safe-Alert Report, 05 May 2003
DI-MGMT-81453	Data Accession List (DAL), 23 January 1995
DI-MGMT-81334	Contract Work Breakdown Structure (CWBS), 01 February 2005

Chapter 14
Quality Assurance

Dana J. Speece
Product and Process Assurance Department
Gary D. Shultz
Product and Process Assurance Department

14.1 Introduction

Quality assurance (QA) is the engineering and management specialty discipline that ensures that a customer-ordered product meets the customer-specified performance parameters. QA activities are related to and support many other disciplines such as reliability engineering, configuration management, parts, materials, and process engineering, safety engineering, systems engineering, manufacturing engineering, purchasing, and systems integration and test. One of the primary goals of QA is to ensure deliverable products are based on established design and workmanship standards.

A QA program provides an organizational framework and implements process controls that are the most conducive to assuring product quality. Basic quality system process controls are put into effect at the system contractor and at associated subcontractors and suppliers. When well defined and implemented, a QA program assures that all quality requirements are met through control of operations, processes, procedures, testing, and inspection.

The government program office team establishes QA requirements for each program via contract and also verifies conformance to those requirements. The contractor flows QA requirements to subcontractors and suppliers in order to successfully execute QA program for NSS programs.

14.2 Definitions

The **quality** of a product is the degree to which the product attributes, such as capability, performance, or reliability, meet the needs of the customer or mission, as specified through the requirements definition and allocation process.

Quality assurance is the technical and management discipline to ensure that a customer-ordered product meets the customer-specified performance parameters.

14.3 Objectives

The primary objective of a contractor's comprehensive QA program is to ensure that the contractor's hardware and/or software products meet the contractual requirements and specific released design documentation. Contractor quality engineering defines and supports the implementation of the program/project QA activities as defined by the contract and program quality plan. Second, contractor quality engineering ensures that the contractor and the subcontractor's/vendor's plans satisfy those requirements. Finally, contractor quality engineering provides oversight of all contractor activities that may have an impact on product quality throughout the life of the contract. In particular, a good QA program implemented by the developer:

- Demonstrates recognition of the quality aspects of the project and the importance of an organized approach
- Ensures that quality requirements are determined and satisfied throughout all phases of the project
- Ensures that quality considerations are fully included in all systems and all operations
- Provides for the detection of potential problems, which could result in less than satisfactory performance
- Provides for timely and effective corrective action

14.4 Practices and Tasks

The basic practices and tasks of a contractor's quality system process include the following:

- Establish, document and maintain a quality management system (QMS) to continually improve its effectiveness. QMS documentation includes documented statements of quality policy, quality objectives, and a quality manual. The quality manual establishes the scope and documented procedures of the QMS. Documents required by the QMS must be controlled to assure that documents are approved for adequacy prior to issue, changes are re-approved, status of the document identified, and relevant versions of the applicable documents

are available to prevent the unintended use of obsolete documents.

- Establish management responsibility so that top management provides evidence of its commitment to the development, implementation, and improvement of the quality management process by communicating the importance of meeting requirements, establishing the quality policy, conducting reviews, and ensuring the availability of resources. Top management reviews the organization's QMS at planned intervals. These reviews include: results of the audits, results from customer feedback, process conformance, and product conformity audits, status of preventative and corrective actions, status of follow-up actions from previous management reviews, potential changes that could affect the QMS, and recommendations for improvement.
- Verify that the QA provisions and requirements adequately reflect mission needs.
- Perform initial quality planning, which encompasses the processes required to review, document, and flow-down requirements imposed from the customer, statutory, regulatory, and contractor's internal organization. The document used to document these requirements is normally referred to as a quality plan. A quality plan is developed by the contractor and submitted to the customer for approval. Once established and documented in the quality plan, the quality requirements are flowed-down through the contractor's internal organizations, suppliers, and vendors through documented media.
- Maintain quality involvement in the design review process, which is another aspect of initial quality planning. Product designs are reviewed for process requirements and the ability of personnel to manufacture/inspect the product as designed.
- Maintain design control by using a pragmatic methodology to evolve a system's design through the use of a system of baselining product design at various stages of maturity during development, including process planning for task sequence, mandatory steps, significant stages, method of configuration control, review, verification, validation, responsibilities and authority. Also manage interfaces between different groups involved in the design and development to ensure effective communication and clear assignment of responsibility.
- Control and identify design changes with well-maintained records. The design is normally frozen at the critical design

review (CDR) just before approval is given to begin manufacturing. Changes from that point forward are required to be processed through the formalized configuration management process.

- Validate that there is a process that assures the adequacy of the specified requirements in the purchase documentation prior to transmittal to the supplier/vendor. This includes a review to assure that the purchase is being directed to an approved supplier/vendor. Approved suppliers/vendors have been periodically reviewed/evaluated for their ability to supply products in accordance with the organization's requirements.
- Establish a system to verify purchased product, including obtaining objective evidence of the quality of the product from the suppliers and verification by the contractor. Verification by the contractor may be accomplished by inspection of the product at the supplier's facilities, by inspection of the products upon receipt, or by delegation of verification to the supplier.
- Establish a contractor's quality control organization to assure that production operations, including inspection operations, are carried out in accordance with approved data. Approved data contains drawings, parts lists, production documents (e.g., manufacturing plans, traveler, router, work order, or planning). Changes to the approved data is documented and approved by an authorized contractor representative.
- Ensure that each developer provides the resources needed to implement and maintain the QMS and enhance customer satisfaction by meeting customer requirements. The quality organization determines the necessary competence for personnel performing work that has an affect on product quality, and provides training or takes other actions to satisfy these needs. Records must be maintained on education, training, skills, and experience. The organization shall also provide buildings, workspace, process-equipment, and support services needed to achieve product quality.
- Maintain the identification and traceability of the product throughout product realization. Identification of the configuration of the product is maintained in order to identify any differences between the actual configuration and agreed configuration. Media used as an acceptance authority (e.g., stamps, electronic signatures, passwords), shall be controlled by established and documented controls.

- Task the contractor's quality organization to assure a disciplined manufacturing system and verify that the contractor has identified and controlled all the manufacturing processes that can affect product quality. This includes the establishment of workmanship standards and certifying assemblers and inspectors for special processes such as soldering and welding.
- Task the contractor's quality organization to assure the conformity of the product during internal processing and delivery. This includes acceptability assessments of products at all stages of assembly and test. Product verification activities such as inspections and tests are performed to ensure that deliverable products meet the customer's specified requirements. Preservation of the product includes identification, handling, packaging, storage, and protection.
- Determine the monitoring and measurement to be undertaken and the measuring devices needed to provide evidence of conformity of the product. The contractor maintains a register of these monitoring and measuring devices and defines the process employed for their calibration and recall to calibration. Records include data from the calibration process and acceptance requirements.
- Monitor and measure product characteristics to verify that product requirements have been met. The product is not to be used until it has been inspected or otherwise verified as conforming to specified requirements, except when released under positive recall procedures pending verification of conformance. This includes control of quality records to provide satisfactory evidence that the contractor-developed product meets customer requirements.
- Maintain inspection documentation, including criteria for acceptance and/or rejection, the sequence of measurement and testing operations that are performed, and a record of the measurement results and required measurement instruments.
- Establish a procedure regarding nonconformance. A nonconformance resulting in a departure from contract requirements requires authorization from the customer, unless the customer has authorized use-as-is or repair dispositions for the product. Product dispositioned scrapped shall be conspicuously and permanently marked or positively controlled until as becomes physically unusable.
- Identify and control nonconforming products to prevent unintended use or delivery. A documented procedure is

required for controls, responsibilities, and authorities for dealing with nonconforming product. One or more of the following ways may be used to deal with nonconforming product:

To assure that nonconformances are not repeated, develop documented procedures to identify the root causes of nonconforming materials and/or processes and correct them through a corrective action process. A preventative action process should be in place to eliminate the cause(s) of potential nonconformances in order to prevent their occurrence.

- In order to prove that the end item or product satisfies the requirements and conforms to specified manufacturing processes so that each end item meets user expectation outputs, collect a variety of data, including quality objectives and requirements of the product, required processes and documents, required verification, monitoring and inspection, and records required to provide evidence of product realization. This includes acceptability assessments of products at all stages of assembly and test.
- The contractor and/or subcontractors shall exercise care with customer property and have a process to identify, protect, safeguard, and notify the customer of lost or damaged customer property.
- The contractor's quality organization shall participate in key program reviews to evaluate the effectiveness in implementing specific contractual QA requirements that ensure compliance with the overall contract technical requirements. These reviews include system requirements reviews (SRRs), design reviews, producibility reviews, manufacturing reviews, test readiness reviews (TRRs), material review boards (MRBs), failure review boards (FRBs), pedigree reviews, hardware acceptance reviews (HARs), and independent readiness reviews (IRRs).
- Implement a process to monitor, measure, analyze, and improve the effectiveness of the QMS. Methods are applied to monitor the ability of the QMS processes to achieve the planned results. When planned results are not achieved, appropriate action is taken to correct the nonconforming processes. An evaluation is conducted to determine if the nonconforming process has resulted in product nonconformance. This also includes internal quality audits to

periodically to ensure the contractor's quality system is effective and maintained.

- Conduct audit activities related to manufacturing and testing of the product, including first article inspection, functional configuration audits (FCAs), physical configuration audits (PCAs), quality system audits (QSAs), and contractor and subcontractor/supplier audits.

14.5 Strategies and Execution by Phase

Traditionally, QA has predominately played a strong role in the "build" acquisition life cycle phases (MAG Phases D1-D3). More recently, contractors and the government have realized that many quality concerns and system failures could have been averted had the QA discipline played a stronger role during the development and design phases of programs. This guide reflects such an expanded role of QA.

Even in Phase Pre-KDP A (concept study), QA plays a role by assuring that quality principles will be adequately addressed during the life of the program. This activity may take the form of verifying that quality requirements are included in the request for proposals (RFPs). Early contractor site visits may include a check for the existence of a robust QMS, especially in facilities developing new technology or contractor sites at which the government does not have prior experience. The advantage of QA involvement at this early stage is if the quality emphasis is found lacking, there is time to correct the issue before contracts are firmed up.

During MAG Phase A (concept development), while trade studies and baselines are being defined, QA should be performing a top-level review of the potential contractor's QMS. Particular attention at this early stage should be dedicated to reviewing corporate vision, quality goal setting, and strategic planning. Superior communication within the organization should be present, so a review of policy deployment, flowdown of information, and strategic planning capabilities is in order. Past performance may be evaluated to determine the contractor's ability to identify product key characteristics, develop measurable process outputs, and produce product that meet the intended requirements. Additional tasks associated with Phase A (such as assessment of the contractor's program quality plan and facility capabilities) are used to support decisions leading to SDR.

During MAG Phase B (preliminary design), QA plays a role in more thoroughly evaluating the contractor's QMS. Specifically the approaches to control purchased product, variability reduction efforts, requirements flowdown, change management (in processes and specifications), risk mitigation methods, the transition from development to production, and imbedding quality requirements into contract deliverables must be reviewed for maturity. Finally, an evaluation of the contractor's ability to properly manage its suppliers is accomplished by assessing the contractor's purchasing process, reviewing the supplier control plan, and participation in supplier site surveys, particularly those conducted with new suppliers or at new facilities. During Phase B, QA is also involved in evaluating the adequacy of quality assurance requirements in the draft statement of work (SOW), associated contract deliverables, and the preliminary design review (PDR) documentation.

As MAG Phase C (final design) is completed, QA is more engaged with evaluating the inner workings of the contractor's QMS. Tasks such as participating in internal and third-party audits, reviewing stamp control, engineering and manufacturing systems, standards and specifications, training and certification, calibration of equipment and tooling, workmanship standards, supplier controls, change control, and handling of nonconformities all must be accomplished. Notice that these efforts are more leveraged if they are done before manufacturing is fully engaged. Finally QA participation in manufacturing readiness reviews (MRRs) and the CDR process helps reduce quality risk to the program.

In MAG Phases D1, D2, and D3 (build, checkout, and operation stages), QA is involved with determining if the product was built to specification and if it performs as intended. Hence, QA will participate in manufacturing and assembly process audits, MRBs and FRBs, TRRs, integration and test activities, FCAs and PCAs, pedigree reviews, HARs, and corrective action boards (CABs). When hardware moves to the launch site, QA reviews the launch site QA plan and monitors the facilities for adherence to process. Should launch or on-orbit failures occur, QA may be involved in root cause determination.

Overall, the flow of QA through the life cycle process is one of evaluating quality systems from the top level at an early stage in the life cycle. If issues are found, quality controls can be established in a more cost-effective manner than later in the life cycle. Before production is fully engaged, QA is involved with determining if the QMS really

operates at the production level. Again, if done during design, problems may be corrected before mistakes are made in the hardware. If these steps are successfully completed, the QA role during build and deployment is one of monitoring systems for continued success.

14.6 Organization of Tasks

The QA supporting discipline has a limited role to play in the initial stages of the acquisition phase. While concept studies and development are taking place, it is important to have the government identify the role that quality will play throughout the life of the program. Therefore in Phases Pre-KDP A and A, the QA supporting discipline is tasked with making sure quality requirements will be identified and flowed down through the contract. It also begins verifying that the contractor possesses an adequate QMS. In addition, QA must determine any weaknesses that exist as the transition is made from development to production and have them addressed before the contract is signed.

As the design matures and the transition to production begins, the QA supporting discipline takes on its more traditional role of verifying quality requirements. Audits may be conducted and participation in the MRBs and FRBs takes place with the goal of assuring the QMS is continuing to function well. Completed hardware may undergo pedigree reviews in preparation for integration and next level test activities. At the launch site, QA is required to assure the safety of the hardware will be maintained through launch. Once on-orbit, the quality role is reduced significantly and supports the program when anomalies occur and records must be retrieved. In addition, QA plays a role when on-orbit anomalies indicate changes must be made in the fleet prior to launch.

14.7 Core Mission Assurance Processes Supported by Quality Assurance Tasks

During Phases Pre-KDP A and A (concept study and development), QA directly supports risk reduction efforts by concentrating on the health of the contractor’s QMS. This aligns with the Lessons Learned activities, contract review, and in general the systems evaluation approach of integration, test and evaluation (IT&E) and mission assurance reviews and activities (MARA) work. In addition, QA may evaluate engineering systems for adherence to command media. Design assurance (DA) and requirements analysis and verification planning (RAVP) depend on the proper operation of these systems for data input.

QA results may support any DA and RAVP system effectiveness evaluations. Quality audits performed by QA directly support the efforts of manufacturing assurance as they attempt to verify the reliability and repeatability of the manufacturing system and to determine if the correct processes are in place.

During Phase B, QA audits would be gathering information on configuration management as well as parts, materials, and process controls. DA needs this information to evaluate the proposed design options. Furthermore, audit results would directly support the need of manufacturing to evaluate process qualification control and traceability, as well as the test planning and program effectiveness (including failure review) conducted by IT&E. QA works closely with manufacturing assurance to assess design reviews for completeness and adequacy.

As the design is finalized, in-depth audits by QA assure the transition from design to manufacturing is supported by the contractor's systems. This helps DA, manufacturing assurance, and IT&E assure that systems are in place to not only correctly implement the design but also learn from mistakes made. In addition QA supports the various design reviews that DA, manufacturing assurance, and IT&E would attend, including the MRR and the CDR.

In MAG Phases D1, D2, and D3 (build), QA assists RAVP, DA, manufacturing assurance, IT&E, and MARA in verifying that the product was built to specification and performs as intended. Often these processes overlap in their support of various audits and technical reviews. QA would verify that the nonconformity and failure reporting systems these processes depend on are functioning properly. The earlier QA activity of checking various manufacturing and test systems directly supports the needs of operations readiness assurance (ORA), the data may be needed for addressing anomalous behavior in the hardware.

14.8 Government and Contractor Tasks and Products

In Phase Pre-KDP A, much of the QA supporting discipline depends on the government addressing the tailoring of quality requirements and their subsequent flowdown. This activity is based on Lessons Learned, often summarized in a checklist; any contractor selections should be influenced by the contractor's attention to quality as evidenced through the results of government surveys conducted during site visits or the contractor's quality performance on previous contracts. Additional

documents such as architecture views and technology development studies are useful input to the QA supporting discipline.

During Phase A (concept development), the QA supporting discipline requires the government release of the SRR, SDR, and interface control document (ICD). Often these documents will not address quality directly, but QA must advocate for the inclusion of quality requirements at the earliest stages when required. The acquisition decision memorandum (ADM) and analysis of alternatives (AoA) must also be reviewed for the inclusion of appropriate quality issues. Any government pre-source selection activities should involve the QA supporting discipline. The contractor is required to make available sufficient internal documentation for QA to verify the QMS is functioning appropriately. When a contractor submits a proposal, the quality program plan should be provided for review by QA. In addition, the contractor's quality history should be reviewed using results of ISO 9001:2000 or AS9100 third-party audits. At issue in this phase is not only assuring that the contractor has the capability and past history to incorporate a quality approach to product realization, but also more importantly that the contractor's QMS is mature enough to design and build quality into the product.

In Phase B, the QA supporting discipline is concerned with the completion of the technology development activities and the preparation for production. QA must review government documents such as the SOW, the capabilities development document, and capability production document for the inclusion of quality requirements. QA may suggest that these quality requirements be enhanced or clarified to avoid future contractual and production problems. QA will participate in audits and site visits of the contractor and their suppliers. The contractor must demonstrate that its design review process is robust, make-buy decisions are appropriately addressed, it exercises the necessary controls over suppliers, and that it can perform adequate trade studies regarding the reuse of technology. The contractor should especially demonstrate how developmental work will be transitioned successfully to the production phase.

As design is matured in Phase C, QA is engaged in the preliminary design reviews (PDRs) and critical design reviews (CDRs) as well as first article review. The QA supporting discipline advises the government on how well the contractor addresses quality in the design phase and the expectations for quality control during the production

phase. The contractor makes its facilities and personnel available for evaluation and QA will participate in various audits.

As the build completes in Phase D and testing begins, the contractor supplies a TRR document. QA is engaged in reviewing action items and corrective action documented by the contractor in several tracking systems: manufacturing nonconformities, test failures, engineering changes, configuration, and contract data requirements list (CDRL) submissions are examples of categories of involvement. The government may organize FCAs and PCAs. The QA supporting discipline will participate in these as well as pedigree reviews and HARs. The launch provider will also submit a launch site QA plan for review. In the final stage, QA must verify that the QMS functioned properly during the life of the program. Any weaknesses must be evaluated for risk before the system is launched.

14.9 References

The QA supporting discipline draws its requirements mainly from the Joint Capabilities Integration and Development System (CJCSI 3170.01D) as well as the DOD Directive on Defense Acquisition System (DODD 5000.1) and its accompanying Instruction on the Operation of the Defense Acquisition System (DODI 5000.2). For guidance, QA will often use SAE Quality Systems Aerospace –Model for Quality Assurance in Design, Development, Production, Installation, and Servicing, January 2004 (SAE AS9100 Rev. B), as many aerospace contractors are registered to this standard. The Aerospace Corporation has developed *Quality Assurance Requirements for Space and Launch Vehicles*, TOR-2005(8583)-3859, which provides detailed assistance based on Lessons Learned from acquisition and execution of successful space programs.

Policy-related

Specifications and Standards

SAE AS9100	Quality Management Systems – Aerospace – Requirements. Rev. B, January 2004
ISO 9001:2000	Quality Management Systems – Requirements, December 2000

Technical

MIL-STD-1520C	Corrective Action and Dispositioning System for Nonconforming Material, June 1986

Contracts that only require ISO 9001:2000 should consider the quality requirements:

MIL-Q-9858A, Quality Program Requirements, December 1963

MIL-STD-1586A, Quality Program Requirements for Space and Launch Vehicles, June 1989

MIL-I-45208, Inspection System Requirements, December 1963

Technical Handbooks

Aerospace TOR-2006(8506)-4494	*Space Vehicle Systems Engineering Handbook*, 30 November 2005
Aerospace TOR-2006(8546)-4591	*Space Vehicle Test and Evaluation Handbook*, 06 November 2006

Best Practices

The following report contains information that is of direct significance and assistance for the execution of tasks associated with the QA discipline as defined in this guide:

Aerospace TOR-2005 (8583)-3859	*Quality Assurance Requirements for Space and Launch Vehicles*, December 2005

Deliverables

DI-QCIC-80107	Quality Program Plan, 15 January 1986

Other

Critical Process Assessment Tool (CPAT)

Chapter 15
Systems Safety Assurance

Lucio U. Tolentino
System Delivery and Operations Department
Richard C. Maynard
CCAE Mission Assurance

15.1 Introduction

The **system safety assurance** discipline applies engineering and management principles, criteria, and techniques throughout the life cycle of a system to control system hazards within the constraints of operational effectiveness, schedule, and cost. System safety should be an inherent element of system design and is essential to system requirements. Successful system safety efforts depend on clearly identifying and mitigating hazards. System safety must be a planned, integrated, comprehensive effort employing both engineering and management resources.

15.2 Definitions

The **system safety** concept is the application of special technical and management skills to the systematic, forward-looking identification and control of hazards throughout the life cycle of a project. The concept calls for safety analyses to identify risk of loss or harm and hazard control actions, beginning with the conceptual phase of a system and continuing through the design, production, testing, use, and disposal phases, until the activity is retired. Risks to the environment and health of personnel are a subset of the system safety hazard analysis.

Hazards are real or potential conditions that directly or through induced effect cause injury, illness, or death to personnel; critical or catastrophic damage to or loss of a system, equipment, property; or the environment. It is the presence of a potential risk situation caused by a mishap or an unsafe act or condition. It is a condition or changing sets of circumstances that presents the potential for adverse or harmful consequences.

15.3 Objectives

A system safety risk management process is established and used to provide effective implementation of safety and occupational health policies. To assure risks are identified, the system safety management organization must be free to examine all areas of design, development, manufacturing, integration, test, operation, and maintenance.

The system safety program shall define a systematic approach to make sure that:

- Safety, consistent with mission requirements, is designed into the system in a timely, cost-effective manner.
- Hazards associated with each system are identified, tracked, evaluated, and eliminated, or the associated risk reduced to a level acceptable to project management throughout the entire life cycle of a system.
- Historical safety data, including "Lessons Learned" from other systems, are considered and used.
- Minimum risk is sought in accepting and using new technology, materials, or designs, and new production, test, and operation techniques.
- Actions taken to eliminate hazards or reduce risk to a level acceptable to project management are documented.
- Changes in design, configuration, or mission requirements are accomplished in a manner that maintains a risk level acceptable to project management.
- Consideration is given early in the life cycle to safety and ease of disposal (including explosive ordnance disposal), and handling of any hazardous materials associated with the system. Actions should be taken to minimize the use of hazardous materials and, therefore, minimize the risks and life cycle costs associated with their use.
- Significant safety data are documented as "Lessons Learned" and are submitted to data banks or as proposed changes to applicable design handbooks and specifications.

15.4 Practices and Tasks

The identification and understanding of hazards and their associated risk is the basic task of system safety. Management provides resources to identify hazards and their associated risks. A systematic approach of

hazard analysis and risk assessment is used to achieve acceptable safety risks. Identification and establishing potential risk mitigation alternatives and their expected effectiveness of each alternative or method is part of this risk management process.

The order of precedence for system safety hazard control is as follows:

- Eliminate hazards through design selection. If a hazard cannot be eliminated, reduce the associated mishap risk to an acceptable level through design selection. Ensure inherent safety through selection of appropriate design. Design features to eliminate hazards or control the risk to an acceptable level. Consider substituting less hazardous technologies, substances, or energy sources. Consider containment and isolation of hazards to limit damage. Consider reduction of energy levels.
- Incorporate safety devices. If the hazard cannot be eliminated through design selection, reduce the mishap risk to an acceptable level using protective safety features or devices. Consider such devices as fuses, circuit breakers, ground fault interrupters, burst disks, latches, catches, guards over moving machinery, switch guards, interlocks, or padding.
- Provide warning devices. If safety devices do not adequately lower the mishap risk of the hazard, include a timely detection and adequate warning system to alert personnel to the particular hazard. Consider using chemical sniffers, low oxygen level alarms, backup alarms, warning lights, and computer hazard monitoring and annunciation.
- Develop procedures and training. Where it is impractical to eliminate hazards through design selection or to reduce the associated risk to an acceptable level with safety and warning devices, incorporate special procedures and training to counter hazardous conditions. Hazardous operations and procedures should be identified and safety procedures are development to minimize the hazards. Ensure adequate warning/caution signs are properly posted. There should be training and certificate programs for hazardous operations. Procedures may include the consideration of personal protective equipment.

15.4.1 System Safety Analysis

There are various tools available to assist in implementing a system safety program to identify hazards and assessing their risks. The tools

can identify hazards in particular settings or at particular times in the system life cycles (i.e., the types of analysis), and those that are distinguished by differences in methodology (i.e., the techniques of analysis).

Elements of system safety programs have some or all of the following types of analysis performed:

- A preliminary hazard list (PHL) is created early in the system acquisition cycle to identify potentially hazardous areas for management emphasis. A PHL is simply a line item inventory of hazards, with no evaluation of probability/severity/risk.
- **Preliminary hazard analysis** (PHA) is an early or initial system study of potential loss events. It identifies safety critical areas to provide initial assessment of hazards and to identify requisite hazard controls and follow-on actions. Hazards associated with the proposed design or function shall be evaluated for hazard severity, hazard probability, and operational constraint.
- **Safety requirements/criteria analysis** (SRCA) relates the hazards identified in the system design and identifies or develops design requirements to eliminate or reduce the risk of the identified hazards to an acceptable level.
- **Subsystem hazard analysis** (SSHA) is designed to identify hazards in subsystems of a major larger system. The analysis would show functional failures of the subsystem resulting in accidental loss.
- **System hazard analysis** (SHA) determines the total system hazards/level of risk. It must integrate the output of the SSHA with emphasis on interactions on the subsystems.
- **Operating and support hazard analysis** (O&SHA) is conducted to identify hazards that may arise during operation of a system, to find causes of these hazards, recommend risk reduction alternatives and impose an acceptable risk to the system.

Descriptions of some deductive tools to systematically assess hazards include:

- **Fault tree analysis (FTA)** is a logic-tree method analyzing from the top-down. It is especially useful for analyzing the risks of foreseeable catastrophic events. It is also valuable in assessing the vulnerability of complex systems with many

integrated system elements. FTA can be complicated and time consuming but it can lead to a cost-effective means of reducing system vulnerability. Valid results can be obtained using short-cut methods without applying complex mathematics.

- **Combinatorial analysis using subjective information** uses stepwise-scaled subjective engineering judgment. The stepwise scales are assigned levels of probability to hazardous conditions or undesirable events. The events or conditions at these stepwise scales can be combined to induce system failures.
- **Event tree analysis** is a bottom-up method that determines system responses to an initiating "challenge." It can assess the probability of either an unfavorable or a favorable outcome. The initiating system challenge may be a failure or fault, an undesirable event, or normal operative commands. The method is especially useful for command-start/command-stop protective devices, emergency response systems, and engineering safety features. It is also useful for analyzing operating procedures, management decision options, and other non-hardware systems. Multiple coexisting system faults/failures can be analyzed. The method identifies and analyzes potential single-point failures, and it identifies areas of system vulnerability and low-payoff countermeasures.
- **Cause-consequence analysis** is a bottom-up symbolic logic technique that explores system responses to an initiating "challenge." It enables assessing the probabilities of unfavorable outcomes at each of a number of stepwise, mutually exclusive loss levels. The system challenge may be a failure or fault, an undesirable event, or a normal system operating command.

These are only a few of the analysis tools available to assist in implementing a system safety program. The available tools should be evaluated and selected as part of the system safety program.

15.5 Strategy and Task Execution by Phase

System safety is an inherent element of the system design process and provides system safety requirements to the design team during Phases 0-A. During Phases B-C, system safety is a member of the design team and supports discussions with range safety, engineering, testing plans, and handling plans. A large safety effort occurs during Phases B-C

when details of the systems, subsystems, operations, and support are fleshed out and hazards are being identified and mitigated. The increased detail and information during Phases B-C require a substantial system safety analysis that is captured in the initial draft of the *Missile System Prelaunch Safety Package* (MSPSP), or Accident Risk Assessment report (ARAR). During Phases D1-D2, system safety completes hazards analysis, tracks all hazard mitigation activities, reviews and monitors all hazardous procedures, and supports all packaging handling and transportation planning associated with the completed system hardware. Early participation and involvement in the life cycle of a system will ensure that system safety is properly addressed during system reviews and meetings with Range safety and other regulating organizations.

System safety is a systematic approach to make sure that safety, consistent with mission requirements, is designed into the system in a timely, cost-effective manner. Hazards associated with each system are identified, tracked, evaluated, and eliminated, or reduced to a level acceptable to the managing activity. Minimum risk is sought in accepting and using new technology, materials, or designs, and new production, test, and operational techniques. Actions taken to eliminate hazards or reduce risk to a level acceptable are documented. Changes in design, configuration, or mission requirements are accomplished in a manner that maintains a risk level that is acceptable. Consideration is given early in the life cycle to safety and ease of end-of-life disposal. Actions should be taken to minimize the use of hazardous materials to minimize the risks and life cycle costs associated with their use.

15.6 Organization of Tasks

The Mission Assurance Verification Matrix (MAVM) task database for system safety is organized in a hierarchy using the MAG phases discussed above. For each life cycle phase, the process is further organized into the following categories: Program Planning, Systems Engineering, and Space Systems.

Program planning includes an evaluation of the contractor's system safety plan, management plans for interaction with Range safety and other regulating agencies, the contractor's programmatic environment, safety, and occupational health evaluation (PESHE) document, and the initial National Environmental Policy Act (NEPA) completion schedule to ensure that a good system safety

process is in place and accessible by the system program office (SPO) technical team.

System engineering includes a series of tasks to ensure that the system safety process traces to all interfacing processes and that there are adequate participation, system safety tools and resources for conducting all system safety activities.

Space systems system safety tasks are required to evaluate whether the contractor's system safety process at lower levels successfully flows up possible hazards to the system operation in the space environment.

Within each category described above, system safety tasks are further organized by level of assembly: unit, subsystem, system, and segment.

15.7 Core MA Processes Supported by System Safety

During requirements analysis and validation, system safety assists with the development of system safety requirements for inclusion in the request for proposal (RFP), the assessment of allocated safety requirements conducted by the prime contractor, and assessment of the flow-down of safety requirements down to subcontractors.

During design assurance, system safety assists with the assessment of hazards analysis studies, the assessment of critical hazards mitigation, and review of required safety documentation.

During manufacturing assurance, system safety assists with a review of safety-critical processes, procedures, hazardous materials, and safety inspections.

During integration, test, and evaluation, system safety assists with the definition and review of hazardous testing processes and procedures, handling and transportation procedures, and witnessing of critical handling operations.

During operations readiness assurance, system safety assists with the collection, review, and analysis of pre-launch mishap reports and review of space vehicle fuelling operations.

During mission assurance reviews and audits, system safety is an agenda item at system requirements review (SRR), preliminary design

review (PDR), critical design review (CDR), and flight readiness review (FRR).

15.8 Government and Contractor Enabling Tasks and Products

During concept studies, a **system safety program plan** (SSPP) should be created to develop a systematic planned approach to accomplishing system safety tasks. The SSPP would establish a system safety organization to accomplish the tasks, establish lines of communication with other elements of the system, establish authority for resolution of identified hazards, establish incident alerting and notification and mishap reporting, and define system safety milestones for inputs/outputs.

Before SRR in MAG Phase A, a PHL should be created. The compiled list of hazards will allow early management emphasis on system risks early in the system's life cycle. The PHL will identify possible hazards inherent in the concept and identify risks generated by the hazards. Concept development (Phase A) activities include producing the initial PESHE document detailing the program office's strategy and responsibility for integrating environmental safety and occupational health (ESOH) into the systems engineering process, the risk matrices and data elements required for ESOH risk management, and an initial NEPA completion schedule. Also, a comprehensive plan for human systems integration (HSI) should be developed.

Before PDR, a PHA should be performed and documented in MAG Phase B. This initial assessment will identify the anticipated safety problems within a system. The PHA will identify and document safety-critical items. It will identify and document preliminary safety requirements and constraints of the system to be placed in the specifications. MAG Phase B activities should include updating the initial PESHE with ESOH risk management data (e.g., identified hazards, risk assessments, mitigation decisions, residual risk acceptance, ongoing assessments of the effectiveness of mitigation measures and documenting in the PESHE and the status of planned and completed NEPA documentation). Also, initial planning for system disposal should be conducted.

In MAG Phase C, a SSHA is prepared. This verifies subsystem compliance with specification safety requirements. The SSHA will identify previously unidentified hazards associated with component

failure modes, critical human error inputs, and functional relationships between subsystem components. It will provide recommended action to eliminate hazards and control associated risk to acceptable levels of risk. Also before CDR, a SHA is prepared. The SHA will verify system compliance with safety requirements contained in system specifications. It will identify previously unidentified hazards associated with subsystem interfaces and system functional faults. The SHA will assess risk associated with total system design, including software and subsystem interfaces. The SHA will recommend actions to eliminate identified hazards, control associated risk to acceptable levels, and define training and procedure requirements for operations and maintenance. Updating the PESHE and system disposal planning should be continued.

In MAG Phase D, an O&SHA is prepared. This will evaluate operational and support procedures for potential introduction of hazards or risk and adequacy in controlling identified hazards or risks. The O&SHA will evaluate adequacy of personnel protective devices and life support equipment. It will evaluate the adequacy of personnel safety training and emergency procedures. Updating the ESOH risk database, the NEPA documentation, and completion status should be continued. Complete system disposal planning. MAG Phase D ends with system disposal.

15.9 References

Policy-related

Guidance for DOD Space System Acquisition Process. National Security Space Acquisition Policy, Number 03-01, 12 December 2005

AFI 91-202	USAF Mishap Prevention Program
SMCI 63-1201	Assurance of Operational Safety, Suitability and Effectiveness for Space and Missile Systems
SMCI 63-1205	Space System Safety Process

Specifications and Standards

AFSPCMAN 91-710	AFSPCMAN Range Safety User Requirements Manual, Volumes 1–7, 01 July 2004
MIL-STD 882C	System Safety Program Requirements, 19 January 1993

Technical Handbooks

Air Force System Safety Handbook 1991
Air Force Safety Agency, Kirtland AFB, NM

Programmatic Environmental, Safety, and Health Evaluation (PESHE) Guide, 25 February 2002, Space and Missile Systems Center

Aerospace TOR-2006 (8506)-4494	*Space Vehicle Systems Engineering Handbook*, 31 January 2005
Aerospace TOR-2006 (8546)-4591	*Space Vehicle Test and Evaluation Handbook*, 06 November 2006

Data Deliverables

DI-SAFT-81065	Safety studies report, 19 January 1993
DI-SAFT-81066	Safety studies plan, 19 January 1993
DI-SAFT-80105A	System safety program progress report, 19 January 1993
DI-SAFT-80103A	Engineering change proposal systems, 19 January 1993
DI-SAFT-80101A	System safety hazard analysis report, 19 January 1993
DI-SAFT-81299A	Explosive hazard classification data, 19 January 1993

DI-SAFT-80104A	Waiver or deviation system safety report, 19 January 1993
DI-SAFT-80100A	System Safety Program Plan (SSPP), 19 January 1993
DI-SAFT-80102A	Safety Assessment Report (SAR) 19 January 1993
DI-SAFT-81300	Mishap Risk Assessment Report, 19 January 1993

Other

Critical Process Assessment Tool (CPAT)

Chapter 16
Software Mission Assurance

Colleen M. Ellis
Computer Applications and Assurance Subdivision
Suellen Eslinger
Software Engineering Subdivision
Leslie J. Holloway
Software Engineering Subdivision
L. David Lutton
Computers and Software Division

16.1 Introduction

This chapter defines a set of tasks that could be performed by personnel from The Aerospace Corporation (Aerospace) for a Space and Missile Systems Center (SMC) program office to increase the probability of mission success for the software aspects of the system acquisition. These tasks also could be performed for a program office under some other government organization. System acquisition at SMC is governed by the policies defined in the National Security Space Acquisition Policy, Number 03-01, *Guidance for DOD Space System Acquisition Process* [NSS04], commonly referred to as NSS 03-01. In the context of [NSS04], system acquisition is defined as the entire life cycle of the system, including concept studies, concept development, preliminary design, complete design, and build and operations. Since many space systems are software intensive, software acquisition forms a significant part of the system acquisition process. This chapter will discuss the software acquisition tasks for **software mission assurance (MA)** within the context of the system acquisition process as defined in [NSS04].

As defined in Section 1.1.1, **mission assurance (MA)** is defined as the disciplined application of general systems engineering, quality, and management principles towards the goal of achieving mission success, and, toward this goal, provides confidence in its achievement. MA focuses on the detailed engineering of the acquired system and, toward this objective, uses independent technical assessments as a cornerstone throughout the entire concept and requirements definition, design, development, production, test, deployment, and operations phases.

Applying that definition to software, MA for software is the disciplined application of *software* engineering, acquisition, and management principles, processes, and standards to achieve mission success. Effective MA for software depends on performing certain practices and tasks correctly and completely, starting early in the system acquisition life cycle. Government pre-contract award acquisition strategy, planning, requirements definition, risk assessment, and cost and schedule estimating are the enablers for establishing a feasible, executable program—the prerequisites for mission success. Therefore, the quality of the government acquisition team's pre-contract award tasks has very high leverage for MA of software. In addition, the supplier performs many of the activities to ensure mission success, so defining the right supplier activities at contract award is also critical.

The tasks defined in this chapter are organized in accordance with the system acquisition life cycle defined in [NSS04]. They represent a complete set of activities that could be performed by Aerospace personnel during the life cycle of the system acquisition. Each program office would need to tailor the activities described in this chapter to the risks, requirements, and constraints of its program. The result of this tailoring process would constitute an agreement between The Aerospace Corporation and the government program office for the tasks that Aerospace will perform. This agreement could be captured in a document that is referred to as the mission assurance plan (MAP). The MAP should be consistent with the program's integrated master plan (IMP), systems engineering plan (SEP), and software acquisition management plan (SWAMP).

16.2 Chapter Organization

This chapter is organized into numerous sections. Sections 16.1–16.6 provide an overview of software MA, the objectives of MA, the purpose and scope of the chapter, and definitions of terms used herein.

Section 16.7 contains the references used in this chapter. References are denoted by square brackets throughout the chapter.

Section 16.8 provides an overview of the software practices and tasks that constitute the best practices for MA. This section is organized by the NSS 03-01 system acquisition phases.

Section 16.9 discusses the relationships among the system acquisition life cycle, software acquisition life cycle, and software development

life cycle. This is intended to assist the reader in mapping the detailed MA tasks, further defined in TOR-2006(8506)-5749, *Mission Assurance Tasks for Software*, to the system acquisition phases as defined in NSS 03-01.

For detailed definitions of each of the tasks introduced in section 16.8, please refer to TOR-2006(8506)-5749, *Mission Assurance Tasks for Software*.

Appendix A4 is a list of government products associated with software MA. Appendix A5 is a checklist for assessing supplier processes and products associated with software MA.

16.3 Background

Modern space systems are dependent on complex software for their successful launch, operation, and mission execution. Onboard software manages critical spacecraft systems and components during orbital operations. For example, software assures attitude control, manages the deployment of complex mechanisms, and controls space-ground communications. Onboard software also manages critical payload systems and components, and may perform mission data processing and collect and send mission data to the ground. Ground software supports routine and anomalous satellite operations, and may perform mission planning, mission data processing, and mission data dissemination.

Today's software-intensive space systems are large systems with multiple-satellite constellations and multiple ground elements, both fixed and mobile, frequently located worldwide. These systems involve complex combinations of hardware and software with complex external and internal interfaces. They are usually unprecedented (have never been built before) and have high reliability and integrity requirements. The size of the software in space systems now under development is on the order of magnitude of 10^5 source lines of code (SLOC) onboard and 10^6 - 10^7 SLOC on the ground.

Acquisition of these large, complex, software-intensive, modern space systems has historically been fraught with major problems, including performance deficiencies, extensive software defects, and cost and schedule overruns. Recent changes in acquisition policy, including a new acquisition policy unique to space systems [NSS04], provide an opportunity to address the errors of acquisition reform and to institute

new acquisition practices that apply Lessons Learned to reduce risk in the acquisition of software-intensive systems.

The NSS acquisition process is partitioned into four phases, with key decision points (KDPs) where program continuation is determined [NSS04]. These phases are: Pre KDP A (concept studies), Phase A (concept development), Phase B (preliminary design), Phase C (complete design), and Phase D (build and operations), and are shown in Figure 16.3-1. In NSS 03-01 terminology, software MA activities span the entire life cycle of program acquisition, from pre-systems acquisition (Pre KDP A) through sustainment (Phase D). The following sections will discuss software MA activities within the NSS acquisition life cycle phases.

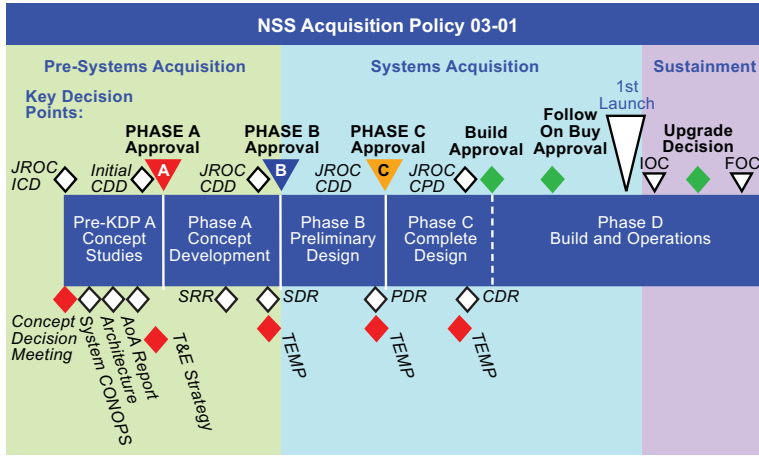


Figure 16.3-1, NSS 03-01 Acquisition Phases [NSS04]

16.4 Objectives of MA for Software

An objective is an aim or goal toward which effort is directed. For software, the objectives for MA are to ensure that:

- The software product meets all allocated functional, interface, and performance requirements. The verification process ensures that this goal has been met.
- The software product performs as intended in the users' operational environment. The validation process ensures that this goal has been met.

- The software product meets the users' expectations for end-to-end operational effectiveness, operability, suitability, and supportability. This goal is verified by analysis during development, validated during operational test and evaluation, and monitored during operations for continued compliance.
- The software product meets quality expectations, exhibiting the required dependability, reliability, maintainability, and availability. This goal is verified by analysis during development, validated during operational test and evaluation, and monitored during operations for continued compliance.
- The software architecture is sufficiently extensible, and computer resources have sufficient margins, to accommodate future required system change and growth. This goal is verified by analysis during development, validated during operational test and evaluation, and monitored during operations for continued compliance.
- The software product is sufficiently robust to gracefully degrade in the presence of anomalous events. This goal is verified by analysis during development, validated during operational test and evaluation, and monitored during operations for continued compliance.

While these objectives are independent of program life cycle phase, the specific practices and tasks to meet these objectives vary throughout the program life cycle as described in sections 3 and 5 also in TOR-2006(8506)-5749, *Mission Assurance Tasks for Software*.

16.5 Purpose and Scope

The purpose of this chapter is to provide both government and Aerospace members of a program office, and their Aerospace Engineering and Technology Group (ETG) support, a list from which to choose necessary software MA activities to achieve mission success. The MA activities span the scope of software acquisition activities performed by the government program office and the software engineering activities performed by the supplier.

This chapter is intended for the use of software acquisition professionals; a thorough and practical knowledge of software acquisition as it applies from the earliest stages of the system acquisition life cycle, through the software development life cycle, through system sustainment, to the retirement of the system, is assumed. References to additional resources are included to assist the

reader. This chapter is not intended to cover every task in the acquisition of software, only those tasks that contribute to MA. It is assumed that the program office will have developed a SWAMP to document all software-related acquisition tasks.

16.6 Definitions

Acquirer: A person or organization that acquires a product from a supplier. The acquirer is responsible for managing the contract that procures the system and is responsible for ensuring the user's needs are met. In this chapter, the acquirer is generally assumed to be a government program office.

Contract: The legally binding agreement between the "acquirer" and the "supplier." Also the legally binding agreement between the prime contractor supplier and a "subcontractor."

Contract data requirements list (CDRL): The itemization of the development products to be delivered by the supplier to the acquirer, part of the contract.

Mission assurance (MA) is defined as the disciplined application of general systems engineering, quality, and management principles towards the goal of achieving mission success, and, toward this goal, provides confidence in its achievement. MA focuses on the detailed engineering of the acquired system and, toward this objective, uses independent technical assessments as a cornerstone throughout the entire concept and requirements definition, design, development, production, test, deployment, and operations phases.

Mission assurance plan (MAP): The set of tasks to be performed by Aerospace personnel in support of a government program office system acquisition. As defined in this chapter, the MAP is limited to software tasks in support of software MA. It is a subset of the software acquisition tasks defined in the software acquisition management plan. The MAP constitutes an agreement between The Aerospace Corporation and the government program office for the software tasks that Aerospace will perform.

Mission success (MS[30]) is defined as the achievement by an acquired system (or system of systems) to singularly or in combination meet not only specified performance requirements but also the expectations of the users and operators in terms of safety, operability, suitability and supportability. Mission success is typically evaluated after operational turnover and according to program specific timelines and criteria, such as key performance parameters (KPPs). Mission success assessments include operational assessments and user community feedback.

Offeror: A person or organization that responds to a request for products or services, but is not yet on contract for those products or services. See also "supplier" below.

Peer review: A peer review is the review of work products performed by peers during development of the work products to identify defects for removal [SEI02].

Prime contractor: The supplier organization that has a contract directly with the government. The prime contractor may contract with "subcontractors" to perform part of the technical effort of the contract. This document refers to the prime contractor and subcontractors as "suppliers."

Program office: The government organization responsible for acquiring the system. It is made up of government, federally funded research and development centers (FFRDCs), and systems engineering and technical assistance (SETA) contractors.

Software: Computer programs, procedures, data, and possibly documentation pertaining to the operation of a computer system [DAU03].

Software acquisition: The process of obtaining a software product, from conception to retirement. In this chapter, software acquisition is part of a larger space system acquisition. This chapter discusses only the role of software acquisition within a software-intensive system acquisition.

Software acquisition life cycle: The set of software acquisition activities performed by the acquirer in obtaining a software product that

[30] In contrast, acquisition success can be defined in terms of performance, cost, and schedule.

begins with the decision to acquire a software product and ends when the software product is longer available for use.

Software acquisition team: The group of people supporting software acquisition for a program office, including military, civilians, FFRDCs, and SETAs. The members of the software acquisition team may not reside in a single organization within the program, but may be dispersed throughout integrated product teams and staff functions.

Software development: An inclusive term encompassing all activities resulting in software products, including new development, modification, reuse, reengineering, and maintenance.

Software development life cycle: The set of software development activities performed by the software supplier from the start of the contract to the final delivery of the product to the acquirer, including requirements analysis, design, code, integration, test, transition to operations, and transition to maintenance.

Software engineering: (1) The application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software; that is, the application of engineering to software. (2) The study of approaches as in (1) [ADA05], [MIL92].

Software mission assurance: The disciplined application of software engineering, acquisition, and management principles, processes, and standards to achieve mission success.

Software quality: Software quality is exhibited when the delivered software meets all functional, performance, and interface requirements, including the required dependability, reliability, maintainability, availability, security, safety, supportability, and usability.

Software team member: Any internal or external organization that develops, tests, or supports software-related work being performed on the contract and has an agreement (formal or informal) with the supplier or any other software team member.

Statement of objectives: The basic, top-level objectives of an acquisition provided in the request for proposal (RFP) in lieu of a government-written statement of work (SOW).

Statement of work: The complete list and description of tasks to be performed and products to be delivered by the supplier. The SOW is part of the contract.

Subcontractor: An organization tasked by the prime contractor to perform part of the required effort of the contract.

Supplier: A person or organization that enters into a contract with the acquirer for the supply of a product or service. The term "supplier" is used within this chapter rather than "contractor" to provide a neutral and broader definition of acquisition that includes all those delivering products or performing services as well as those contracted (such as a prime contractor) to develop and deliver products.

Suitability: A measure of the degree to which a system is appropriate for its intended use with respect to non-operational factors such as man-machine interface, training, safety, documentation, producibility, testability, transportability, maintainability, manpower availability, supportability, and disposability. The level of suitability determines whether the system is the right one to fill the customer's needs and requirements. Suitability measures can be used as performance requirements, design constraints, and/or technical exit criteria. Suitability is a systems engineering metric [MIL92].

Sustainment: Sustainment begins with the transition of the system to operational use and to maintenance, and concludes with retirement of the system.

System acquisition life cycle: The set of system acquisition activities performed by the acquirer from the inception of the program to the retirement of the system. The system acquisition life cycle for SMC programs is defined by NSS 03-01. In NSS terminology, the system acquisition life cycle begins in Pre-Phase A (concept studies), and ends at the completion of Phase D (build and operations).

Validation: The process of demonstrating that a product or product component fulfills its intended use when placed in its intended environment [SEI02].

Verification: The process of ensuring that selected work products meet their specified requirements [SEI02].

16.7 External Guidance, Standards, and References

[ABE04] Abelson, L.A., R.J. Adams, S. Eslinger, *Metrics-based Software Acquisition Management,* Aerospace TOR-2004(3909)-3405, May 2004

[ADA04] Adams, R. J., S. Eslinger, K. L. Owens, and M. A. Rich, *Software Acquisition Best Practices: Experiences from the Space Systems Domain*, Aerospace TR-2004(8550)-1, 30 September 2004

[ADA05] Adams, R. J., et. al., *Software Development Standard for Space Systems*, Aerospace TOR-2004(3909)-3537B, 11 March 2005

[ADA06] Adams, R. J., S. Eslinger, K. L. Owens, and M. A. Rich, *Software Acquisition Best Practices for the Early Phases*, Aerospace TR-2006(8550)-1, 31 January 2006

[DAU03] Defense Acquisition University, *Glossary of Defense Acquisition Acronyms and Terms*, Defense Acquisition University Press, 2003

[ESL00] Eslinger, S., *Software Acquisition and Software Engineering Best Practices*, Aerospace TR-2000(8550)-1, 15 November 1999

[ESL05] Eslinger, S., M. A. Rich, *Software Acquisition Best Practices Tutorials,* Aerospace TR-2005(8550)-1, 30 September 2005

[GEI01] GEIA Standard *Earned Value Management System*, ANSI/EIA-748-A-1998, reaffirmed 2002

[HAN05] Hantos, Peter, *Life Cycle Models for the Acquisition and Development of Software-Intensive Systems*, Systems and Software Technology Conference 2005

[IEE05] IEEE Standard for Software Verification and Validation, IEE Standard 1010™-2004, Institute of Electronics and Electrical Engineers, 08 June 2005

[KER06] Kerner, J.S., et al, *Ground Software Study: Roadmap of Recommendations*, Aerospace TOR-2006(3000)-5391, 30 June, 2006

[MIL92] MIL-STD-499B, *Draft Military Standard for Systems Engineering*, 06 May 1992

[NEI99] Neitzel Jr., A.C., *Managing Risk Management*, CrossTalk, July 1999

[NSS04] National Security Space Acquisition Policy, Number 03-01, 27 December 2004, *Guidance for DoD Space System Acquisition Process*

[OWE03] Owens, K. L., B. R. Troup, *A Practical Guidebook for Performing Software Capability Appraisals*, Aerospace TR 2003(8550)-1, 20 September 2003

[OWE04] Owens, et. al., *Recommended Software-related Contract Deliverables for National Security Space System Programs*. Aerospace TOR-2006(8506)-5738, in press

[PAU93] Paulk, M., The Capability Maturity Model for Software, Version 1.1, (SEI-93-TR-25), 1993, © 1993, Carnegie Mellon University

[SEI02-1] Software Engineering Institute, *Capability Maturity Model® Integration[SM], Version 1.1, CMMI® for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI®-SE/SW/IPPD/SS, V1.1), Continuous Representation*, Carnegie Mellon University, (SEI-2002-TR-011), March 2002

[SEI02-2] Software Engineering Institute, *Capability Maturity Model® Integration[SM], Version 1.1, CMMI® for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI®-SE/SW/IPPD/SS, V1.1), Staged Representation*, Carnegie Mellon University, (SEI-2002-TR-012), March 2002

[SEI05] CMU/SEI-2005-HB-005, *Handbook for Conducting Standard CMM®I Appraisal Method for Process Improvement (SCAMPI)[SM] B and C Appraisals*, Version 1.1, December 2005

[SEI94] CMU/SEI-94-SR-001, *An Introduction to Team Risk Management (Version 1.0)*, May 1994

[SMC04] *SMC FFRDC User's Guide*, 20 January 2004

16.8 Practices and Tasks

16.8.1 Overview

Many of the highest leverage activities for MA are done by the acquisition team pre-contract award. It is important, therefore, for software mission success that the software elements of a system acquisition are fully considered from the start of system concept definitions and preliminary trade studies. Lessons learned from previous NSS programs [KER06] indicate that the two most important tasks in the early phases of system acquisition are to develop realistic software cost and schedule estimates and to have a robust risk management program.

It is the responsibility of the system acquirer to develop realistic system cost and schedule baselines, based on the system requirements. The requirements and schedule milestones will be the basis for the supplier's cost and schedule estimates. It is also the responsibility of the system acquirer to review the offeror's software development plans, schedules, and cost estimates. It is important to start software development with mature software development plans and realistic software development schedules and cost estimates. Unrealistic schedules and cost estimates will result in processes being shortchanged and will adversely affect software quality, and reduce software MA.

Software has inherent complexity that is not completely uncovered until later steps in the development life cycle, even with good analysis and design processes. Most major programs encounter issues during development that cause requirements change, redesign, and rework. Preparation for these issues requires robust risk management and planning for adequate cost and schedule reserves to allocate for corrective actions when risks materialize. MA for software should be risk driven in order to most effectively focus resources and tasks. Software risk analysis starts in the early phases of system acquisition and should be a continuous process throughout the system acquisition life cycle in close collaboration with the suppliers. See [SEI94], [NEI99].

The supplier performs many activities to assure mission success. It is, therefore, important to include MA activities for software in the contract. Table 16.8-1 summarizes the pre-contract award activities that facilitate MA for software. A more detailed discussion of pre-contract award space system software acquisition best practices can be found in [ADA04].

Table 16.8-1, Pre-Contract Award Activities

Activity	Mission Assurance Tasks
Establish program baseline	• Include software in system performance requirements • Perform software architecture-inclusive trade studies • Determine realistic, independent baseline software estimates • Define required software metrics for progress, change, staffing, risk, and quality [ABE04]
Obtain contractual insight	• Require key software technical and management deliverables • Require timely electronic access to all software products • Require software level technical and management reviews
Obtain contractual commitment	• Mandate compliance with a robust full life cycle software development standard • Require supplier commitment to the software development plan (SDP)
Select capable supplier team	• Perform a software capability appraisal as part of the source selection • Evaluate software architecture with system design • Evaluate realism of cost and schedule bids
Provide contract management tools	• Provide contract incentives for software quality, not just cost and schedule • Mandate periodic team software capability appraisals • Require a system for collection, reporting, analysis, and corrective action of software metrics

A plan should be developed by the Aerospace program office to define the Aerospace tasks as part of the MA team. Potential Aerospace activities span the scope of all program systems and software engineering tasks—supporting the government activities and assuring a disciplined application of software principles, processes, and standards by the supplier after contract award.

The MAP for software describes the activities, and tasks to be performed, and the roles and responsibilities of the participants. The activities required to develop the plan are to: 1) understand and characterize the environment in which the software development takes place, 2) define the elements of the plan, 3) execute the plan and make recommendations to the government program office, and 4) review results and improve processes.

16.8.2 Understand and Characterize the Software Acquisition and Development Environment

In order to plan the MA tasks for software, it is important to understand the program as a whole, as well as the software acquisition and development environment within the program. For a program already under contract, this begins with a review of the terms of the contract, the acquirer's acquisition strategy, the acquisition management plan, the system test plan, and all required specifications and standards. The contract is the binding legal document between the acquirer and the supplier. The contract identifies the acquirer, the supplier, and the roles, responsibilities, and relationships among the participating organizations.

Figure 16.8-1 illustrates the roles and responsibilities for the acquirer, supplier, and The Aerospace Corporation in performing system acquisition, design, development, integration, test, transition, operation, and maintenance. Aerospace roles include acquisition support to the government on software requirements analysis, concept studies, plans, and architecture. An additional role is to perform independent technical analysis for government decision support or to confirm or refute supplier data. Aerospace also reviews the work of the suppliers who are designing or manufacturing the system, assessing processes, products, and activities to determine quality and makes recommendations to the government program office.

Contract provisions govern what the supplier is required to perform, and therefore, determine the scope of MA activities for software. Some

of the contract provisions that impact MA for software are summarized in Table 16.8-2.

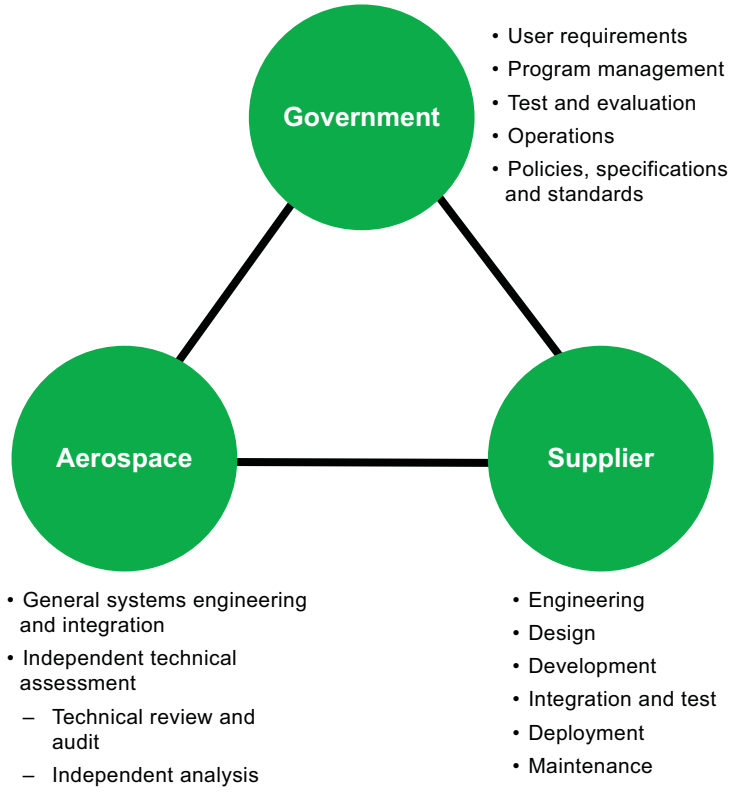


Figure 16.8-1, Organizational Roles and Responsibilities

Table 16.8-2, Contract Provisions Impacting Mission Assurance

Contract Element	Mission Assurance Implications
Statement of work (SOW)	The SOW is the part of the contract that specifies all tasks to be performed and all hardware and software items to be delivered on the contract.
Fee structure	The fee structure (e.g., fixed fee, cost plus, award fee) determines the supplier's financial incentives. Look for incentives based on quality as well as cost and schedule.
Specifications and standards	Specifications and standards add requirements that often increase MA. These may include government, commercial, and other specifications and standards.
Contract data requirements list (CDRL)	The CDRL identifies all documentation, hardware, and software items to be delivered. These are the major products that can be reviewed for technical content and quality.
Work breakdown structure (WBS)	The WBS identifies the system, the segments and elements that comprise the system, and the tasks to be performed within each segment and element. The WBS also reflects the organizational structure of the program, identifying tasks performed by the prime contractor and any subcontractor organizations. The organizational structure provides insight into informal meetings that may be opportunities for technical review.
Technical and management reviews	The supplier's integrated management plan (IMP) is usually on contract. The IMP identifies the events during the life of the contract (usually defined to be the formal program reviews), significant accomplishments for each event, and accomplishment criteria used to determine if the goals of the event have been achieved. Program reviews are opportunities for reviewing the technical baseline. Management reviews provide an opportunity to review cost, schedule, and risk.
Electronic environment	Many programs have consolidated all documentation in a single database, which provides electronic access (if specified in the contract) to all program members, including the government and Aerospace.

The acquisition and development environment is fundamentally determined by the acquirer's acquisition strategy. The acquirer has selected an acquisition strategy, which may be a once-through (waterfall), where the supplier designs, builds, tests, and delivers the system only once, or an evolutionary strategy (e.g., incremental or spiral), where the supplier designs, builds, tests, and delivers multiple versions of the system iteratively [NSS04]. The acquisition strategy must be understood in order to know what products and functionality are expected at what point in the system development life cycle. It is important to note where the program currently is in the acquisition life cycle, because that determines what activities have already been accomplished and which remain to be executed.

The supplier determines the software engineering activities, work products, and schedules in accordance with the requirements of the contract and the selected system acquisition strategy. All supplier plans and significant events, accomplishments, and accomplishment criteria for the program are documented in the integrated management plan (IMP). The tasks comprising the planned significant events and accomplishments are documented in the integrated master schedule (IMS). The supplier's software development plan identifies any additional principles, processes, and standards that apply to the software development environment. The software development plan also identifies the software to be developed, the associated computer resources hardware and interfaces, and the functions and functional relationships among the software, computer resources hardware, and the rest of the program elements.

In response to the system acquisition strategy, the supplier selects a software development life cycle model. This can be a waterfall model or an iterative model (e.g., evolutionary). Together with the contract provisions, the software life cycle model must be understood in order to know what specifications and standards apply, what products and functionality are expected at what point in the life cycle, and what opportunities exist for formal and informal technical review. Using the supplier's IMP, IMS, and software development plan, the software development processes and products available for review can be identified, along with the schedule for their availability.

16.8.3 Define Elements of the MAP for Software

A MAP for software can now be developed for acquisition support to the government, for technical review of the supplier's and/or the government's processes and products, and for independent analysis. The first step in developing a plan is to prioritize the processes and products, based on their criticality to program success and the time and resources available for the review. The acquirer and supplier's program risk assessments should be used to perform the prioritization, using a risk-driven MA approach. The acquirer's budget determines the resources available. A set of evaluation criteria should be developed to assess the quality of the processes and products. The evaluation criteria can be derived from the specifications and standards, both government-imposed and supplier-selected. Using the acquirer and supplier's program risk assessments, areas that are candidates for independent analysis can also be identified. These may include high-risk technology areas, or technical risk areas that are not being addressed by the supplier.

16.8.3.1 Acquisition Support to the Government

Acquisition support could include any activity described in [SMC04].The MAP would describe those activities that enhance software quality to meet the objectives of section 16.4. Particular emphasis would be given to establishing a feasible software architecture for acquisition, risk assessment, and realistic software cost and schedule estimates. Such activities could include:

- Assisting the development of, or evaluating the system acquisition strategy
- Assisting the development of, and evaluating software architectures
- Reviewing or developing software cost and schedule estimates
- Advising on software specifications and technical standards applicable for the source selection
- Advising on and/or evaluating software elements of proposals during source selection
- Evaluating software supplier capability

Similar activities would be performed post-contract award for changes due to requirements modifications or additions, or programmatic revisions.

16.8.3.2 Technical Review

Technical review refers to review by Aerospace personnel of the work of the suppliers who are developing the software. Aerospace personnel are responsible for the review of supplier's plans, procedures, processes, products, measurement data, and activities to determine technical accuracy, completeness, and quality, and to identify any shortfalls that may negatively impact mission success.

Table 16.8-3 identifies some of the items typically available for review during the software development life cycle. Technical review of these items may include review of documentation, observation of activities, and analysis of data. Review activities are based on the requirements of the applicable specifications and standards, software best practices, and documented evaluation criteria.

Table 16.8-3, Plans, Procedures, Processes, and Products for Technical Review

Review Opportunities	Items to be Reviewed	Review Tasks
Plans	Software development plan, software test plans, software integration and verification plans, installation plan, software transition to operations plan, software transition to maintenance plan.	Review documentation for consistency with standards and for the technical correctness and completeness of the plans.
Procedures	Step-by-step instructions within a process.	Review procedure documentation for consistency with standards and associated process and for the technical correctness and completeness of the procedures.

Review Opportunities	Items to be Reviewed	Review Tasks
Processes	Project planning and oversight, software development environment, system requirements definition, system design, software requirements definition, software design, software implementation and unit testing, unit integration and testing, software item qualification testing, software-hardware item integration and testing, system qualification testing, preparing for software transition to operations, preparing for software transition to maintenance, software configuration management (CM), software product evaluation, software quality assurance, corrective action, joint technical and management reviews, risk management, software management indicators, administrative security and privacy protection, managing subcontractors, interfacing with software independent verification and validation (IV&V) agents, coordinating with associate developers, project process improvement.	Review process documentation for consistency with standards and for technical correctness and completeness of the documented processes. Evaluate the quality of the execution of the documented processes through observation or interviews with developer personnel. This can be done in a systematic fashion using one of the Software Engineering Institute's standard CMMI® appraisal methods for process improvement (SCAMPI^{SM}).
Products	Software engineering analysis products, operation concept products, requirements products, architecture products, design products, testing products, maintenance products, operations products.	Review documentation for consistency with standards and for technical correctness and completeness of the products.

Review Opportunities	Items to be Reviewed	Review Tasks
Measurement data	Metrics, technical performance measures (TPMs), key performance parameters (KPPs).	Review measurement data regularly, analyze data for trends, evaluate the thresholds for taking action, evaluate the corrective action plans, follow up corrective action activities to closure, use results from metrics analysis for potential process improvement areas.
Activities	Formal reviews, informal reviews, unit test, software item integration test, qualification test.	Participate in the developer's informal reviews, observe informal test, witness formal test, review test plans, test procedures, test data, and test results, follow up regression testing to closure.

The product of technical reviews is an assessment of the quality of the product, process, or procedure reviewed, with particular attention to areas that may adversely impact mission success. For software, "the quality of the software product is dependent on the quality of the processes used to develop or maintain it" [PAU93], so review of processes is of particular importance in MA for software.

16.8.3.3 Independent Analyses

Independent analysis refers to work that Aerospace performs independently of the supplier. Aerospace performs independent analyses at the request of the government program office, or on its own initiative, to supplement supplier activity or to support or refute results of supplier activity. Table 16.8-4 lists some typical analyses that Aerospace may be called upon to perform in support of assessing software MA.

Table 16.8-4, Independent Analysis Opportunities

Analysis	Description
Risk assessment	The supplier typically has a defined risk assessment and handling process and has identified the major risks on the program. The software engineering organization participates in the system risk assessment process and software risk assessment is part of that process. Aerospace may perform an independent assessment of the program risks.
Requirements analysis	The supplier typically has a defined requirements analysis process, has elaborated requirements at the system, segment, element, and subsystem level, and has an automated tool to manage requirements traceability. The software engineering organization participates in the system requirements analysis process and software requirements analysis is part of that process. Aerospace may perform an independent analysis of the requirements to determine if they are correct, complete, testable, and verifiable, and whether the requirements traceability is correct and complete.
Modeling and analysis	The supplier typically performs many modeling and analysis tasks during the life of the program to predict performance of the system, system components, hardware, and software, and to verify and validate requirements. Aerospace may perform independent modeling and analysis to validate the supplier's models against benchmark models.
Specialty engineering	System requirements for dependability, reliability, maintainability, availability, safety, and security apply to both software and hardware. Aerospace may perform an independent quantitative or qualitative analysis of the integrated system and software architecture to determine the software contribution to the system performance in these areas. Such activities include DRMA modeling and prediction, DRMA measurement, functional and software safety analyses, failure modes and effects analyses, failure review boards, trending and summarization, and root cause analyses.

Analysis	Description
Software architecture and design analysis	The software architecture and design, together with the hardware on which it resides, determine the ability of the system to meet functional, performance, and interface requirements. Aerospace may perform an independent analysis of the software architecture and design, particularly in mission-critical areas, to determine if they will meet allocated system requirements.
Static code analysis	The quality of the code can adversely impact the ability of the system to meet functional, performance, and interface requirements. Aerospace may perform an independent analysis of the code, particularly in mission-critical areas, to determine if it will meet allocated system requirements.
Technology readiness	Technology readiness levels measure system and component technical maturity. A low technology readiness level can stop a program from continuing. Aerospace may perform an independent assessment of the technology readiness level.
Processor throughput, memory and storage capacity, and communications bandwidth margins	System requirements typically include performance margins to accommodate system growth, and contingency operations. Software, in particular must allow margin in processor throughput, memory and storage capacity, and communications bandwidth. Aerospace may perform an independent assessment of the software performance on the selected hardware to assure that adequate margins are maintained.
Launch readiness reviews, mission readiness reviews, and independent readiness review teams	Aerospace participates in several types of independent readiness reviews, including launch readiness reviews, mission readiness reviews, and independent readiness review teams.
Independent verification and validation	A role that Aerospace occasionally takes on is that of an independent verification and validation agent.

The sequence of technical review and independent analysis activities can now be documented into a MAP for software.

16.8.4 Execute the Plan and Make Recommendations

Aerospace implements the MAP for software by reviewing government plans, concepts, and architectures, and assessing technical performance of the contractor through meetings, exchanging information on progress and problems, reviewing reports, evaluating presentations, reviewing hardware and software, witnessing and evaluating tests, analyzing plans for future work, and evaluating efforts relative to contract technical objectives [SMC04]. Based on the results of the technical review, Aerospace makes recommendations to the government program office about any necessary steps that the supplier should be required to perform to improve the quality of its processes or products.

16.8.5 Review Results and Improve Processes

Aerospace ensures that technical deficiencies and weaknesses are isolated; that the impact of new data, new developments, and modified requirements on total systems concepts and technical performance are properly addressed; and that appropriate changes are promptly introduced. Aerospace provides comments and recommendations to the government program manager for consideration for modifying the program or redirecting the supplier's efforts to assure timely and economical accomplishment of software development, while maintaining software quality.

16.9 Phase-Dependent Software Task Execution for MA

16.9.1 Phase Dependence and Flow of MA Tasks for Software

The impact of ineffective software methods and processes can be (and has been) very disruptive to the success of NSS programs. To improve processes and minimize program impacts, MA tasks for software are recommended in this section for all NSS 03-01 phases, using appropriate software life cycle models as illustrated in Figures 16.9-1 and 16.9-2. The MA tasks of this section are equally applicable, with appropriate tailoring, to any of the software development life cycle models and the tasks would be selected based on the characteristics and size of the required development.

As stated in section 16.8, software is developed successfully using different approaches or life cycle models, depending on the nature and size of the software development, as well as the maturity of development processes in the supplier organization. Onboard software, composed of both the spacecraft bus and payload(s) software, is often developed using a traditional waterfall life cycle. Large-scale software is typically developed with some form of iterative development – designing, building, and testing some components, accompanied by additional development stages that augment and correct the earlier stages until the complete product is integrated and tested. Thus, actual development is carried out in asynchronous, concurrent streams. At any given time, these process streams will be in different states with the potential need for periodic synchronization. This complex software development life cycle needs to be planned in the context of NSS 03-01 system acquisition life cycle phases. Figure 16.9-1 [HAN05] illustrates potential software development life cycle models, with requirements analysis, design, coding, and testing conducted more than once, out of synchronization with the NSS 03-01 phases.

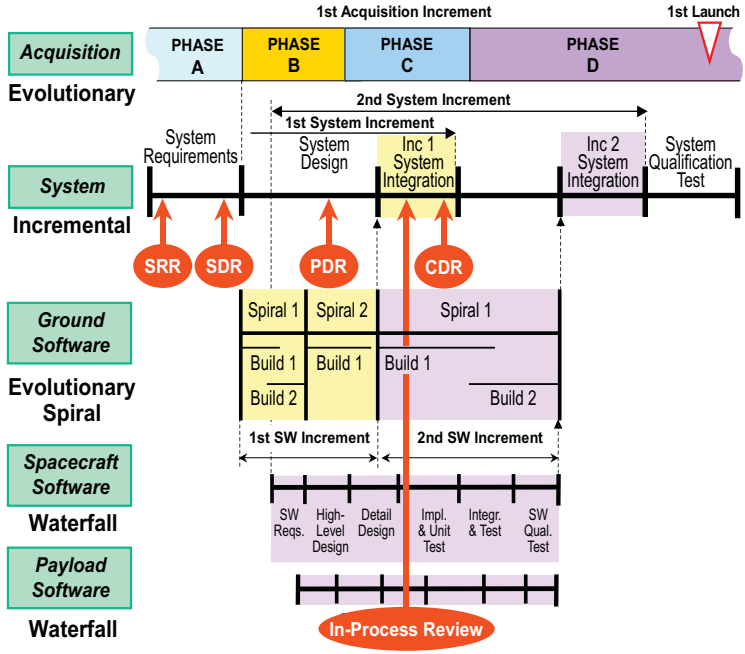


Figure 16.9-1, Life Cycle Model Complexity [HAN05]

The software development life cycle model for a program will be based on the experience and established processes of the selected supplier. However, analysis should be done in acquisition planning to consider the phasing of software tasks with respect to the NSS 03-01 system acquisition life cycle phases.

The increments, spirals, and builds shown in Figure 16.9-1 will not all be applicable in the chosen software development life cycle of a particular program. Each increment, spiral, or build will have requirements, design, development and test activities with associated reviews, e.g., software requirements review (SRR), architecture review, increment design walkthrough(s), code walkthroughs, increment qualification test readiness review, etc. The number and timing of the tasks and reviews of the asynchronous, concurrent streams of activities that make up the software development life cycle will depend on the nature and size of the program. Refer to [ADA05] and [HAN05] for guidance.

Figure 16.9-2 shows the software life cycle periods and events for an iterative software development life cycle in relation to the system acquisition life cycle.

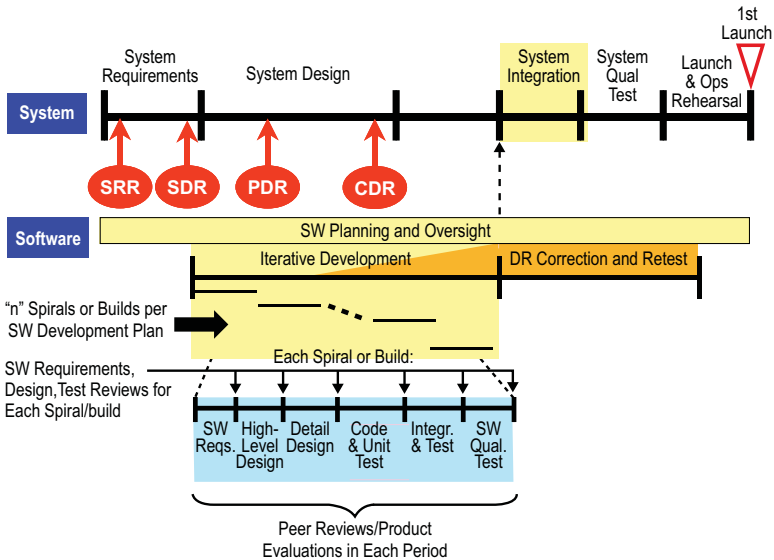


Figure 16.9-2, Software Life Cycle within the System Life Cycle

Software engineering staff would participate in system requirements analysis and decomposition. The initial software development increment would start following system design review (SDR), unless an early software increment was planned for risk reduction. Software requirements analysis and design for early increments might complete before system preliminary design review (PDR), and for later increments, after system critical design review (CDR).

16.10 Key Government and Contractor Enabling Tasks and Input in Each Phase

Performance of MA tasks after contract award requires: 1) timely access to artifacts and metrics of the supplier's software development processes, and 2) supplier participation and response in reviews and audits that are required to perform the tasks. The vehicle to obtain timely access to supplier data and supplier participation in reviews and audits is the statement of work (SOW). The SOW is based on the work breakdown structure (WBS), and describes every task that the supplier must perform and every product the supplier must deliver. The SOW is a part of the request for proposal (RFP). The contract data requirements list (CDRL) specifies the content, format, and delivery requirements for every product that the supplier must deliver. For support of MA, the RFP, SOW, and CDRL must specify all tasks and data required on the contract.

16.11 MA Task Structure

Section 16.8 introduced the practices and tasks for software MA, including pre-contract award activities, acquisition support to the government, technical review, and independent analyses. Section 16.9.1 discussed how these activities relate to the system acquisition, software acquisition, and software development life cycle phases. Appendix A3-13 lists the tasks, which are further elaborated on in TOR-2006(8506)-5749, *Mission Assurance Tasks for Software* and in Appendices A4 and A5. In Appendix A3-13, the primary tasks are designated Level 1; Level 2 and 3 sub-tasks further delineate the primary task. Many of these tasks can be performed in more than one phase of the NSS 03-01 system acquisition life cycle; the details of the task will vary depending on the current life cycle phase, and must be tailored accordingly. For example, the task "Assess software test planning" could be performed as early as Phase B at the level of software test plans. In later phases, the task could address software test cases and test procedures.

Similarly, many of the tasks in Appendix A3-13 can be performed in more than one software life cycle phase; the details of the task will vary and would be tailored to match actual activities being performed at each stage of development. For example, in an incremental software development, Increment I may have software test plans, cases, and procedures whereas later increments only have test plans at this stage.

Appendix A1
Definitions

Acquirer is the organization responsible for managing the contract that procures the system and responsible for ensuring the user's needs are met. One of the contracting parties; also known as the "buyer" or "customer."

Activation is a set of activities whereby newly acquired capabilities and/or systems are operationally checked out by a government program office/engineering development team before it is released for mission operations. For the purposes of this guide, activation include space vehicle activation on orbit, launch vehicle "activation" after successfully completing launch base processing when judged ready to perform flight operations, and ground system "activation" after it has been deployed, the crews proficient and ready for mission operation.

Audits are independent inspections of each configuration item (CI) or process, by discipline or subsystem experts, within a system to ensure that functional characteristics and physical attributes comply with relevant specifications, standards, and concepts of operations.

Contract is the legally binding agreement between the "acquirer" and the "supplier." Also the legally binding agreement between the prime contractor/supplier and a "subcontractor."

Contract data requirements list is the itemization of the development products to be delivered by the supplier to the acquirer, part of the contract.

Design assurance is the traceable systematic multi-level activity ensuring accurate translation of all requirements/specifications/ standards into a detailed producible, testable, supportable design.

Design synthesis is the translation of requirements, standards, concept of operations, and functions (functional architecture) into solutions (physical architecture) through tradeoffs, technology evaluations, and design optimization.

Developer is the organization responsible for managing and performing the technical effort required by the contract and developing

the system or component that meets contract requirements. One of the contracting parties; also known as the "contractor."

Engineering discipline is a well-established and documented technical body of knowledge governing the execution of a certain set of tasks to achieve a specific set of technical objectives.

Evaluation is an activity to objectively determine the suitability of the product to perform its intended mission and satisfy requirements. Evaluation in the context of test is the set of tasks necessary to assess the suitability of a planned test program to provide adequate proof of performance; to compare analytical results and predictions with comparable test results; and to determine the adequacy of the test program as actually executed. In context of verification, evaluation includes the necessary tasks to plan and execute analysis, simulation, and inspection.

Hazards are real or potential conditions that directly or through induced effect cause injury, illness, or death to personnel; physical or catastrophic damage to or physical loss of a system, equipment, or property; or damage to the environment. It is the presence of a potential risk situation caused by an unsafe act or condition. It is a condition or changing sets of circumstances that presents the potential for adverse or harmful consequences.

Independent technical assessment (ITA) is defined as a formal or informal process, or combination of processes, formulated and executed using program, engineering, and laboratory resources to proactively evaluate system performance and independently validate contractor processes, techniques, and results using methods different from, and complementary to, those employed by the contractors. In some cases, ITA can be conducted by separate contractors. More commonly, ITA is performed in the context of the government program office-FFRDC-SETA team, where The Aerospace Corporation performs that FFRDC role for NSS systems.

Integration is a process whereby components, subassemblies, assemblies, units, and subsystems are combined functionally and physically to form and perform as a complete system.

Manufacturing is the conversion of raw materials into products or components through a series of processes. It includes such major functions as manufacturing planning, tool design, scheduling,

manufacturing engineering, material procurement, fabrication, assembly, test, packaging, installation and checkout, product assurance, and determination of resource requirements throughout systems acquisition.

Manufacturing engineering is the specialty of professional engineering that requires such education and experience as is necessary to understand and apply engineering procedures in manufacturing processes and methods of production of industrial commodities and products. It requires the ability to plan the practices of manufacturing, to research and develop tools, processes, machines and equipment, and to integrate the facilities and systems for producing quality products with optimal expenditure.

Mission assurance (MA) is defined as the disciplined application of general systems engineering, quality, and management principles toward the goal of achieving mission success, and, toward this goal, provides confidence in its achievement. MA focuses on the detailed engineering of the acquired system and, toward this objective, uses ITAs as a cornerstone throughout the entire concept and requirements definition, design, development, production, test, deployment and operations phases.

Mission assurance phases emphasize that MA is an active process throughout a system's life cycle from concept definition to disposal.

Mission design analysis provides assurance that the system is capable of delivering the specific space vehicle to its planned orbit with sufficient margin to guarantee mission success.

Mission operations is the program stage after launch vehicle processing and/or satellite activation where operators and users control the intended mission for the launch vehicle or satellite until completion of design life.

Mission success (MS) is defined as the achievement by an acquired system (or system of systems) to singularly or in combination meet not only specified performance requirements but also the expectations of the users and operators in terms of safety, operability, suitability and supportability. Mission success is typically evaluated after operational turnover and according to program specific timelines and criteria, such as key performance parameters. Mission success assessments include operational assessments and user community feedback. In contrast,

acquisition success can be defined in terms of performance, cost and schedule.

Practice is a set of tasks customarily accepted and routinely performed.

Prime contractor is the supplier organization that has a contract directly with the government. The prime contractor may contract with subcontractors to perform part of the technical effort of the contract.

Process is a series of tasks involving the practical application of accepted principles conducted to achieve a specific end. MA processes contribute to mission success in terms of direct attributable positive consequences.

Producibility is a design accomplishment that enables manufacturing to repeat ably fabricates hardware that satisfies both functional and physical objectives at an optimal cost. Producibility results from a coordinated effort by systems/design engineering and manufacturing/industrial engineering to create functional hardware designs that optimize the ease and economy of fabrication, assembly, inspection, test, and acceptance of hardware without sacrificing desired function, performance, or quality.

Quality of a product is the degree to which the product attributes, such as capability, performance, or reliability meet the needs of the customer or mission, as specified through the requirements definition and allocation process.

Quality assurance is the technical and management discipline which ensures that a customer-ordered product meets the customer-specified performance parameters.

Readiness refers to all activities required to transport, receive, accept, store, handle, test, deploy, and control space vehicle, launch vehicle, and supporting ground systems such that associated flight or mission operations can be conducted safely while maintaining vehicle integrity.

Readiness reviews are used as formal gates to approve transition to operational status (flight or mission) of the space vehicle or launch vehicle once system integration is completed. Readiness reviews ensure that government program office and launch/mission operations personnel are satisfied that all requirements that can be verified prior to launch have been executed (including documentation), and that

personnel have been trained, certified, and are available to support the operation.

Risk refers to events that are possible, but not yet realized, and that carry adverse consequences for a program or mission. Risk is usually characterized by the identification of the risk events that pertain to a specific program or mission (by their probability of occurrence), and by the magnitude of the possible impacts as measured in some appropriate scale of assessable consequences.

Software includes computer programs, procedures, data, and possibly documentation pertaining to the operation of a computer system.

Software development is an inclusive term encompassing all activities resulting in software products, including new development, modification, reuse, reengineering, and maintenance.

Software engineering is (1) the application of a systematic, disciplined, quantifiable approach to the development, operation, and maintenance of software; that is, the application of engineering to software. (2) The study of approaches as in (1).

Software mission assurance is the disciplined application of software engineering, acquisition, and management principles, processes, and standards to achieve mission success.

Software quality is exhibited when the delivered software meets all functional, performance, and interface requirements, including the required dependability, reliability, maintainability, availability, security, supportability, and usability.

Software team member is any internal or external organization that develops, tests, or supports software-related work being performed on the contract and has an agreement (formal or informal) with the supplier or any other software team member.

Statement of work is the complete list and description of tasks to be performed and products to be delivered by the supplier; specified in the contract.

Subcontractor is an organization tasked by the supplier to perform part of the required effort of the contract.

Suitability is a measure of the degree to which a system is appropriate for its intended use with respect to nonoperational factors such as man-machine interface, training, safety, documentation, producibility, testability, transportability, maintainability, manpower availability, supportability, and disposability. The level of suitability determines whether the system is the right one to fill the customer's needs and requirements. Suitability measures can be used as performance requirements, design constraints, and/or technical exit criteria. Suitability is a systems engineering metric.

Supporting MA discipline is an engineering discipline that is executed, in its whole or, more frequently, in partial terms, to support MA processes and the entire MA program.

System is defined as a composite of equipment, skills, and techniques capable of performing or supporting an operational role. A system includes all operational equipment, related facilities, materials, software, services, and personnel required for its operation. A government program office or the procurement agency responsible for its acquisition typically defines the scope of a system. In the context of the guide, "system" refers to the spacecraft and/or launch vehicle and associated ground system hardware, software, communications links, facilities and personnel. The "system" may exclude mission data processing and distribution of mission products to the user.

System design is the process of defining, selecting, and describing solutions to requirements in terms of products and processes. It also is the product of the design activities that describes the solution (either conceptual, preliminary, or detailed) of the system, system elements, or system end-items. A detailed design, usually in graphical form, describes the arrangement of parts, how the parts are attached, process features and notes, and details of the end-item to be produced, manufactured, constructed, or acquired traceable to the requirements and standards identified for the system.

System safety is the application of special technical and management skills to the systematic, forward-looking identification and control of hazards throughout the life cycle of a project. The concept calls for safety analyses to identify risk of loss or harm and hazard control actions, beginning with the conceptual phase of a system and continuing through the design, production, testing, use, and disposal phases, until the activity is retired. Risks to the environment and health of personnel are a subset of the system safety hazard analysis.

Technical reviews are activities accomplished by technical experts established to exhaustively investigate the state, status, and performance of units, subsystems, and systems throughout the design, development, production, and test phases to uncover risks and issues, and to recommend steps to resolve risks/issues affecting mission success.

Test is an activity performed to determine output characteristics of the item under test as a function of variable inputs. For the purpose of this guide, there are two categories of testing: formal testing and informal testing. Formal testing applies rigorous test planning and flight-like test articles and is used to contractually verify requirements and validate unit, subsystem, and system performance. Informal testing, such as development testing, uses engineering models, breadboards, or prototypes to assist in design decisions (e.g., first of a kind) or flight-like units (e.g., qualification unit) to investigate problems/anomalies in latter stages of development.

Validation provides confidence, through independent analysis or test, that the technical means and processes accomplish their intended purpose, in this case to meet user needs. At the system level, validation occurs before the as-built system is transitioned into mission operations.

Verification is a system engineering process that proves the as-built item complies with requirements baseline as determined by test, analysis, demonstration, inspection, and/or similarity performed at all levels from the lowest level configuration item to the system. Verification is typically done in a hierarchical fashion from the lowest level requirements up to systems requirements. Test, analysis, demonstration, and inspection are known as verification methods and are applied at the appropriate and lowest level of assembly where the selected method is most perceptive at providing the needed data.

Appendix A2
Acronyms

1-PoF	Reliability
AoA	Analysis of alternatives
ACO	Administrative contracting office
ADM	Acquisition decision memorandum
AFSPC	Air Force Space Command
ALRR	Aerospace launch readiness review
ALT	Accelerated life testing
APR	Aerospace president's readiness review
ARR	Aerospace readiness review
BIST	Baseline integrated system test
BIT	Built-in-test
C&C	Civil and commercial
CAB	Corrective action board
CAD	Computer-aided design
CCB	Change control board
CDA	Critical design audit
CDC	Concept Design Center
CDD	Capability development document
CDR	Critical design review
CDRL	Contract data requirements list
CI	Configuration item or critical item
CIL	Critical items list
CM	Critical item or configuration management
CMMI	Capability maturity model integration
CMP	Core MA process
CMU	Carnegie Mellon University
COE	Common operating environment
CONOPS	Concept of operations
COPV	Composite overwrapped pressure vessel
COTS	Commercial off-the-shelf
CPD	Capability production document
CRR	Contractor readiness review
CSCI	Computer software configuration item
CSD	Computer Systems Division
DA	Design assurance
DCMA	Defense Contract Management Agency
DFMA	Design for manufacturing and assembly
DID	Data item description

DPA	Destructive physical analysis
DRMA	Dependability, reliability, maintainability, availability
DSCC	Defense Supply Center Columbus
DTC	Design to cost
ECP	Engineering change proposal
ECS	Environmental control system
EOC	Evidence of completion
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EMRR	Executive mission readiness report
ESD	Event-sequence diagram
ESOH	Environmental safety and occupational health
ESS	Environmental stress screening
ET	Event tree
ETG	Engineering and Technology Group
EVMS	Earned value management system
FCA	Functional configuration audit
FDIR	Failure detection, isolation, and recovery
FFRDC	Federally Funded Research and Development Center
FIST	Final integrated systems test
FMEA	Failure modes and effects analysis
FMECA	Failure modes effects and criticality analysis
FOC	Full operational capability
FPGA	Field programmable gate array
FQR	Formal qualification review
FRACAS	Failure reporting and corrective action system
FRB	Failure Review Board
FRR	Flight readiness review
FTA	Fault tree analysis
GFE	Government-furnished equipment
GFP	Government furnished property
GIDEP	Government industry data exchange program
GST	Ground System test
GOTS	Government off-the-shelf
GN&C	Guidance, navigation, and control
GPS	Global Positioning System
GSE&I	General systems engineering and integration
HAR	Hardware acceptance review
HBT	Heterogeneous bipolar transistor
HW	Hardware
HWCI	Hardware configuration item
I&T	Integration and test

IBR	Integrated baseline review
ICA	Independent cost assessment
ICD	Initial capability document or interface control document
IMP	Integrated management plan
IMS	Integrated master schedule
IOC	Initial operational capability
IPA	Independent program assessment
IPS	Integrated program summary
IPT	Integrated program team
IRRT	Independent readiness review team
IST	Integrated system test
ITA	Independent technical assessment
IUT	Item under test
IV&V	Independent verification and validation
JPO	Joint Program Office
JROC	Joint Oversight Requirements Committee
KDP	Key decision point
KTR	Contractor
LRR	Launch readiness review
LLIL	Limited life items list
MA	Mission assurance
MA	Manufacturing assurance
MAF	Mission assurance framework
MAG	*Mission Assurance Guide*
MAITF	Mission Assurance Improvement Task Force
MAP	Mission assurance plan
MARA	Mission assurance reviews and activities
MLE	Mean life estimate
MLD	Master logic diagram
MM	Manufacturing management
MMD	Mean mission duration
MMP	Manufacturing management plan
MM/PCR	Manufacturing management/production capability review
MRR	Mission readiness review or (as used in Chapter 6) manufacturing readiness review
MS	Mission success
MTTF	Mean time to failure
NDI	Nondevelopmental item
NEPA	National Environmental Policy Act

NPS	Nonprogram-specific
NSS	National Security Space
NSS 03-01	National Security Space Acquisition Policy, Number 03-01
O&SHA	Operating and support hazard analysis
OD	Operational demonstration
OHHA	Occupational health hazard assessment
OOH	Orbit Operation Handbook
OSS&E	Operational safety, suitability, and effectiveness
OT&E	Operational test and evaluation
OV	Operational architecture view
PAPL	Program approved parts list
PAR	PMP approval request
PCA	Physical configuration audit
PCR	Production capability review
PDA	Preliminary design audit
PDR	Preliminary design review
PESHE	Programmatic environment, safety, and occupational health evaluation
PFR	Post-flight review
PHA	Preliminary hazard analysis
PHL	Preliminary hazard list
PPL	Preliminary parts list
PH&ST	Packaging, handling, storage, and transportation
PI	Program integrator
PLR	Post-launch review
PM&P or PMP	Parts, materials, and processes
PMPSL	PMP selection list
PoF	Probability of failure
PRA	Probabilistic risk assessment
Pre-KDP	Pre-key decision point
PRR	Production readiness review
QA	Quality assurance
QCI	Quality conformance inspections
QML	Qualified manufacturing line
QMS	Quality management system
QPL	Qualified product list
RAVP	Requirements analysis and verification planning
RBD	Reliability block diagrams
RFP	Request for Proposal
RM	Risk management

RMP	Risk management plan
SAMP	System acquisition and management plan
SCAMPI	Standard CMMI® appraisal methods for process improvement
SDF	Software development folder
SDP	Software development plan
SDR	System design review
SE	Systems engineering
SEE	Single-event effect
SEI	Software Engineering Institute
SEP	Systems engineering plan
SETA	System Engineering and Technical Assistance
SHA	System hazard analysis
SLOC	Source lines of code
SM	Single manager
SMC	Space and Missile Systems Center
SMD	Supporting MA Discipline
SoS	System of systems
SPF	Single-point failure
SPO	System program office
SOO	Statement of objectives
SOW	Statement of work
SRCA	Safety requirements/criteria analysis
SRD	System requirements document
SRR	System requirements review
SSHA	Subsystem hazard analysis
SSPM	Software standards and procedures manual
SSPP	System safety program plan
SV	Space vehicle
SVR	System verification review
SW	Software
SWAMP	Software acquisition management plan
SWCI	Software configuration item
T&E	Test and evaluation
TEMP	Test and evaluation master plan
TIM	Technical interchange meeting
TLYF	Test Like You Fly
TPM	Test performance metric or technical performance measure
TRD	Technical requirement document
TRR	Test readiness review
TT&C	Telemetry, Tracking and Command

TV	Technical architectural view
UIS	User interface specification
UUT	Unit under test
VWG	Verification working group
WBS	Work breakdown structure
WCCA	Worst-case circuit analysis

Appendix A3
Mission Assurance Verification Matrix Task Database Report (from September 27, 2006)

NOTE: A report from the Mission Assurance Verification Matrix database (aka MA task database), MA core process (section 1) and discipline hierarchy (section 2) tree views is provided below. This MA task database report reflects the database as of September 27, 2006, and is provided for illustrative purposes. Since the MAVM task database is a living database, the MA specialist should request an updated report with the current database contents before using this reference material. To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Appendix A3-1
Core Process Hierarchy Tree View
Requirements Analysis and Validation

Pre-KDP A Concept Studies (Phase 0)
- Program planning
  - Assess program planning
    - Assess acquisition strategy
    - Assess readiness for KDP A
    - Verify adequacy of Phase A RFP
      - Assess indicated program resources
      - Asses compliance documents
      - Assess TRD
      - Assure SOO-SOW/CDRL
  - Structural technology assessment, validation, and transition (example)
- Systems engineering
  - Assess systems engineering processes and products
    - Validate simulations and modeling tools
    - Validate selection of system concept
      - Assess AoA
      - Conceptual design studies
        - Verify multispectral and hyperspectral imaging concept and risk (example)
        - Mass properties studies (example)
        - Space mechanism studies (example)
        - Space structures studies (example)

- Conduct laser active remote sensing concept study (example)
- Assess nano satellite constellation concepts (example)
- Assess laser active remote sensing concept (example)

Verify system concept

- Verify initial capabilities description document
  - Assess spacecraft energy storage concept (example)
  - Assess space materials (example)
  - Technology concept risk assessment—controls (example)
  - Assess spectral signatures, backgrounds, and calibration technology (example)
  - Propulsion technology assessments (example)
    - Propulsion requirements analysis
    - Assess electric propulsion technology (example)
    - Technology concept risk assessment—propulsion
  - Assess space weather impacts (example)
- Assess threats
- Assess technology maturity
  - Assess space system technology
    - Assess nano technology and nano satellite (example)
    - Assess space materials (example)
  - Assess launch vehicle technology
    - Structural technology assessment, validation, and transition
  - Assess ground systems technology
- Assess architectural views
- Assess spectrum availability

Assess CONOPS

Assess technology demonstration requirements

Concept Development (Phase A)

- Program planning
  - Assess program planning
    - Assess updated acquisition strategy
    - Assess program executability
      - Assess Phase A negotiated contract
      - Assess Phase A baseline
      - Assess program cost and schedule estimate
      - Assure compliance to recommended standards and specifications
    - Verify technology maturity level requirement
    - Verify readiness for KDP B
    - Verify follow-on RFP
      - Assess updated acquisition strategy
      - Assess compliance documents
      - Verify TRD/system specification
      - Assess SOO/SOW
- Systems engineering
  - Assess systems engineering products and processes
    - Assess model and simulation accuracy and plans
      - Assess preliminary mission planning
      - Develop independent system performance simulation/model
    - Evaluate system concept and requirements
      - Assess system trade studies
        - Control system concept evaluation (example)
        - Spacecraft and payload controls concept development (example)

- Assess threats and mitigations
- Assess radio frequency plan
- Assess system requirements
  - Verify system characteristics
    - Assess status of orbital allocation planning
    - Assure completeness of performance evaluation
    - Verify KPPs and TPMs
    - Define and assess mission-unique requirements
    - Incorporate requirements into implementing documentation (ICD/PRD)
    - Review mission specifications
    - Review mission PRDs
  - Verify system specifications and interface requirements completeness and accuracy
  - Verify traceability to top-level program requirements
    - Identify derived requirements
    - Assure completeness of requirements
  - Assure situation awareness has been adequately addressed
- Assure supporting MA disciplines
  - Link to risk management
  - Link to reliability engineering
  - Link to configuration control
  - Link to parts, materials, and processes
  - Link to quality assurance
  - Link to system safety
  - Link to software assurance
- Assure other supporting specialty engineering
  - Assess electromagnetic compatibility plans

- Assess mass property plans
- Assess contamination control plan
  - Assess outgassing control (example)
- Assess information assurance plans
- Assess human/machine interface standards and plans
- Assess environmental health and safety plans
- Assess environmental analysis plans
- Assess integrated logistic support plan
- Assess survivability requirements
  - Assure radiation requirements

Assess preliminary verification plan
- Assure integrated verification test plan
- Assess best practice compliance

Assess systems engineering process maturity
- Assess SEMP

Capture Lessons Learned

System

Verify system requirements allocations

Space segment

Verify space segment interface requirements

Verify space segment requirement allocation flow-down
- Validate space vehicle/adaptor and subsystem requirements and allocations

Validate space segment verification plans
- Verification planning CDRL (example)

Space vehicle
- Validate spacecraft and adaptor requirements

- Spacecraft
  - Spacecraft subsystems
    - Thermal control
      - Space vehicle thermal requirements definition
    - Electrical power and distribution
      - Power subsystem requirements review
      - Spacecraft energy storage concept development (example)
    - Propulsion and ordnance
      - Requirements definition (example)
        - Specification requirements development
      - Satellite propulsion requirements analysis (example)
      - Trade study analysis
        - Concept analysis tool development—propulsion
      - Electric propulsion support (example)
    - Structures and mechanisms
      - Requirements definition and proposal evaluation
      - Structural requirements definition
        - Space vehicle conceptual design of structures (example)
    - GN&C
      - Space vehicle control systems requirements analysis
        - Requirements analysis (example)
        - Control system concept evaluation (example)
    - Software
      - Software requirements analysis
      - Software design analysis
    - Telemetry, tracking, and command

Added task
- Payload
  - Validate payload requirements
    - Multispectral and hyperspectral imaging (example)
    - P/L communication requirements verification (example)
    - Optical communication concept development (example)
  - GSE
    - Verify space system GSE requirements
- Launch segment
  - Verify launch segment requirement and allocations
    - Verify launch segment verification plans
    - Verify launch segment requirement allocations
      - Verify launch vehicle and subsystem requirements and allocations
      - Fluid and thermal requirements definition (example)
        - Launch vehicle configuration concept studies
        - Fluid and thermal analysis tools development
      - Propulsion requirements definition (example)
      - Assess liquid propulsion system trade studies (example)
        - Propulsion requirements definition
        - Propulsion feasibility/prototype demonstration
        - Propulsion system trade studies
      - Assess launch vehicle conceptual structural design (example)
      - Assess structural requirements (example)
      - Assess launch vehicle thermal requirements (example)
      - Requirements definition (example)
        - Specification requirements development

- Verify launch system GSE requirements
- Verify ground segment requirements and allocations
  - Assess allocated ground control element, subsystem, and CI requirements
  - Assess allocated mission processing elements, subsystem, and CI requirements
  - Assess requirements verification plans

Preliminary Design (Phase B)

- Program planning
  - Assess program planning
    - Assess updated acquisition strategy
    - Assess program executability
      - Assess Phase B negotiated contract
      - Assess Phase B baseline
      - Assess program cost and schedule estimate
      - Assure compliance with pertinent standards and specifications
    - Verify technology maturity level requirement
    - Verify readiness for KDP C
    - Verify follow-on RFP
      - Assess updated acquisition strategy
      - Assess compliance documents
      - Verity TRD/system specification
      - Assess SOO/SOW
- Systems engineering
  - Assess systems engineering products and processes
    - Assess simulations and models for end-to-end performance accuracy
      - Assure simulations and models are updated and validated

- Assess systems engineering process maturity
  - Assess updated SEMP
- Evaluate preliminary design and requirements
  - Assess system requirements and interfaces
    - Assess preliminary mission planning
    - Verify updated requirements for completeness and accuracy
      - Verify systems requirements allocation
        - Assess system performance margins
        - Verify KPPs and TPMs
        - System requirements traceability
        - Identify derived requirements
    - Assess space vehicle external interface definition
    - Assess requirements verification and tracking system
      - Assess preliminary verification plan
      - Assess VCRM adequacy
        - Verification tracking system
      - Assess integrated verification strategy
      - Verification compliance
    - Assure interface control process is understood and managed at the SPO level
  - Assess frequency plan
- Assure supporting MA disciplines
  - Link to risk management
  - Link to reliability engineering
  - Link to configuration control
  - Link to parts, materials, and processes
    - Single event upset requirements flow-down

- Dose rate survivability requirements flow-down
  - Link to quality assurance
  - Link to system safety
  - Link to software assurance
- Assure other supporting specialty engineering
  - Assess EMC plans
  - Assess mass property plans
  - Assess contamination control plan
  - Assess information assurance plans
  - Assess human/machine interface standards and plans
  - Assess environmental health and safety plans
  - Assess environmental requirements
  - Assess integrated logistic support plan
  - Assess survivability requirements
- Capture Lessons Learned

System

- Verify ground segment requirements and allocations
  - Verify allocated ground control element, subsystem, and CI requirements
  - Verify allocated mission processing elements, subsystem, and CI requirements
  - Assess requirements verification plans
- Validate updated system requirements allocations
- Space segment
  - Validate updated space segment interface requirements
    - Validate updated space segment verification plans
    - Validate updated space segment requirement allocations
  - Space vehicle

- Validate space vehicle/adaptor and subsystem requirements and allocations
  - Validate environmental and ordnance requirements (example)
- Spacecraft
  - Spacecraft subsystems
    - Thermal control
      - Space vehicle thermal requirements definition (example)
    - Electrical power and distribution
      - Power subsystem/FSW compatibility
      - Power subsystem requirements review
      - Power subsystem requirements flow down
        - Solar array requirements (example)
        - Spacecraft energy storage concept development (example)
    - Propulsion and ordnance
      - Satellite propulsion requirements analysis
    - Structures and mechanisms
      - Preliminary design load requirements
      - Review moving mechanical assembly requirements
    - GN&C
      - GN&C requirements analysis (example)
      - Space vehicle control systems requirements analysis (example)
    - Software
      - Software requirements analysis (example)
- GSE
  - Verify space system GSE requirements and interfaces
- Launch segment
  - Verify launch segment requirement and allocations

- Assess launch segment verification plans
- Verify launch segment requirement allocations
  - Verify launch vehicle and subsystem requirements and allocations
    - Assess structural requirements
    - Fluid and thermal requirements definition
    - Propulsion requirements definition
    - Assess launch vehicle thermal requirements (example)
    - Preliminary design load requirements
    - Advanced technologies adaptation
- Verify launch system GSE requirements
- Verify allocated facilities and range support

Complete Design (Phase C)

- Program planning
  - Assess program planning
    - Assess program executability
      - Assess Phase C negotiated contract
      - Assess Phase C baseline
      - Assess program cost and schedule estimate
      - Verify compliance with pertinent standards and specifications
    - Verify technology maturity level requirement
    - Verify readiness for build/production decision
    - Verify follow-on RFP
      - Assess updated acquisition strategy
      - Assess compliance documents
      - Verity TRD/system specification

- Assess SOO/SOW
- Systems engineering
  - Assess systems engineering processes and products
    - Assess simulations and models for end-to-end performance accuracy
      - Assure simulations and models are updated and validated
    - Evaluate complete design and requirements
      - Verify and maintain requirement set integrity
        - Verify updated system specifications and interface requirements completeness and accuracy
          - Assess change control process
      - Assess preliminary mission planning
      - Assess requirements verification and tracking system
        - Assess VCRM adequacy
        - Final verification planning
        - Verification tracking system
      - Assess frequency filing status
    - Assure supporting MA disciplines
      - Link to risk management
      - Link to reliability engineering
      - Link to configuration control
      - Link to parts, materials and processes
        - Dose rate survivability requirements flow-down
      - Link to quality assurance
      - Link to system safety
      - Link to software assurance
    - Assure other supporting specialty engineering
      - Assess EMC plans

- Assess mass property plans
- Assess contamination control plan
- Assess information assurance plans
- Assess human/machine interface standards and plans
- Assess environmental health and safety plans
- Assess environmental requirements
- Assess integrated logistic support plan
- Assess survivability requirements

Assess systems engineering process maturity

- Assure interface control process is understood and managed at the SPO level
- Assess updated SEMP

Capture Lessons Learned

System

Validate updated system requirements allocations

Space segment

Validate updated space segment requirement

- Validate updated space segment verification plans
- Validate updated space segment requirement allocations
  - Validate updated allocated subsystem and CI requirements

Space vehicle

- Spacecraft
  - Spacecraft subsystems
    - Assess updates to spacecraft subsystem requirements
- Payload
  - Assess updates to payload subsystem requirements
- GSE

Assess updated space system GSE requirements and interfaces
Launch segment
Validate updated launch segment requirement and allocations
Assess updated launch segment verification plans
Validate launch segment requirement allocations
Validate updated launch vehicle and subsystem requirements and allocations
Assess allocated facilities and range support
Ground segment
Validate ground segment requirements and allocations
Validate updated ground control element, subsystem, and CI requirements
Validate updated allocated mission processing elements, subsystem, and CI requirements

Fabrication/Coding, Test, and Integration (Phase D1)
Program planning
Assess production contract
Systems engineering
Assess systems engineering processes and products
Evaluate product baseline design and requirements
Assess system requirements and interfaces
Verify updated system specifications and interface requirements completeness and accuracy
Assure interface control process is understood and managed at the SPO level
Assess system performance
Verify KPPs and TPMs
Assure change management process is being maintained
Assess requirements verification and tracking system

- Final verification planning
- Verification tracking system
- Assess frequency filing status
- Assure simulations and models are updated and validated
- Assess systems engineering process maturity level
- Assess updated SEMP
- Assure supporting MA disciplines
- Assure other supporting specialty engineering
- Capture Lessons Learned

System

- Validate updated system requirements allocations
- Space segment
- Validate updated space segment requirements
- Validate updated space segment verification plans
- Validate updated space segment requirement allocations
- Validate updated allocated subsystem and configuration item requirements
- Space vehicle
- Spacecraft
- Spacecraft subsystems
- Assess updates to spacecraft subsystem requirements
- Payload
- Assess updates to payload subsystem requirements
- GSE
- Validate updated space system GSE requirements and interfaces
- Launch segment
- Verify updated launch segment requirement allocations

- Assess updated launch segment verification plans
- Verify launch segment requirement allocations
  - Verify updated launch vehicle and subsystem requirements and allocations
- Verify updated launch system GSE requirements
- Verify allocated facilities and range support

Verify updated launch system GSE requirements

Ground segment

Verify ground segment requirement allocations

- Verify updated ground control element, subsystem, and CI requirements
- Verify updated allocated mission processing elements, subsystem, and CI requirements

Fielding and Checkout (Phase D2)

Systems engineering

Assess systems engineering processes and products

Continue assessment of product baseline design and requirements

- Verify updated system specifications and interface requirements completeness and accuracy
- Verify system effectiveness
  - Verify KPPs and TPMs
  - Assess demonstrated margins
- Assess final mission planning

Assure simulations and models are updated and validated

Assess SE process maturity level

Assure supporting MA disciplines

- Link to risk management
- Link to reliability engineering
- Link to configuration control

- Link to parts, materials and processes
- Link to quality assurance
- Link to system safety
- Link to software assurance

Assure other supporting specialty engineering

- Assess mass property plans
- Assess contamination control plan
- Assess information assurance plans
- Assess human/machine interface standards and plans
- Assess environmental health and safety plans
- Assess environmental analysis plans
- Assess integrated logistic support plan
- Assess survivability requirements
- Assess EMC plans

Capture Lessons Learned

Operations, Maintenance, Disposal (Phase D3)

Systems engineering

Assess systems engineering processes and products

Evaluate the operational system

- Verify system effectiveness
  - Verify KPPs and TPMs
  - Assess demonstrated margins

Update simulations and models for end-to-end performance accuracy

- Assure simulations and models are updated and validated

Assure supporting ma disciplines

- Link to risk management
- Link to reliability engineering
- Link to configuration control
- Link to parts, materials and processes
- Link to quality assurance
- Link to system safety
- Link to software assurance

Assure other supporting specialty engineering

- Assess EMC plans
- Assess mass property plans
- Assess contamination control plan
- Assess information assurance plans
- Assess human/machine interface standards and plans
- Assess environmental health and safety plans
- Assess environmental analysis plans
- Assess integrated logistic support plan
- Assess survivability requirements

Capture Lessons Learned

Non-program specific

System

Space segment

Space vehicle

Spacecraft

Spacecraft subsystems

Structures and mechanisms

Structural analysis methods and standards

Appendix A3-2
Design Assurance

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Pre-KDP A Concept Studies (Phase 0)
- Program planning
  - Assess program planning
    - Assess acquisition strategy
    - Assure RFP adequacy
      - Asses compliance documents
      - Assess TRD
      - Assure SOO-SOW/CDRL
- Systems engineering
  - Assess design related systems engineering processes and products
    - Assure readiness for technology push programs
    - Assure analysis of alternate concept designs
    - Verify system architecture and interface designs are compatible

Concept Development (Phase A)
- Program planning
  - Assess program planning
    - Assess updated acquisition strategy
    - Assess program executability
      - Assure Phase A contract maintains design assurance integrity

- Assess Phase A program baseline
- Assure adequacy of follow-on RFP
  - Assess compliance documents
  - Assess TRD
    - RFP—mechanisms requirement definition (example)
    - RFP—satellite propulsion (example)
    - RFP—space vehicle mass properties verification (example)
    - RFP—structural dynamics processes (example)
  - Assure SOO-SOW/CDRL

Systems engineering

- Assess design-related systems engineering processes and products
  - Assess system design tools and simulations
  - Assess system design concept studies
  - Assess system design effectiveness
    - Assess design relative to KPPs and TPMs
    - Assess system design margins
  - Assess system design specifications
  - Assess design management process
    - Assess contractor's design management plan
    - Assess government design assurance plan
    - Assess general design standards and processes
    - Assess design process execution
  - Assess technology push demonstrations
  - Assure system design feasibility demonstration
    - Verify enabling technology readiness level and demonstrations
      - Assure adequacy of technology demonstrations

- Assess microelectronics, optoelectronics, and MEMS technology (example)

Assure supporting MA disciplines

- Risk assessment and management
- Reliability engineering
- Configuration management
- Parts, materials, and processes
  - Assess space materials (example)
- Quality assurance
- System safety assurance
- Software assurance

Assure other specialty engineering disciplines

- Assess space weather impacts
- Assess EMC design
- Assess mass property design process
  - Mass model verification
  - Assess mass properties estimates
  - Mass properties control plan
  - Mass properties support
  - Mass properties verification
- Assess contamination control design approach
  - Spacecraft and launch vehicle contamination
- Assess information assurance plans
- Assess human/machine interface standards and plans
- Assess environmental health and safety plans
- Assess environmental analysis plans
- Assess integrated logistic support plan

- Assess survivability system design
- Capture Lessons Learned

System

- Assure adequacy of the segment designs
- Space segment
  - Verify space segment system design
    - Assess space segment design feasibility/utility
    - Assure design testability
    - Assure design producibility
    - Assure design supportability
  - Space vehicle
    - Spacecraft
      - Spacecraft subsystems
        - Thermal control
          - Thermal requirements definition
        - Electrical power and distribution
          - Assess power subsystem trade studies technology readiness
          - Assess power hardware architecture
          - Assess solar array trade studies
        - Propulsion and ordnance
          - Assess advance ordnance technologies adaptation
          - Assess satellite propulsion trade studies
        - Structures and mechanisms
          - Assess conceptual mechanisms design
        - GN&C
          - Assess ACS design concept

- Spacecraft and payload concept development
- Assess spacecraft GN&C design concept
- Spacecraft mission design
- ACS design integrity verification planning

Payload

- Assess space instrumentation (example)
- Assess laser active remote sensing concept development (example)
- Assess spectral signatures, backgrounds, and calibration (example)

Launch segment

Assess launch segment system design

Verify enabling technology readiness level and demonstrations

- Assess solid propulsion technology readiness
- Assess advance ordnance technologies adaptations
- Assess propulsion feasibility/prototype demonstration

Assess system design feasibility/utility

- Conceptual design-mechanisms
- Launch vehicle configuration concept studies
- Propulsion system conceptual design assessment
- Assess liquid propulsion system trade studies
- Solid motor performance analysis
- Assess launch vehicle conceptual structural design
- Assess GN&C design concept
- Assess power hardware architecture

Assure design testability

Assure design producibility

Assure design supportability

- Ground segment
  - Verify ground control segment system design
    - Verify enabling technology readiness level and demonstrations
    - Assess system design feasibility/utility
    - Assure design testability
    - Assure design producibility
    - Assure design supportability

Preliminary Design (Phase B)

- Program planning
  - Assess program planning
    - Assess updated acquisition strategy
    - Assess program executability
      - Assure Phase B contract maintains design assurance integrity
      - Assess Phase B program baseline
    - Assess follow-on RFP
      - Assess compliance documents
      - Assess TRD
        - RFP—mechanisms requirement definition (example)
        - RFP—satellite propulsion (example)
        - RFP—SV mass properties verification (example)
        - RFP—structural dynamics processes (example)
      - Assure SOO-SOW/CDRL
- Systems engineering
  - Assess design related systems engineering processes and products
    - Assess system design tools and simulations

- Assess system design concept studies
- Prepare mission-specific Aerospace IV&V plan
  - Assess adequacy of contractor requirements verification matrix
  - Review of contractor analysis of interface requirements changes
  - Review of contractor analysis of interface requirements verification
- Assess updated system design effectiveness
  - Assess system design margins
  - KPPs
- Assess preliminary design specifications
  - Acoustic, vibration and shock modeling (example)
- Assess design assurance implementation
  - Assure adequacy of PDAs—see also PDA task in MA reviews and audits
  - Verify execution of KTR design management plan
  - Verify execution of government design assurance plan
  - Design assurance metrics
- Assess technology push demonstrations
- Assure system design feasibility demonstration
  - Validate microelectronics, optoelectronics, and MEMS technology insertion plans (example)
- Assure supporting MA disciplines
  - Risk assessment and management
  - Reliability engineering
  - Configuration management
  - Parts, materials and processes
    - Microelectronics reliability and radiation effects
    - Assess space materials
  - Quality assurance

- System safety assurance
- Software assurance

Assure other specialty engineering disciplines

- Assess EMC design
- Assess mass property estimates
  - Design review and analysis
  - Critical mass properties analysis
  - Weight growth allowance
  - Design optimization
  - Mass properties control plan
  - Balance weight design analysis
  - Mass properties verification
- Assess contamination control design
  - Assess vehicle contamination-control design approach
- Assess information assurance plans
- Assess human/machine interface standards and plans
- Assess environmental health and safety plans
- Assess environmental analyses
  - Assess thermal vacuum sensitivity
  - Verify vehicle acoustic, vibration, and shock environments (example)
- Assess integrated logistic support plan
- Assess preliminary survivability design
  - Radiation hardness assurance
  - Space weather
  - Hypervelocity impact analysis

Lessons Learned

- System
  - Assess ground system design attributes
    - Assess ground control system design attributes
      - Assess mission processing hardware design attributes
      - Assess ground control hardware design attributes
      - Assess mission processing software design attributes
      - Assess ground control software design attributes
    - Assess mission processing design attributes
  - Verify preliminary segment designs
  - Space segment
    - Verify preliminary space segment design
      - Assess space segment design feasibility/utility
      - Assure design testability
      - Assure design producibility
      - Assure design supportability
    - Space vehicle
      - Assure design requirements are flowed-down
      - Verify detailed preliminary design
      - Verify preliminary space vehicle, subsystem, and unit designs
      - Spacecraft
        - Spacecraft subsystems
          - Thermal control
            - Assess thermal optical properties (example)
            - Thin film coating evaluation (example)
            - Verify thermal environmental constants
            - Preliminary thermal design review

- Electrical power and distribution
  - Assess electrical/power subsystem design attributes
    - Assess S/A design
    - Assess S/A design analyses and tests
    - Assess power subsystem worst-case analyses
    - Assess energy storage preliminary design
    - Verify electrical power Phase B milestone exit criteria are met
- Propulsion and ordnance
  - Assess propulsion and ordnance subsystem design attributes
    - Perform independent propulsion design verification
    - Ordnance requirements definition
    - Assess ordnance design
    - Ordnance verification planning
    - Ordnance development oversight
    - Device design review
    - Electric propulsion support (example)
- Structures and mechanisms
  - Assess structural and structural dynamics subsystem design attributes
    - Preliminary structural design review
    - Preliminary design load requirements
  - Assess mechanical/mechanisms subsystem design attributes
    - Verify mechanical design
- GN&C
  - Assess control subsystem design attributes
    - Assess attitude and P/L ctrl algorithm design and analyses
    - Perform independent stability and control analysis

- Assess ACS preliminary design
- Assess navigation and guidance subsystem design attributes
- Spacecraft mission design—flight mechanics
- ACS design integrity verification planning
- Data management
- Assess data handling/TT&C subsystem design attributes
- Software
- Assess flight software design attributes
- Payload
- Verify preliminary payload design
- Assess payload sensor subsystem design attributes
- Laser active remote sensing preliminary design
- Assess spectral signatures, backgrounds, and calibration
- Assess multispectral and hyperspectral imaging
- Assess payload signal and data processing subsystem design attributes
- Assess payload communications and antenna subsystem design attributes
- Assess optical communication subsystem design
- Space instrumentation
- GSE
- Assess GSE attributes
- Assess ground hardware elements design attributes
- Assess ground software element design attributes
- Launch segment
- Verify preliminary launch segment system design
- Verify preliminary launch subsystems and unit designs
- Assure design testability

Assure design producibility
Assure design supportability
Assess range safety interface and destruct subsystem design attributes
Design review and assessment
Assess flight software design attributes
    Likelihood/consequence risk assessment
Assess navigation and guidance subsystem design attributes
    Assess launch vehicle guidance algorithm design and analyses
Assess flight controls subsystem design attributes
    Assess attitude and payload control algorithm design and analysis
    Perform an independent stability and control analysis
    Assess ACS preliminary design
Assess structural and structural dynamics subsystem design attributes
    Preliminary design load requirements
Assess electrical/power subsystem design attributes
    Power subsystem worst-case analysis
    Energy storage preliminary design
    Electrical Phase B exit milestones
Assess thermal subsystem design attributes
    Preliminary design of fluid and thermal systems
    Preliminary thermal design review
Assess structural and structural dynamics subsystem design attributes
    Preliminary structure design
Assess propulsion and ordnance subsystem design attributes
    Assess launch vehicle engine performance analysis
    Assess preliminary launch vehicle liquid propulsion design

- Assess launch vehicle solid motor performance analysis
- Assess launch vehicle solid motor performance analysis
- Launch vehicle solid propulsion verification planning
- Ordnance requirements definition
- Launch vehicle ordnance specification requirements development
- Ordnance verification planning
- Ordnance development oversight
- Device design review
- Assess mechanical/mechanisms subsystem design attributes
  - Verify mechanical design
- Assess TT&C system design attributes
- Assess preliminary mission design attributes
  - Launch vehicle mission design
  - Launch vehicle performance
- Assess launch site facilities and range interface design attributes
- Assess GSE design attributes
  - Assess ground hardware elements design attributes
  - Assess ground software element design attributes

Complete Design (Phase C)

- Program planning
  - Assess program planning
    - Assess program executability
      - Assure Phase C contract maintains design assurance integrity
      - Assess Phase C program baseline
    - Assess follow-on RFP preparation activities

- Assess compliance documents
- Assess TRD
- Assure SOO-SOW/CDRL

Systems engineering

- Assess design-related systems engineering processes and products
  - Assess system design tools and simulations
    - Assess space vehicle/launch vehicle interface structural qualification history
    - Assess prelaunch ECS analysis (fairing purge)
    - Assess contamination analysis
    - Assess EMC/EMI analysis
    - Performance mass properties validation
    - Assess CLA
    - Calculate space vehicle loads, accelerations, deflections
    - Compare CLA response results with contractor results and resolve any differences
  - Assess updated system design effectiveness
    - Assess transportation and handling equipment
    - Assess launch vehicle/space vehicle assembly, erection, and mating systems
    - Assess payload compatibility drawing compliance with requirements
    - Assess mission modifications
    - Assess system design margins
    - KPPs
  - Assess final design specifications
  - Assess design assurance implementation
    - Validate CDA process (see also CDA task in MA reviews and audits)
    - Assess FCA process (see also FCA task in MA reviews and audits)
    - Verify execution of KTR design management plan

- Verify execution of government design assurance plan
- Assess design change process
- Design assurance metrics

Assess technology push demonstrations

Assure system design feasibility demonstration

- Microelectronics, optoelectronics, and MEMS technology implementation validation

Update simulations and models for end-to-end performance verification

Assure supporting MA disciplines

- Risk assessment and management
- Reliability engineering
- Configuration management
- Parts, materials, and processes
  - Evaluate space materials (example)
- Quality assurance
- System safety assurance
- Software assurance

Assure other specialty engineering disciplines

- Assess EMC design
  - EMC requirements
- Assess mass property estimates
- Assess contamination control
- Assess information assurance plans
- Assess human/machine interface standards and plans
- Assess environmental health and safety plans
- Assess survivability design verifications

Lessons Learned

- System
  - Verify the complete segment designs
  - Space segment
    - Verify final space segment design
      - Assure design testability
      - Assure design producibility
      - Assure design supportability
    - Space vehicle
      - Spacecraft
        - Verify final spacecraft subsystems and unit designs
          - Validate space vehicle fluid and thermal subsystems design (example)
        - Spacecraft subsystems
          - Thermal control
            - Assess thermal subsystem design attributes
              - Thermal uncertainty margin
              - Thermal test effectiveness
              - Thermal model verification
              - Heater control authority
              - Thermal unit design techniques
              - Evaluate thin film coating
          - Electrical power and distribution
            - Assess electrical/power subsystem design attributes
              - Solar array design
              - Power subsystem design
              - Assess spacecraft energy storage final design
          - Propulsion and ordnance

- Assess propulsion and ordnance subsystem design attributes
  - Space vehicle independent verification of propulsion critical design
  - Verification of qualification test plans for propulsion
  - System design review
  - Performance analysis
  - Space vehicle ordnance test planning
  - Modeling capability development
  - Assess electric propulsion design
- Fluid mechanics independent assessment and analysis

Structures and mechanisms

- Assess mechanical/mechanisms subsystem design attributes
  - Independent analysis
  - Assess moving assembly reliability
- Assess structural and structural dynamics subsystem design attributes
  - Independent design loads assessment
  - Independent loads analysis methodologies
  - Load cycle process
    - Structural design review and assessment

GN&C

- Assess navigation and guidance subsystem design attributes0
  - Spacecraft mission design—flight mechanics
- Assess control subsystem design attributes
  - Stability and control analysis for spacecraft
  - Trajectory control and performance validation
  - Stability and control analysis for space vehicles
  - Space vehicle ACS independent design verification

- Independent space vehicle stability and control analysis
- Independent space vehicle stability and control analysis
- Data management
  - Assess data handling/TT&C subsystem design attributes
- Software
  - Assess flight software design attributes

Payload

- Assess payload subsystem design attributes
  - Assess payload sensor design attributes
    - E/O performance test approach
    - Assess laser active remote sensing final design
    - Verify spectral signatures, backgrounds and calibration
    - Multispectral and hyperspectral imaging
  - Assess payload signal and data processing subsystem design attributes
  - Assess payload communications and antenna subsystem design attributes
    - Optical communication technology
    - Assess CES integrated design
    - Assess payload communication performance
    - CES environmental requirements
    - CES performance capabilities vs. requirements
    - CES unit reliability
    - Assess optical communication design
  - Space instrumentation

GSE

- Assess GSE design attributes
  - Assess ground hardware elements design attributes

GSE
Assess ground software element design attributes
Launch segment
Verify final launch segment system design
Verify final launch subsystems and unit designs
Assure design testability
Assure design producibility
Assure design supportability
Assess range safety interface and destruct subsystem design attributes
Assess flight software design attributes
Assess navigation and guidance subsystem design attributes
Validate trajectory control and performance
Validate GN&C and trajectory performance
Assess inertial navigation performance
Assess GN&C failure detection and isolation
Range safety verification
Assess flight controls subsystem design attributes
Assess launch vehicle stability and control
Validate spacecraft separation
Verify launch vehicle ACS design
Verify launch vehicle independent stability and controls
Verify launch pad clearance and drift
Stability and control analysis for launch vehicle
Launch vehicle controllability and placard design evaluation
Collision and contamination avoidance analysis
Staging analysis

- Assess electrical/power subsystem design attributes
  - Power subsystem worst-case analysis
  - Energy storage final design
  - Electrical Phase C exit milestones
- Assess thermal subsystem design attributes
  - Thermal uncertainty margin
  - Thermal test effectiveness
  - Thermal model verification
  - Heater control authority
  - Thermal unit design techniques
  - Launch vehicle fluid and thermal environments definition
  - Launch vehicle design review of fluid and thermal systems
  - Independent assessment and analysis
- Assess structural and structural dynamics subsystem design attributes
  - Independent design loads assessment
  - Independent loads analysis methodologies
  - Load cycle process
  - Structural design review and assessment
  - Independent structural integrity analyses
- Assess propulsion and ordnance subsystem design attributes
  - Verification of flight design for launch vehicle liquid prop
  - Launch vehicle engine performance analysis
  - Launch vehicle liquid propulsion design review and assessment
  - Solid motor performance analysis
  - Launch vehicle solid propulsion verification
  - Launch vehicle system design review—ordnance

Launch vehicle ordnance performance analysis
Launch vehicle ordnance test planning
Independent verification of completed design
Assess the mechanical/mechanisms subsystem design attributes
Independent analysis
Moving assembly reliability
Assess TT&C system design attributes
Assess mission design attributes
Launch vehicle mission design
Assess launch site facilities and range interface design attributes
Assess GSE design attributes
Assess ground hardware elements design attributes
Assess ground software element design attributes
Ground segment
Assess ground system design attributes
Assess ground control system design attributes
Assess mission processing hardware design attributes
Assess ground control hardware design attributes
Assess mission processing software design attributes
Assess ground control software design attributes
Assess mission processing design attributes

Fabrication and Integration (Phase D1)

Program planning
Assess program planning
Assess program executability

- Assure Phase D contract maintains MA integrity
- Assess Phase D program baseline

Systems engineering

- Maintain design-related systems engineering processes and products
  - Update simulations and models
  - Assess updated system design effectiveness
    - Assess system design margins
    - Assess KPPs
  - Assess design change implementation
    - Assess design change process
    - Verify design changes
    - Design assurance metrics for design changes
  - Review closeout photos
  - Verify acceptability of problem/anomaly investigations, resolution, tracking, and documentation
    - Verify hardware nonconformance resolution process
    - Identify and evaluate out-of-family conditions
  - Assess flight worthiness
  - Assure supporting MA disciplines
    - Risk assessment and management
    - Reliability engineering
    - Configuration management
    - Parts, materials, and processes
    - Quality assurance
    - System safety assurance
    - Software assurance
  - Assure other specialty engineering disciplines

- Assess EMC design
  - Verify comm/payload EMC requirements (example)
- Assess mass property estimates
- Assess contamination control
- Assess information assurance plans
- Assess human/machine interface standards and plans
- Assess environmental health and safety plans
- Verify design environments
- Assess survivability design

Lessons Learned

System

Space segment

Verify as-built segment designs meet requirements

- Verify as-built space segment design met requirements

Space vehicle

Spacecraft

Spacecraft subsystems

- Verify as-built spacecraft subsystem and unit-level designs met requirements
  - Verify as-built control subsystem and unit-level designs met requirements
- Thermal control
  - Verify as-built thermal subsystem and unit-level designs met requirements
  - Thermal blanket design verification
- Electrical power and distribution
  - Verify as-built electrical and power subsystem and unit-level designs met requirements
    - Power subsystem flight readiness

- Propulsion and ordnance
  - Verify fluid mechanical subsystem flight worthiness (example)
  - Verify as-built propulsion and ordnance subsystems and unit-level designs meet requirements
    - Ordnance qualification/margin testing
  - Hardware qualification—fluid mechanical components
- Structures and mechanisms
  - Pre-launch IV&V
  - Verify as-built mechanical, mechanism subsystems, unit-level designs met requirements
  - Verify as-built structure, structural dynamics subsystems, unit-level designs met requirements
    - Execute independent loads analyses
    - Monitor structure tests
    - Assess loads, deployments, and vibration structural dynamic models
- GN&C
  - Verify mission-specific design
- Data management
  - Verify as-built data handling/TT&C subsystem and unit-level designs met requirements
- Software
  - Verify as-built flight software design meets requirements
    - Validate SV-ACS hardware/software interfaces

Payload

- Verify as-built payload subsystem meets requirements
  - Verify as-built signal processing subsystem meets requirements

- Verify as-built communications and antenna subsystems meet requirements
- Verify as-built payload sensor subsystem meets requirements
  - Electro-optical sensors environmental evaluation (example)
  - Assess laser active remote sensing test and integration (example)

GSE

- Verify as-built GSE system meets requirements
  - Verify as-built GSE hardware meets requirements
  - Verify as-built GSE software meets requirements

Launch segment

- Verify as-built launch segment meets requirements
  - Verify as-built launch vehicle subsystems meet requirements
    - Verify as-built flight software design meets requirements
    - Verify as-built navigation and guidance subsystems meet requirements
    - Verify as-built flight controls subsystem meets requirements
    - Verify as-built electrical and power subsystems meet requirements
    - Verify as-built thermal subsystem meets requirements
    - Verify as-built structural and structural dynamics subsystem meet requirements
      - Independent loads analysis methodologies
      - Independent loads analyses
    - Verify as-built propulsion and ordnance subsystem meet requirements
    - Verify as-built mechanical and mechanism subsystems meet requirements
      - Pre-launch IV&V (example)
    - Verify as-built TT&C subsystems meet requirements
    - Verify the mission-specific design
  - Verify as-built GSE system design meets requirements
    - Verify as-built GSE hardware design meets requirements

- Verify as-built GSE software design meets requirements
- Ground segment
  - Verify as-built ground systems design meet requirements
    - Verify as-built ground control hardware elements design meet requirements
    - Verify as-built ground control segment design meets requirements
      - Verify as-built ground control software elements design meet requirements
    - Verify as-built mission processing segment design meet requirements
      - Verify as-built mission processing hardware elements design meet requirements
      - Verify as-built mission processing software element designs meet requirements

System Fielding, Test, and Check-out (Phase D2)

- Systems engineering
  - Maintain design related systems engineering processes and products
    - Assure update simulations and models
    - Design changes
    - Assure supporting MA disciplines
      - Risk assessment and management
      - Reliability engineering
      - Configuration management
      - Parts, materials, and processes
      - Quality assurance
      - System safety assurance
      - Software assurance
    - Assure other specialty engineering disciplines
      - Assess EMC design
      - Assess mass properties estimates

- Assess fielded system contamination control
- Assess information assurance implementation status
- Assess human/machine interface implementation status
- Assess environmental health and safety implementation status
- Verify design environments
- Assess survivability design
- Lessons Learned

System

- Verify system and interface performance
  - Verify as-launched and checked-out system design satisfies KPP thresholds
- Validate and support segment designs
- Space segment
  - Validate and support space segment design
  - Space vehicle
    - Spacecraft
      - Spacecraft subsystems
        - Software/avionics reliability assessment
        - Orbit transfer operations
        - Launch and deployment support
        - IMU calibration and alignment
- Launch segment
  - Validate and support launch segment design
    - Launch vehicle performance —flight mechanics
    - HIL system testing
    - Software/avionics reliability assessment
    - Mission unique design review

- Ground segment
  - Validate and support ground systems design

Operations and Disposal (Phase D3)

- Systems engineering
  - Maintain system engineering design assurance related products and processes
    - Verify system and interface performance
      - TPMs
    - Assure supporting ma disciplines
      - Risk assessment and management
      - Reliability engineering
      - Configuration management
      - Parts, materials, and processes
      - Quality assurance
      - System safety assurance
      - Software assurance
    - Assure other specialty engineering disciplines
      - Assess EMC design
      - Assess mass property
      - Spacecraft contamination
      - Assess information assurance plans
      - Assess human/machine interface standards and plans
      - Assess environmental health and safety plans
      - Verify design environments
      - Assess survivability design
    - Lessons Learned

- System
  - Space segment
    - Verify space segment on-orbit mission design
    - Space vehicle
      - Spacecraft
        - Spacecraft subsystems
          - Thermal control
            - On-orbit thermal control system verification
          - GN&C
            - Reentry trajectory reconstruction
            - De-orbit operations

- Non-program specific
  - Program planning
    - ACS technology concept risk assessment
  - Systems engineering
    - Archive and CM assets requirements for software valid and operations support
    - Archive and CM assets requirements for software valid and operations support
  - System
    - Space segment
      - Space vehicle
        - Spacecraft
          - Spacecraft subsystems
            - Propulsion and ordnance
              - Satellite propulsion technology concept risk assessment
              - Advanced prop technology assessment and planning
              - Ordnance specification development

- Structures and mechanisms
  - Fluid and thermal analysis tools development
  - Concept analysis tool development-propulsion
  - Structural analysis methods and standards
  - Independent loads analysis methodologies
- GN&C
  - Over-flight risk assessment

Payload

- Assess spectral signatures, backgrounds, and calibration

Appendix A3-3
Manufacturing Assurance

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Pre-KDP A Concept Studies (Phase 0)
- Program planning
  - Assess program planning
    - Assess adequacy of Phase A RFP for manufacturing assurance

Concept Development (Phase A)
- Program planning
  - Assess program planning
    - Assess contract compliance to manufacturing assurance
    - Assess manufacturing plan
- Systems engineering
  - Assess systems engineering
    - Verify manufacturing management system control
    - Assess manufacturing process integration
    - Assess existing approach for certification of manufacturing process qualification
      - Nano technology and nano satellite fabrication (example)
    - Assess new manufacturing process qualification effectiveness
    - Phase A Lessons Learned
    - Assess manufacturing risk management process
    - Assess process for selection and management of key suppliers

Assure appropriate MA disciplines, plans, and processes relative to manufacturing assurance are integrated
Assure appropriate specialty engineering disciplines, plans, and processes relative to manufacturing assurance are integrated

Preliminary Design (Phase B)

Program planning

Assess program planning

Producibility assessment/review
Assess design for manufacturing and assembly planning
Assess make buy process plans

Systems engineering

Assess systems engineering

Assess preliminary materials, processes, and manufacturing methods for adequacy
Assess accommodation of production-related issues
Assess obsolescence and diminishing manufacturing resources (DMS)
Assure appropriate MA disciplines, plans, and processes relative to manufacturing assurance are integrated
Assure appropriate specialty engineering disciplines, plans, and processes relative to manufacturing assurance are integrated
Phase B Lessons Learned

Complete Design (Phase C)

Program planning

Assess program planning

Assess contractor's facilities, production plan and delivery schedule

- Systems engineering
  - Assess systems engineering
    - Assess contractor's packaging handling and transportation process
    - Assess contractor capability and stability of production process
    - Assess contractor's manufacturing/production readiness reviews
    - Assess contractor's manufacturing control effectiveness
    - Assess manufacturing risk management process
    - Assure appropriate mission assurance disciplines
    - Assure appropriate specialty engineering disciplines
    - Phase C Lessons Learned

Fabrication and Integration (Phase D1)

- Program planning
  - Assess program planning
    - Verify contract ready to manufacture product
- Systems engineering
  - Assess systems engineering
    - Assess manufacturing flow charts
    - Verify manufacturing processes are qualified
    - Evaluate process control methods
      - Assess variability reduction process
    - Verify traceability system
    - Assess as-designed and as-built process
    - Assess manufacturing anomaly resolution process
    - Phase D1 Lessons Learned
- System

Launch segment

Assess hardware acceptance reviews

Liquid propellant (example)

Appendix A3-4
Integration, Test, and Evaluation

Pre-KDP A Concept Studies (Phase 0)

- Program planning
  - Assess program planning
    - Assess readiness for KDP A
    - Assess acquisition strategy
    - Verify adequacy of Phase A RFP
      - Assess updated acquisition strategy
      - Assess compliance documents
      - Assess TRD
      - Assure SOO-SOW/CDRL for IT&E tenets
- Systems engineering
  - Assess systems engineering processes and products
    - Assess testability of all concept alternatives
      - Assess testability of candidate space vehicle system/subsystem technologies
      - Assess testability of the space vehicle system
      - Assess ground support and special test equipment validation strategy
      - Assess needed test infrastructure
      - Assess testability and test requirements of technology demonstrations
    - Assess segment-level verification strategy
    - Evaluate technical performance measures for perceptive testability
    - Assess mission and system operations concepts
    - Assess mission requirements validation strategy
    - Assess segment-level verification strategy

- Assess SV system-level verification strategy
- Verify spec and standard applicability for Phase A
- Assure support from MA disciplines
  - Link to system safety
  - Link to reliability engineering
  - Link to risk management
  - Link to parts, materials, and processes
  - Link to configuration and data management
  - Link to quality assurance
- Assure support from specialty disciplines
  - Links to contamination control
  - Links to electromagnetic compatibility
  - Links to environmental health and safety
  - Links to material sciences
  - Links to physical sciences

Concept Development (Phase A)

- Program planning
  - Assess program planning
    - Assess program executability
      - Review Phase A contract
      - Assess Phase A baseline
      - Assure standards and specifications for applicability and compliance
      - Assess SPO compliance to MAG verification tenets
      - Assure SPO access to contractor facilities and data

- Assess program T&E roles and responsibilities
- Assess test data access and management adequacy

Verify readiness for KDP B
- Assess KDP B readiness

Verify adequacy of follow-on RFP
- Verify TRD/system specification
- Assess SOO/SOW
- Assess compliance documents
- Evaluate Phase B contractor proposal

Systems engineering

Assess systems engineering processes and products

Assess mission and system CONOPS for completeness and to support testability

Assess mission and system requirements for completeness and to support testability

Assess TEMP

Assess service environment requirements

Evaluate TPM adequacy
- Assess end-to-end TPMs
- Assess system-level TPMs

Evaluate contractor test capability

Assess test like you fly deviations

Assess space vehicle internal and external interface definition

Assess need for simulations, models, and test-beds

Evaluate long lead planning and procurement concerns

Assess MA specifications and standards on contract for testing

Assure supporting MA disciplines
- Link to system safety

- Link to reliability engineering
- Link to risk management
- Link to parts, materials and processes
- Link to configuration and data management
- Link to quality assurance
- Assess technology development strategy
- Capture Lessons Learned

System

- Assess concept alternative life cycle test strategy
  - Assess testability of the integrated space and ground elements
    - Assess the testability of the space vehicle system
    - Assess the testability of the ground system
    - Assess the end-to-end testability of the SoS
  - Assess required ground support and special test equipment
  - Assess test infrastructure concepts
  - Assess inter-segment test perceptivity
  - Assess the risk to the flight units/subsystem/system concept due to the stress of ground testing
- Establish integration and test working group
- Space segment
  - Space segment integration
    - Evaluate adequacy of assembly and integration strategy
    - Evaluate long lead planning and procurement issues
    - Assess internal and external interfaces for completeness and testability
      - Assess space to ground interface strategy and functional allocations
  - Space segment test engineering
    - Assess space segment verification strategy and the role of testing

- Assure support from IT&E MA disciplines
  - Link to system safety
  - Link to reliability engineering
  - Link to risk management
  - Link to parts, materials, and processes
  - Link to configuration and data management
  - Link to quality assurance
- Assure support from IT&E specialty engineering disciplines
  - Links to contamination control
  - Links to electromagnetic compatibility
  - Links to environmental health and safety
  - Links to material sciences
  - Links to physical sciences
- Space vehicle
  - Assess IT&E schedule realism
  - Space system test engineering
    - Assess testability of space vehicle system, subsystems, and units
    - Assess the risk to the flight units/subsystem/system concept due to the stress of ground testing
    - Assess IT&E schedule realism
    - Assess contractor certification test strategy
    - Assess contractor development test strategy
    - Assess space vehicle internal and external interface verification/validation strategy (e.g., space to ground)
    - Assess space system integration strategy
    - Assembly and integration evaluation

Assess plan for acquisition and certification of ground support and special test equipment
Long lead planning and procurement
Assess test results from technology demonstrations
Assess support from specialty engineering
Links to engineering disciplines
Links to contamination control
Links to electromagnetic compatibility
Links to environmental health and safety
Links to material sciences
Links to physical sciences
Assure support from IT&E MA disciplines
Link to system safety
Link to reliability engineering
Link to risk management
Link to parts, materials, and processes
Link to configuration and data management
Link to quality assurance

Preliminary Design (Phase B)

Program planning
Assess program planning
Assess program executability
Assess SPO compliance to MAG verification tenets
Review post award contract
Assess program T&E roles and responsibilities

- Assess test data access and management adequacy
- Assure SPO access to contractor facilities and data
- Evaluate development and test facility needs
- Assess tailored test requirements and standards on contract

Assess D&OTE certification requirements
Assess verification tailoring and planning
Assess Phase C RFP
- Assess tailored MA specification and standards for testing

Phase C contractor proposal evaluation
- Evaluate contractor test strategy compliance to tailored MA specs/standards

Verify readiness for KDP C

Systems engineering

Assess systems engineering processes and products

Assess IT&E schedule realism
Assess verification requirements and planning
- Assess risk and impact of MA/test requirement tailoring
- Assess TEMP and system verification test plan
- Assure operational concepts and requirements margin suitability
- Assess need for simulations, models, and test-beds
- Assess accelerated life test program
- Evaluate COTS and heritage hardware test requirements
- Evaluate COTS and heritage software test requirements
- Evaluate integrated verification planning
  - Evaluate preliminary segment integration planning
  - Evaluate space vehicle system integration planning.

- Evaluate GSE integration planning for the test support, handling, calibration, transportation, and protection equipment
  - Evaluate pre-integration build up and assembly sequence
  - Evaluate module integration planning
  - Evaluate bus module subsystems integration planning
    - Evaluate guidance, navigation and pointing subsystem integration planning
    - Evaluate structures and mechanisms subsystem integration planning
    - Evaluate electrical power distribution subsystem integration planning
    - Evaluate communications subsystem integration planning
    - Evaluate thermal control subsystem integration planning
    - Evaluate flight software/data subsystem integration planning evaluation
    - Evaluate command and data handling subsystem integration planning
    - Evaluate command, control and telemetry subsystem integration planning
    - Evaluate propulsion subsystem integration planning
  - Evaluate preliminary SoS integration planning
  - Evaluate system integration planning
- Assure verifiability of TPMs

Assess verification management process

- Assess service life requirements flow-down
  - Test requirements allocation
- Evaluate executed test plans and test results
- Assess test like you fly deviations

Assess the adequacy of T&E IPT

Assess technology development strategy

Evaluate ground control and on-orbit test perceptiveness

- Assess factory to factory test requirements/planning for completeness

- Assure support from IT&E MA disciplines
  - Link to risk management
  - Link to configuration and data management
  - Link to reliability engineering
  - Link to quality assurance
  - Link to parts, materials and processes
  - Link to system safety
- Assure support from IT&E specialty engineering disciplines
  - Links to engineering disciplines
  - Links to physical sciences
  - Links to material sciences
  - Links to environmental health and safety
  - Links to electromagnetic compatibility
  - Links to contamination control
- Capture Lessons Learned

System

- Evaluate GFE verification criteria and responsibilities
- Assess adequacy of GFE repair and retest criteria
- Space segment
  - Assess segment to segment verification/validation strategy
    - Space to ground
    - Space to launch
  - Space vehicle
    - Evaluate the space vehicle system test program
      - Assess space vehicle test conditions
      - Evaluate test risks

- Evaluate suitability of ground and orbital tests
- Evaluate the “environmental test thoroughness index”
- Evaluate informal test data
- Assess space to ground interface validation strategy

Evaluate I&T schedule as a “gated” process

Space vehicle system preliminary design

- Evaluate space vehicle module and subsystem testing
  - Evaluate subsystem testing
- Evaluate bus subsystems test planning
  - Thermal control (TC)
    - Evaluate the contractor’s conduct of thermal control subsystem testing
    - Evaluate the contractor’s conduct of unit testing
  - EPDS
    - Evaluate contractor’s conduct of EPDS subsystem testing
    - Evaluate contractor’s conduct of EPDS unit testing
  - Propulsion and ordnance
    - Evaluate the contractor’s conduct of propulsion subsystem testing
    - Evaluate the contractor’s conduct of unit testing
  - Structures and mechanisms
    - Evaluate the contractor’s conduct of structures and mechanisms testing
  - Communications subsystem (CS)
    - Evaluate the contractor’s conduct of CS testing
    - Evaluate the contractor's conduct of unit testing
  - GN&C
    - Evaluate the contractor’s conduct of GN&C testing
    - Evaluate the contractor’s conduct of unit testing

- Data management
  - Evaluate the contractor’s validation of flight data
- Software
  - Evaluate flight software/data subsystem verification/validation
    - Evaluate the contractor’s conduct of subsystem testing
    - Evaluate the contractor’s conduct of CI (unit-level) testing
- CC&T subsystem
  - Evaluate the contractor’s CC&T testing
  - Evaluate the contractor's conduct of unit testing

Payload

- Evaluate mission payload(s) integration planning
  - Evaluate payload integration to bus
- Evaluate mission payload(s) module integration and test planning
- Evaluate mission payload(s) subsystem integration and test planning
- Evaluate the contractor’s conduct of mission payload testing
  - Evaluate the contractor’s conduct of mission payload subsystem testing
  - Evaluate the contractor’s conduct of mission payload unit testing

GSE

- Evaluate adequacy of automated testing
- Evaluate space system GSE
  - Verify GSE final design
  - Assess GSE for the test environments
  - Assess GSE IV&V planning
  - Evaluate GSE development schedule
  - Evaluate GSE sparing plan
- Evaluate mission payload module subsystem GSE test planning

Complete Design (Phase C)

- Program planning
  - Assess program planning
    - Verify readiness for build/production decision
    - Assess program executability
      - Assess SPO compliance to MAG verification tenets
      - Assess program T&E roles and responsibilities
      - Assure SPO access to contractor facilities and data
      - Assess test data access and management adequacy
      - Evaluate program specific tailoring of design verification and test standards
    - Review post-award contract
    - Assess D&OTE certification requirements
    - Assess follow-on Phase D (if applicable) RFP
      - Evaluate the contractor's strategy to comply with tailored MA specs/standards
- Systems engineering
  - Assess systems engineering processes and products
    - Assess verification requirements and planning
      - Assure operational concepts and requirements margin suitability
      - Evaluate integration verification planning
        - Assure interface control plan is integrated with IT&E plan
      - Assess TEMP and system verification test plan
      - Evaluate SoS test planning
      - Assess completeness of verification cross reference matrix
        - Assure use of test as the preferred verification method
        - Assure proper use of simulation and analysis

- Assess verification management process
  - Assure verifiability of TPMs
  - Assure system requirements are verified at the system level
  - Assess test like you fly deviations
  - Ensure adequacy of sell-off package test data
    - Evaluate executed test plans and test results
  - Assess the risk and impact of test requirement tailoring
- Assess IT&E schedule realism
- Assess the effectiveness of T&E IPT
- Assure supporting IT&E MA engineering disciplines
  - Link to system safety
  - Link to quality assurance
  - Link to configuration and data management
  - Link to risk management
  - Link to reliability engineering
  - Link to parts, materials, and processes
- Assure support from IT&E specialty engineering disciplines
  - Links to engineering disciplines
  - Links to physical sciences
  - Links to material sciences
  - Links to environmental health and safety
  - Links to electromagnetic compatibility
  - Links to contamination control
- Capture Lessons Learned

System

- Evaluate GFE verification criteria and responsibilities

- Assess adequacy of GFE repair and retest criteria
- Assess factory to factory test requirements/planning for completeness
- Space segment
  - Assess segment to segment interface verification/validate planning
    - Space to ground
    - Space to launch
  - Evaluate STE integration and verification planning
  - Assure end-to-end space segment integration verification
  - Evaluate thoroughness and perceptivity of testing to verify/validate internal and external interfaces
  - Space vehicle
    - Assure SPO approved tailoring of qualification and acceptance plan
    - Evaluate I&T schedule as a “gated” process
    - Evaluate suitability of ground and on-orbit tests
    - Evaluate the space vehicle system test program
      - Evaluate “environmental test thoroughness”
      - Assess performance test thoroughness
      - Evaluate efficiency of space vehicle integration plan
        - Evaluate final system integration planning
        - Evaluate space vehicle integration planning
      - Evaluate space vehicle system test risks
        - Evaluate pre-integration build up and assembly sequence
      - Evaluate informal test data
      - Evaluate space vehicle subsystem test planning
      - Evaluate module integration planning
      - Evaluate space vehicle module testing
      - Evaluate bus to payload interface verification planning

- Evaluate space vehicle to ground interface verification planning
- Evaluate space vehicle module testing for thoroughness and perceptivity
- Evaluate space vehicle bus testing for thoroughness and perceptivity
  - Thermal control
    - Evaluate thermal control subsystem integration planning
    - Evaluate thermal control subsystem test requirements and planning
  - Electrical power and distribution
    - Evaluate electrical power distribution subsystem integration planning
    - Evaluate electrical power distribution subsystem test requirements and planning
    - Electrical power distribution subsystem test execution and results
      - Evaluate the contractor's conduct of subsystem testing
      - Evaluate the contractor's conduct of unit testing
      - Evaluate pretest review data
      - Evaluate post-test data
  - Propulsion and ordnance
    - Evaluate propulsion subsystem integration planning
    - Evaluate propulsion subsystem test requirements and planning
    - Evaluate propulsion subsystem test execution and results
      - Evaluate the contractor's conduct of subsystem testing
      - Evaluate the contractor's conduct of unit testing
      - Evaluate pretest review data
      - Evaluate post-test data
  - Structures and mechanisms
    - Evaluate structures and mechanisms subsystem integration planning
    - Evaluate structures and mechanisms subsystem test requirements and planning
  - GN&C

- Evaluate GN&C test requirements and planning
- Evaluate guidance, navigation and pointing subsystem integration planning
- Evaluate guidance, navigation and pointing subsystem test planning
    - Evaluate GN&C GSE test plans

Data management

- Evaluate command and data handling subsystem integration planning
- Evaluate command and data handling test requirements and planning

Software

- Evaluate flight software/data subsystem integration planning
- Evaluate flight software/data subsystem test, test requirements and planning
- Evaluate flight software/data subsystem test execution and results
    - Evaluate the contractor's conduct of subsystem testing
    - Evaluate the contractor's conduct of CI (unit-level) testing
    - Evaluate pretest review data
    - Evaluate post-test data

TT&C

- Evaluate command, control and telemetry subsystem integration planning
- Evaluate command, control and telemetry subsystem test requirements and planning

Communications

- Evaluate communications subsystem integration planning
- Evaluate communications subsystem test, test requirements and planning

Internal and external interfaces

- Evaluate internal interface verification/validation test planning
- Evaluate external interface verification/validation test planning
- Evaluate pretest review data

- Evaluate post-test review data
- Evaluate SV payload(s) testing for thoroughness and perceptivity
  - Evaluate mission payload(s) module integration and test planning
    - Evaluate mission payload(s) module integration planning
    - Evaluate mission payload module subsystem test planning
  - Evaluate mission payload(s) module and subsystem testing
    - Evaluate mission payload(s) module integrated testing
    - Evaluate mission payload module subsystem testing
    - Evaluate mission payload(s) internal and external interface verification/ validation test planning
    - Evaluate pretest review data
    - Evaluate post-test data
- GSE
  - Evaluate space system GSE
    - Evaluate GSE integration planning
    - Assess GSE IV&V planning
    - Verify GSE final design
    - Assess GSE for the test environments
  - Evaluate adequacy of automated testing
    - Evaluate GSE development schedule
    - Evaluate GSE sparing plan

Fabrication and Integration (Phase D1)

- Program planning
  - Assess program planning
    - Assess program executability

- Assess SPO compliance to MAG verification tenets
- Assess test data access and management adequacy
- Assure SPO access to contractor facilities and data
- Assess program T&E roles and responsibilities
- Review post-award contract
- Assess test data access and management adequacy

Systems engineering

- Assess systems engineering processes and products
  - Assess IT&E schedule adequacy
  - Evaluate verification requirements and planning
    - Assure system-level verification of operational test and evaluation requirements
    - Evaluate TEMP and system verification test plan
    - Assess flowdown and linkage from system verification plan to test plans and procedures
    - Assess launch vehicle/space vehicle integrated test plans
    - Review assembly, test and checkout procedures
  - Evaluate verification management process
    - Assure system requirements are verified at the system level
    - Assess TLYF deviations
    - Verify sell-off package test data
      - Evaluate executed test plans and test results
  - Assess test risk items
  - Assure supporting MA disciplines
    - Link to system safety
    - Link to reliability engineering
    - Link to risk management
    - Link to parts, materials, and processes

- Link to configuration and data management
- Link to quality assurance
- Assure other supporting specialty engineering
  - Links to contamination control
  - Links to electromagnetic compatibility
  - Links to environmental health and safety
  - Links to material sciences
  - Links to physical sciences
  - Links to engineering disciplines
- Capture Lessons Learned

System
- Space segment
  - Space vehicle
    - Space vehicle system test
      - Evaluate space vehicle external interface testing
      - Evaluate space vehicle module/subsystem certification testing
      - Evaluate space vehicle system-level testing
        - Evaluate system dynamics test
        - Evaluate BIST
          - Evaluate pretest review data
          - Evaluate conduct of the test
          - Evaluate post-test data
          - Evaluate buy-off/sell-off packages
          - Evaluate informal testing conduct and results
          - Conduct informal testing for diagnostics
        - Evaluate system EMI/EMC test

- Evaluate system thermal vacuum test
- Evaluate FIST
  - Evaluate pretest review data
  - Evaluate conduct of the test
  - Evaluate post-test data
  - Evaluate buy-off/sell-off packages
  - Evaluate informal testing conduct and results
  - Conduct informal testing for diagnostics
- Evaluate IST
  - Evaluate pretest review data
  - Evaluate conduct of the test
  - Evaluate post-test data
  - Evaluate buy-off/sell-off packages
  - Evaluate informal testing conduct and results
  - Evaluate informal testing conduct and results
  - Conduct informal testing for diagnostics
  - Conduct informal testing for diagnostics
- Evaluate factory confidence/pre-ship test
  - Evaluate pretest review data
  - Evaluate conduct of the test
  - Evaluate post-test data
  - Evaluate buy-off/sell-off packages
- Evaluate certification testing
  - Evaluate pretest review data
  - Evaluate conduct of the test
  - Evaluate post-test data

- Evaluate buy-off/sell-off packages
- Evaluate informal testing conduct and results
- Conduct informal testing for diagnostics

Track and assess mass properties data
Assure disciplined test configuration control plan

Space vehicle bus

Evaluate spacecraft bus module integration planning
Assess hardware and software pedigree review data to identify discrepant items that may affect test results
Evaluate spacecraft bus module testing
Space vehicle subsystems

Thermal control

- Evaluate thermal control subsystem integration planning
- Evaluate thermal control subsystem test requirements and planning
- Evaluate thermal control subsystem test execution and results
  - Evaluate the contractor's conduct of subsystem testing
  - Evaluate the contractor's conduct of unit testing
  - Evaluate pretest review data
  - Evaluate post-test data

Electrical power and distribution

- Evaluate electrical power and distribution subsystem integration planning
- Evaluate electrical power and distribution subsystem test requirements and planning
- Electrical power distribution subsystem test execution and results
  - Evaluate the contractor's conduct of subsystem testing
  - Evaluate the contractor's conduct of unit testing

- Evaluate pretest review data
- Evaluate post-test data

Propulsion and ordnance

- Evaluate propulsion subsystem integration planning
- Evaluate propulsion subsystem test requirements and planning
- Evaluate propulsion subsystem test execution and results
  - Evaluate the contractor's conduct of subsystem testing
  - Evaluate the contractor's conduct of unit testing
  - Evaluate pretest review data
  - Evaluate post-test data

Structures and mechanisms

- Evaluate structures and mechanisms subsystem integration planning
- Evaluate structures and mechanisms subsystem test requirements and planning
- Evaluate structures and mechanisms subsystem test execution and results
  - Evaluate the contractor's conduct of subsystem testing
  - Evaluate the contractor's conduct of unit testing
  - Evaluate pretest review data
  - Evaluate post-test data

GN&C

- Evaluate GN&C subsystem integration planning
- Evaluate GN&C test requirements and planning
- Evaluate GN&C subsystem test execution and results
  - Evaluate the contractor's conduct of subsystem testing
  - Evaluate the contractor's conduct of unit testing
  - Evaluate pretest review data

- Evaluate post-test data
- Data management
  - Evaluate command and data handling subsystem integration planning
  - Evaluate command and data handling subsystem test requirements and planning
  - Evaluate data management subsystem test execution and results
    - Evaluate the contractor's conduct of subsystem testing
    - Evaluate the contractor's conduct of unit testing
    - Evaluate pretest review data
    - Evaluate post-test data
- Software
  - Evaluate flight software/data subsystem integration planning
  - Evaluate flight software/data subsystem test planning evaluation
  - Evaluate flight software/data subsystem test execution and results
    - Evaluate the contractor's conduct of subsystem testing
    - Evaluate the contractor's conduct of CI (unit-level) testing
    - Evaluate pretest review data
    - Evaluate post-test data
- TT&C
  - Evaluate TT&C subsystem test requirements and planning
  - Evaluate TT&C subsystem integration planning
  - Evaluate TT&C subsystem test execution and results
    - Evaluate the contractor's conduct of subsystem testing
    - Evaluate pretest review data
    - Evaluate post-test data
    - Evaluate the contractor's conduct of unit testing

- Communications
  - Evaluate communications subsystem test requirements and planning
  - Evaluate communications subsystem integration planning
  - Communications subsystem test execution and results
    - Evaluate the contractor's conduct of subsystem testing
    - Evaluate the contractor's conduct of unit testing
    - Evaluate pretest review data
    - Evaluate post-test data
- Space vehicle payloads
  - Assess hardware and software pedigree review data to identify discrepant items that may affect test results
  - Evaluate space vehicle payload module testing
    - Evaluate pretest data
    - Evaluate buy-off/sell-off packages
    - Evaluate post-test data
    - Evaluate informal testing conduct and results
    - Evaluate the conduct of informal testing for diagnostics
- Evaluate mission payload(s) module and subsystem testing
  - Evaluate mission payload(s) module integrated test conduct
    - Evaluate post-test data
    - Evaluate buy-off/sell-off packages
    - Evaluate informal testing conduct and results
    - Conduct informal testing for diagnostics
  - Evaluate mission payload module subsystem testing
    - Evaluate pretest review data
    - Evaluate the contractor's conduct of subsystem testing

Evaluate post-test data
Evaluate buy-off/sell-off packages
Evaluate informal testing conduct and results
Conduct informal testing for diagnostics

Provide APR

Fielding and Checkout (Phase D2)

Program planning

Assess program planning

Review post-award contract

Evaluate periodic operational space vehicle performance checks
Evaluate the conduct and results of the space vehicle performance testing

Assure SPO access to contractor facilities and data
Assess test data access and management adequacy

Systems engineering

Assess systems engineering processes and products

Verify compliance with contractor test plans and procedures

Segment to segment system testing
Pathfinder and first article testing
Ground support special test equipment, and processing facility capability

Evaluate pretest review data
Assess test risks
Evaluate post-test data
Evaluate informal testing conduct and results
Verify orbital sell-off report
Assess launch base DT&E verification

- Conduct informal testing for diagnostics
- TLYF deviations and assessment
- Assess O&M schedule
- Assure support from MA disciplines
  - Link to risk management
  - Link to configuration and data management
  - Link to reliability engineering
  - Link to quality assurance
  - Link to parts, materials, and processes
  - Link to system safety
- Assure support from IT&E specialty engineering disciplines
  - Links to electromagnetic compatibility
  - Links to environmental health and safety
  - Links to material sciences
  - Links to physical sciences
  - Links to engineering disciplines

System

- Space segment
  - Evaluate launch base inter-segment checkout results
    - Evaluate pretest review data
    - Evaluate conduct of the test
    - Evaluate post-test data
    - Evaluate test packages
    - Evaluate informal testing conduct and results
    - Conduct informal testing for diagnostics
  - Deployment test and checkout

- Space segment and SoS testing
  - Evaluate on-orbit space vehicle segment testing
    - Evaluate pretest review data
    - Evaluate the conduct of the test
    - Evaluate post-test data
    - Evaluate buy-off/sell-off packages
    - Evaluate informal testing conduct and results
    - Conduct informal testing for diagnostics
  - Evaluate on-orbit space vehicle inter-segment testing
    - Evaluate pretest review data
    - Evaluate conduct of the test
    - Evaluate post-test data
    - Evaluate buy-off/sell-off packages
    - Evaluate informal testing conduct and results
    - Conduct informal testing for diagnostics
  - Evaluate OT&E phase
    - Evaluate pretest review data
    - Evaluate conduct of the test
    - Evaluate post-test data
    - Evaluate buy-off/sell-off packages
    - Evaluate informal testing conduct and results
    - Conduct informal testing for diagnostics
- Space segment testing at initialization
  - Evaluate space vehicle subsystem calibration/performance
    - Evaluate pretest review data
    - Evaluate the conduct of the test

Evaluate post-test data
Evaluate test packages
Evaluate informal testing conduct and results
Conduct informal testing for diagnostics
Evaluate spacecraft anomalies

Operations and Disposal (Phase D3)

Program planning
Evaluate contractor proposal for Phase D
Evaluate mission specific post-flight/de-orbit evaluation plan
Systems engineering
Assess systems engineering processes and products
Assess OT&E verification (SMC only)
Assess periodic mission performance testing
Assess periodic space vehicle subsystem calibration results
Evaluate system baseline changes impacting performance
Assure support to MA specialty engineering
Link to risk management
Link to configuration and data management
Link to reliability engineering
Link to quality assurance
Link to parts, materials, and processes
Link to system safety
Assure support from specialty engineering
Links to contamination control
Links to electromagnetic compatibility

- Links to environmental health and safety
- Links to material sciences
- Links to physical sciences
- Links to engineering disciplines
- Provide Lessons Learned

System

- Space segment
  - Evaluate conduct of mission operations to assess mission effectiveness
  - Evaluate mission and system impact of software and data baseline changes
  - Evaluate conduct and results of periodic end-to-end mission performance testing
  - Evaluate conduct and results of periodic space vehicle subsystem calibration testing
  - Evaluate causes and corrective actions for space vehicle anomalies
    - Evaluate mission impacts from payload anomalies and work arounds
    - Evaluate mission impacts from bus anomalies and work arounds
  - Evaluate disposal strategies, plans and procedures for executability
  - Assess execution of disposal actions
- Provide Lessons Learned

Appendix A3-5
Operational Readiness Assurance

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Pre-KDP A Concept Studies (Phase 0)
- Program planning
  - Assess program planning
    - Verify adequacy of Phase A RFP
      - Asses compliance documents
      - Assess TRD
      - Assure SOO-SOW/CDRL
        - Verify adequacy of refinement of concept in RFP
- Systems engineering
  - Assess system engineering processes and products
    - Assess operations related system engineering products
      - Pre-milestone A operational assurance

Concept Development (Phase A)
- Program planning
  - Assess program planning
    - Assess program executability
      - Assure Phase A negotiated contract maintained operational readiness assurance integrity
      - Assess Phase A operations program baseline

- Verify adequacy of follow-on RFP
  - Assess compliance documents
  - Assess TRD
  - Assure SOO-SOW/CDRL
- Participate in multi-mission working group and develop launch options

Systems engineering

- Assess operations related engineering processes and products
  - Assess operational system design
    - Assess the system operational suitability and effectiveness
    - Assure operational supportability
    - Assess operational requirements allocations
  - Capture Lessons Learned

System

- Space segment
  - Assess space segment operations concept
    - Assess space segment operational plans and processes
    - Assess space segment operational suitability
    - Assess space segment operational supportability
- Launch segment
  - Assess launch segment operational concept
    - Assess launch segment operational plans and processes effectiveness
    - Assess launch segment operational suitability
    - Assess launch segment operational supportability
- Ground segment
  - Assess ground segment operational concept

Assess ground segment operational plans and processes
Assess ground segment operational suitability
Assess ground segment operational supportability

Preliminary Design (Phase B)

Program planning
Assess program planning
Assess program executability
Assure Phase B contract maintained operational readiness assurance integrity
Assess Phase B operations program baseline
Verify adequacy of follow-on RFP
Assess compliance documents
Assess TRD
Assure SOO-SOW/CDRL

Systems engineering
Assess operations-related engineering processes and products
Assess preliminary operational concepts and plans
Assess system operational suitability and effectiveness
Assure operational supportability
Assure operational requirements and allocation
Capture Lessons Learned

System
Assess ground segment operational requirements and preliminary plans
Assess ground control operational requirements and preliminary plans
Assess ground control preliminary operational plans

- Assess ground control operational suitability
- Assess ground control operational supportability
- Assess mission processing operational requirements and preliminary plans
  - Assess mission processing preliminary operational plans
  - Assess mission processing operational suitability
  - Assess mission processing operational supportability

Assess segment operations

Space segment

- Assess space segment operational requirements and preliminary plans
  - Assess space segment operational safety
  - Assess operational supportability
  - Assess space segment launch site activation plans
- Space vehicle
  - Assess space vehicle preliminary operational plans and processes
    - Assess space vehicle operations
    - Assess space vehicle preliminary operational planning for suitability
    - Assess ground and inflight diagnostic capability

Launch segment

- Assess launch segment operational requirements and preliminary plans
  - Assess suitability of preliminary launch segment operational planning
  - Assess launch vehicle preliminary operational plans and processes
    - Assess launch vehicle operations
    - Assess preliminary launch vehicle operational planning
    - Assess diagnostic capability
  - Assess launch segment operational safety

Assess launch segment operational supportability
Assess launch segment launch site activation plans

Complete Design (Phase C)

Program planning
Assess program planning
Assess program executability
Assure Phase C contract maintained operational readiness assurance integrity
Assess Phase C operations program baseline
Verify adequacy of follow-on RFP
Assess compliance documents
Assess TRD
Assure SOO-SOW/CDRL

Systems engineering
Assess operations related system engineering products and processes
Assess updated operational concepts and plans
Assess system operational suitability and effectiveness
Assure operational supportability
Assure operational requirements and allocation
Mission targeting validation
Mission constraints compliance validation
Assure other specialty engineering disciplines
EMC design
Mass property control
Assess information assurance plans

- Assess human/machine interface standards and plans
- Assess environmental health and safety plans
- Environmental analyses
- Logistics
- Survivability

Assure supporting MA disciplines

- Software assurance
- System safety assurance
- Quality assurance
- Risk assessment and management
- Reliability engineering
- Configuration management
- Parts, materials, and processes

Capture Lessons Learned

System

Assess segment operational requirements and plans

Space segment

Assess space segment operational requirements and final plans

- Assess space segment operational safety
  - Range safety verification
- Assess space segment operational supportability
- Assess space segment site activation planning

Space vehicle

- Assess space vehicle final operational plans and processes
  - Assess space vehicle operational suitability

- Assess space vehicle final operational planning for suitability
- Assess ground and inflight diagnostic capability

Launch segment

- Assess launch segment operational requirements and final plans
  - Assess suitability of final launch segment operational planning
  - Assess launch vehicle final operational plans and processes
    - Assess final launch vehicle operational planning
    - Assess diagnostic capability
    - Assess launch vehicle operational suitability
  - Assess launch segment operational safety
    - Range safety verification
    - Controllability and placard design evaluation
  - Assess launch segment operational supportability
  - Assess launch site activation plans

Ground segment

- Assess ground segment operational requirements and final plans
  - Assess ground control operational requirements and final plans
    - Assess ground control final operational plans
    - Assess ground control operational supportability
    - Assess ground control operational suitability
    - Assess site activation planning
  - Assess mission processing operational requirements and final plans
    - Assess mission processing site activation planning
    - Assess mission processing operational supportability
    - Assess mission processing final operational plans

Assess mission processing operational suitability

Fabrication and Integration (Phase D1)

Program planning

Assess program planning

Assess program executability

Assure Phase D contract has maintained operational readiness assurance integrity

Assess Phase D operations program baseline

Systems engineering

Assess operational systems engineering processes and products

Assess updated operational requirements and allocation

Assess updated operational concepts and plans

Assure supporting MA disciplines

Risk assessment and management

Reliability engineering

Configuration management

Parts, materials, and processes

Quality assurance

System safety assurance

Software assurance

Assure other specialty engineering disciplines

EMC design

Mass property control

Contamination control

Assess information assurance plans

- Assess human/machine interface standards and plans
- Assess environmental health and safety plans
- Environmental analyses
- Logistics
- Survivability
- Capture Lessons Learned

System
- Assess segment readiness to support the mission
- Space segment
  - Assess space segment operational readiness
    - Assess training program and material
    - Assess operational safety
    - Assess launch site activation readiness
  - Space vehicle
    - Verify space vehicle operational plans and procedures
    - Assure manufactured space vehicle operational readiness
    - Assess space vehicle updated operation requirements
- Launch segment
  - Assess launch segment operational readiness
    - Assure manufactured launch vehicle operational readiness
      - Assess launch vehicle updated operational requirement, plans, and procedures
    - Verify launch segment operational planning and procedures
    - Assess training program and material
    - Assess launch segment operational safety
    - Assess launch site activation readiness

- Ground segment
  - Assess ground segment operational readiness
    - Assess ground control system operational readiness
      - Assess site activation plan
      - Assess training program and material
      - Assure manufactured ground control system operational readiness
      - Assess ground control updated operational requirement, plans, and procedures
    - Assess mission processing system operational readiness
      - Assess site activation plan
      - Assess training program and material
      - Assure manufactured mission processing system operational readiness
      - Assess mission processing updated operational requirement, plans, and procedures

Fielding and Checkout (Phase D2)

- Systems engineering
  - Assess operational readiness systems engineering products and processes
    - Assess updated operational concepts and plans
    - Assess updated operational requirements and allocation
    - Participate in launch rehearsal planning and execution
    - Assure supporting MA disciplines
      - Risk assessment and management
      - Reliability engineering
      - Configuration management
      - Parts, materials, and processes
      - Quality assurance

- System safety assurance
- Software assurance
- Assure other specialty engineering disciplines
  - EMC design
  - Mass property control
  - Contamination control
  - Assess information assurance plans
  - Assess human/machine interface standards and plans
  - Assess environmental health and safety plans
  - Environmental analyses
  - Logistics
  - Survivability

- System
  - Assure segment operational readiness processes
  - Space segment
    - Assure space system operational readiness planning
    - Space vehicle
      - Assure space vehicle integrity and readiness
        - Launch site mass properties support (example)
        - Assure on-orbit mission operations readiness
      - Spacecraft
        - Spacecraft subsystems
          - FSW operations readiness assurance
          - Support ordnance anomaly investigation (example)
          - Launch support operations—satellite propulsion (example)

- Thermal control
  - Thermal hardware site verification (example)
- Electrical power and distribution
  - Power system readiness (example)

GSE
- Assure readiness of GSE

Launch segment
- Assure launch vehicle segment operational readiness planning
- Day-of-launch loads analysis monitoring
  - Day-of-launch structural parameter monitoring
- Assure launch vehicle integrity and readiness
  - Power system readiness (example)
  - Assure launch vehicle operations
  - Day-of-launch monitoring of fluid and thermal parameter (example)
  - Mission readiness assessment—launch vehicle liquid propulsion (example)
  - Liquid engine performance analysis (example)
  - Launch support operations—liquid propulsion (example)
  - Anomaly investigation—ordnance
  - Day-of-launch GN&C analysis (example)
  - IMU calibration and alignment
- Assure readiness of GSE
- Independent day-of-launch loads analyses (placards)
- Day-of-launch monitoring of mechanisms
- Operations readiness assurance (example)
- Launch support operations

- Ground segment
  - Assure ground segment operational readiness planning
    - Assure ground control readiness
    - Assure mission processing readiness

Operations and Disposal (Phase D3)

- System
  - Assure space system operations
    - Assure on-orbit mission operations
      - On-orbit mass properties assessment (example)
      - Evaluate mission planning and on-orbit certification
      - Flight data analysis (example)
      - Disposal operations support (example)
      - Orbit transfer operations
  - Space segment
    - Assure space system operational readiness
      - Launch and on-orbit support operations (example)
      - Spacecraft launch and deployment support (example)
    - Space vehicle
      - Assure space vehicle integrity and readiness
      - Spacecraft
        - Spacecraft subsystems
          - Electrical power and distribution
            - Power systems operations (example)
          - Propulsion and ordnance

- Operations anomaly investigation (example)
- Anomaly investigation—ordnance
- On-orbit support operations—prop (example)
- Post-flight data analysis (example)

GN&C

- Launch and on-orbit support operations—ACS (example)
- Launch and on-orbit support operations—controls (example)
- On-orbit performance analysis and anomaly resolution

Software

- Support on-orbit FSW anomaly resolution (example)

GSE

- Assure readiness of GSE

Launch segment

- Assure launch vehicle system operations
  - Post-flight data analysis (example)
  - Post-flight analysis and anomaly resolution
  - Anomaly investigation support—environmental test (example)
  - Anomaly investigation—ordnance (example)
  - Launch vehicle launch support (example)
  - Post-flight reviews (example)
  - Post-flight data analysis (example)
  - Post-flight data review and assessment

Ground segment

- Assure ground segment operations
  - Assure ground control readiness

Assure mission processing readiness

Non-program specific

Systems engineering

Overflight risk assessment

Appendix A3-6
MA Reviews, Audits, and Lessons Learned

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Pre-KDP A Concept Studies (Phase 0)

- Program planning
  - KDP A review
  - Request for proposal
- Systems engineering
  - Concept decision meeting
  - Standards update
  - Lessons Learned

Concept Development (Phase A)

- Program planning
  - PMRs
  - KDP B review
- Systems engineering
  - Verify adequacy of technical reviews
    - Verify MM/PC
    - Verify IBR
    - Verify adequacy of system requirements incremental space flight worthiness review

Verify SDR
Verify SRR

Preliminary Design (Phase B)

Program planning
PMRs
Assure a design/verification review planning process is in place in the SPO
KDP C review
Systems engineering
Verify adequacy of technical reviews
Evaluate technical review entrance criteria
Verify adequacy of PDR
Space vehicle preliminary engineering designs
Launch vehicle preliminary engineering designs
Launch vehicle mass properties review (example)
Verify adequacy of audits
Evaluate audit entrance criteria
Space vehicle subsystems
Verify adequacy of PDAs

Complete Design (Phase C)

Program planning
PMRs
Assure a design/verification review planning process is in place in the SPO
Systems engineering

- Verify adequacy of CDR
  - Space vehicle critical engineering designs
  - Launch vehicle critical engineering designs
- Verify adequacy of technical reviews
  - Evaluate review/audit entrance criteria
  - Verify adequacy of system design and manufacturing readiness incremental space flight worthiness review
- Verify adequacy of audits
  - Verify adequacy of CDAs (see also CDA process task in design assurance)
  - Assure FCA

Fabrication and Integration (Phase D1)

- Program planning
  - PMRs
- Systems engineering
  - Verify adequacy of technical reviews
    - Assure HAR adequacy
    - Assure TRR
    - Verify FQR
    - Verify adequacy incremental SFW—SMC only
    - Assure PRR
  - Assure IRRT reviews
  - Verify adequacy of audits
    - Assure PCA
- WBS not assigned

- Assure government reviews

Fielding and Checkout (Phase D2)

- Systems engineering
  - Verify adequacy of technical reviews
    - Assure SVR
      - Space vehicle GN&C mission assurance review
      - Flight readiness assessments—solid propellant
  - Assure IRRT reviews
  - Aerospace readiness reviews
    - Conduct an Aerospace program readiness review
    - Conduct an Aerospace launch site readiness review
    - APR
  - Assure government reviews
    - Assure MRR
    - Assure FRR
    - Assure LRR

Operations and Disposal (Phase D3)

- Systems engineering
  - Assure PLR

Appendix A3-7
Risk Management

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Pre-KDP A Concept Studies (Phase 0)

- Assess and evaluate system-concept risk trade-offs
  - Identify top-level system-concept technological and acquisition risks
  - Identify system-concept risk mitigation strategies
  - Evaluate system-concepts in terms of key risk issues and mitigation strategies
- Generate Phase 0 RM Lessons Learned

Concept Development (Phase A)

- Develop Phase-A government program office RM plan
  - Review contractor Phase A RM plan
  - Identify and define key elements of government Phase A RM plan
- Define/validate Phase A program RM baseline
  - Identify Phase A program risk items
    - Review and validate identification of contractor-defined Phase A risk items
    - Review and validate identification of government-defined Phase A risk items
    - Verify and complete Phase-A risk item identification list and definitions
    - Participate in mission technical and management working groups
  - Assess Phase A program risk items

- Validate contractor assessment of Phase A risk items
- Assess government program office Phase A risk items
- Define handling plans and actions for Phase A program risks
- Validate contractor Phase A risk handling plans
- Define government program Phase A risk handling plans
- Monitor and verify execution of Phase A risk handling/risk reduction activities
- Generate Phase A RM Lessons Learned

Preliminary Design (Phase B)

- Update government RM plan into Phase B formulation
- Review contractor Phase B RM plan
- Review subcontractor Phase B RM plans
- Identify and define key elements of government Phase B RM plan
- Define and validate Phase B program RM baseline
- Update/transition Phase A risk baseline items
- Assess/verify completion status of Phase A risk handling plans
- Assess/verify completion status of contractor and subcontractor Phase A risk handling plans
- Assess/verify completion status of government Phase A risk handling plans
- Reassess residual Phase A risk items
- Update/validate assessment of residual Phase A contractor risk items
- Reassess government program office residual Phase A risk items
- Revalidate/adjust handling plans for residual Phase A risk items
- Revalidate contractor handling plans for residual Phase A risk items
- Update government program handling plans for residual Phase A risk items
- Incorporate new Phase B risk items into RM baseline

- Identify Phase B risk items
  - Review and validate identification of contractor-defined Phase B risk items
  - Review and validate identification of government-defined Phase B risk items
  - Verify and complete Phase B risk item identification list and definitions
- Assess newly identified Phase B risk items
  - Validate contractor assessment of Phase B risk items
  - Assess government program office Phase B risk items
- Define handling plans/actions for newly identified Phase B risk items
  - Validate contractor Phase B risk handling plans
  - Define government program Phase B risk handling plans
- Monitor and verify execution of Phase B risk handling/risk reduction activities
- Generate Phase B RM Lessons Learned

Complete Design (Phase C)

- Update RM plan into Phase C formulation
  - Review contractor Phase C RM plan
    - Review subcontractor Phase C RM plans
  - Identify and define key elements of government Phase C RM plan
- Define and validate Phase C program RM baseline
  - Update/transition Phase B risk baseline items
    - Assess/verify completion status of Phase B risk handling plans
      - Assess/verify completion status of contractor and subcontractor Phase B risk handling plans
      - Assess/verify completion status of government Phase B risk handling plans
    - Reassess residual Phase B risk items
      - Update/validate assessment of residual Phase B contractor risk items

- Reassess government program office residual Phase B risk items
- Revalidate/adjust handling plans for residual Phase B risk items
  - Revalidate contractor handling plans for residual Phase B risk items
  - Update government program handling plans for residual Phase B risk items
- Incorporate new Phase C risk items into RM baseline
  - Identify Phase C risk items
    - Review and validate identification of contractor-defined Phase C risk items
    - Review and validate identification of government-defined Phase C risk items
    - Verify and complete Phase C risk item identification list and definitions
  - Assess newly identified Phase C risk items
    - Validate contractor assessment of Phase C risk items
    - Assess government program office Phase C risk items
  - Define handling plans/actions for newly identified Phase C risk items
    - Validate contractor Phase C risk handling plans
    - Define government program Phase C risk handling plans
- Monitor and verify execution of Phase C risk handling/risk reduction activities

Generate Phase C RM Lessons Learned

Fabrication and Integration (Phase D1)

Update RM plan into Phase D formulation

- Review contractor Phase D RM plan
  - Review subcontractor Phase D RM plans
- Identify and define key elements of government Phase D RM plan

Define and validate Phase D1 (fabrication/coding, test and integration) program RM baseline

- Update/transition Phase C risk baseline items

- Assess/verify completion status of Phase C risk handling plans
  - Assess/verify completion status of contractor and subcontractor Phase C risk handling plans
  - Assess/verify completion status of government Phase C risk handling plans
- Reassess residual Phase C risk items
  - Update/validate assessment of residual Phase C contractor risk items
  - Reassess government program office residual Phase C risk items
- Revalidate/adjust handling plans for residual Phase C risk items
  - Revalidate contractor handling plans for residual Phase C risk items
  - Update government program handling plans for residual Phase C risk items

Incorporate fabrication/coding risk items into RM baseline

- Identify fabrication/coding risk items
  - Review and validate identification of contractor-defined fabrication/coding risk items
  - Review and validate identification of government-defined fabrication/coding risk items
  - Verify and complete fabrication/coding risk item identification list and definitions
- Assess newly identified fabrication/coding risk items
  - Validate contractor assessment of fabrication/coding risk items
  - Assess government program office fabrication/coding risk items
- Define handling plans/actions for newly identified fabrication/coding risk items
  - Validate contractor risk handling plans for fabrication/coding risk items
  - Define government program risk handling plans for fabrication/coding risk items

Incorporate test and integration risk items into RM baseline

- Identify test and integration risk items
  - Review and validate identification of contractor-defined test and integration risk items
  - Review and validate identification of government-defined test and integration risk items
  - Verify and complete test and integration risk item identification list and definitions

- Assess newly identified test and integration risk items
  - Validate contractor assessment of test and integration risk items
  - Assess government program office test and integration risk items
- Define handling plans/actions for newly identified test and integration risk items
  - Validate contractor risk handling plans for test and integration risk items
  - Define government program risk handling plans for test and integration risk items
- Monitor and verify execution of Phase D1 risk handling/risk reduction activities
- Generate Phase D1 RM Lessons Learned

Fielding and Checkout (Phase D2)

- Pre-launch risk resolution
  - Identify and assess residual mission risk
    - Verify handling and close-out status of all risks in Phase D1 RM baseline
      - Verify handling and close-out status of contractor and subcontractor Phase D1 risk items
      - Verify handling and close-out status of government Phase D1 risk items
    - Identify and assess any new Phase D2 risk items
      - Review and assess any new Phase D2 contractor risk items
      - Identify and assess any new Phase D2 government risk items
      - Assess risk items identified in Phase D2 MA reviews and audits
  - Mitigate/accept residual deployment/flight risk
- Generate Phase D2 RM Lessons Learned

Operations and Disposal (Phase D3)

- Identify and resolve operational risk items
  - Review operational data to identify potential risks
  - Assess identified operational risk items
  - Define mitigation plans/actions for identified operational risk items
- Compile and record operational lessons learned for continuing utilization

Appendix A3-8
Reliability Engineering

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Pre-KDP A Concept Studies (Phase 0)

- Reliability input to RFP
- Program reliability and availability requirements

Concept Development (Phase A)

- Assess negotiated contract reliability sections
- System reliability requirements
  - Subsystem reliability requirements
    - Unit reliability requirements
- Reliability management

Preliminary Design (Phase B)

- Preliminary system reliability/availability prediction
  - Preliminary subsystem reliability prediction
    - Preliminary unit reliability prediction
      - Preliminary worst-case and parts stress analysis
      - Preliminary parts reliability analysis
      - Preliminary accelerated life testing

Preliminary FMEA
Preliminary critical/limited life item control

Complete Design (Phase C)
Final system reliability prediction
Final subsystem reliability prediction
Final unit reliability prediction
Final worst-case and parts stress analysis
Final parts reliability analysis
Final accelerated life testing
Final FMEA
Final critical/limited life item control
Reliability management

Fabrication and Integration (Phase D1)
System anomaly resolution verification
Subsystem anomaly resolution verification
Subcontractor failures verification
Participate in contractors' failure analysis and corrective action boards
ESS verification

Fielding and Checkout (Phase D2)
Field anomaly resolution verification

Operations and Disposal (Phase D3)

Launch/on-orbit anomaly resolution verification

Non-Program Specific

Aerospace SSED database

Appendix A3-9
Configuration Management

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Pre-KDP A Concept Studies (Phase 0)
RFP CM input

Concept Development (Phase A)
Assess contractual implementation of CM
CM infrastructure

Preliminary Design (Phase B)
Added task
Configuration identification process

Complete Design (Phase C)
Configuration change control process
Configuration management implementation
Audit FCA process

Fabrication and Integration (Phase D1)
Configuration status accounting process

Audit PCA process

Fielding and Checkout (Phase D2)

Assure configuration control activities are implemented

Operations, maintenance, disposal

Assure configuration control activities are implemented

Non-program specific

Appendix A3-10
Parts, Materials, and Processes

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Pre-KDP A Concept Studies (Phase 0)

- PMP input to RFP or SOO
- Evaluate PMP sections in proposal or SOW

Concept Development (Phase A)

- PMP Input to SRD
- Document PM&P management requirements
  - PM&P control program plan
    - Evaluate GIDEP alerts and contractor bulletins for potential impact to flight hardware
  - PMPCB
- PM&P requirements input to SRD
  - PM&P control and assurance attributes definition
  - Subcontractor evaluation and flow-down of PMP requirements
  - PM&P system definition

Preliminary Design (Phase B)

- PMP management review
  - IPT meetings participation from PMP

- Update PMPCP plan
- Subcontractor's PM&P control tasks
- Evaluate preliminary design PM&P process
- PMPCB meetings

PM&P requirements in PM&P control plan

- PAPL
- PM&P derived requirements

Verify PM&P products

- PM&P derating implementation
- Producibility assessment of design/manufacturing engineering documents
- Material compatibility
- Material environmental evaluation
- Evaluate parts test plans

Complete Design (Phase C)

PM&P management evaluation

- PMPCB meetings
- Evaluate detailed design of PM&P process
- Subcontractors

Verify PM&P implementation

- PM&P validation of system-level SEE analysis
- PM&P validation of WCCA—stress derating
- Radiation and aging degradation limits
- Assessment of PM&P capabilities
- CES materials requirements verification

PM&P validation of WCCA—parameter EOL value
Outgassing requirements verification
Evaluate parts test plans

Fabrication and integration (Phase D1)
Failure analysis
Functional and product configuration audit
PM&P document update
Evaluate fabrication and integration PM&P process
Radiation lot acceptance testing

Fielding and Checkout (Phase D2)
PM&P anomaly resolution

Operations and Disposal (Phase D3)
Anomaly resolution

Non-program specific

Appendix A3-11
Quality Assurance

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Pre-KDP A Concept Studies (Phase 0)

- Review and evaluation of RFP
- Conduct pre-award surveys and fact finding

Concept Development (Phase A)

- Quality management system assessment
  - Quality plan assessment
  - Design and development process assessment
  - Quality risk mitigation
  - Facility capabilities review

Preliminary Design (Phase B)

- PDR
  - Assessment of purchasing function
  - Supplier control plan
  - Supplier surveys and/or facility reviews
  - Reporting of key quality metrics
- Specification flow-down process review

Review and evaluate draft SOW

Complete Design (Phase C)

CDR

- Stamp control process review
- Evaluation of contractor's production controls
- Workmanship standards assessment
- Personnel training
- Equipment and process controls
- Supplier assessment

MRR

Fabrication and Integration (Phase D1)

Manufacturing/assembly process audits
Drawing and change control audits
TRR
Material and test nonconformance controls

- Assess fleet-wide performance impacts of anomalous conditions with components and subsystems
- Corrective action process (via CAB)
- Corrective and preventive action plans
- Participate in component, subsystem, and system anomaly resolution and disposition

Production verification audits
Test and integration activities

Fielding and Checkout (Phase D2)

Launch site quality plan assessment

Operations and Disposal (Phase D3)

Launch anomaly or on-orbit failure analysis review

Appendix A3-12
System Safety Assurance

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Pre-KDP A Concept Studies (Phase 0)
- System safety input to RFP

Concept Development (Phase A)
- Assess negotiated contract system safety sections
- Verify compliance with system safety requirements
  - Assess system safety program integration with engineering
- Assess preliminary hazard list
  - Assess PHA

Preliminary Design (Phase B)
- Subsystem hazard analysis
- System hazard analysis
- Operating and support hazard analysis
- Health hazard assessment

Complete Design (Phase C)
- Safety assessment

Validate compliance with orbital debris mitigation requirements
Assess space vehicle waivers to EWR 127-1(T)
Assess TRD
Assess systems engineering processes and products
Assure adequacy of missile system pre-launch safety package (MSPSP)
Test and evaluation safety
Safety review of changes and deviations/waivers

Fabrication and Integration (Phase D1)

Safety verification
Safety compliance assessment
Explosive hazard classification and characteristics
Explosive ordnance disposal source data

Fielding and Checkout (Phase D2)

Review contractor system safety and health implementation to assure protection of government interests

Operations and Disposal (Phase D3)

Non-program specific

Appendix A3-13
Software Assurance

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2. Since several tasks within the software assurance list of tasks are applicable to more than one phase, and in order to conserve space, the tasks are not listed by phase. Software assurance tasks are listed once within this appendix, with each task's applicable phases noted in parentheses.

Assess software acquisition strategy (preparation for Phase A)
Assess government pre-KDP A plans, activities, and products (pre-KDP A)
Assess government software acquisition management approach (pre-KDP A)
Assess pre-KDP A contracts, software plans, activities, and products (pre-KDP A)
Assess government Phases B and C plans, activities, and products (preparation for Phases B and C)
Assess pre-contract award tasks for software MA (pre-KDP A)
- Assess government's software acquisition concept, cost, and schedule (pre-KDP A)
- Perform Phase B award supplier software risk assessment (preparation for Phase B)
- Ensure source selection guidance addresses software (preparation for Phase B)
- Assess supplier's software capability (preparation for Phase B)

Develop and/or assess government software MAP (preparation for Phase B)
Conduct independent analyses (any period of system acquisition life cycle as needed)
- Assess software development risks and propose risk mitigation (any period of system acquisition life cycle as needed)
- Perform software modeling and analysis (any period of system acquisition life cycle as needed)
- Perform technology maturity assessment (any period of system acquisition life cycle as needed)
- Perform independent verification and validation (preparation for Phase B; must start at earliest requirements analysis phase)

- Validate onboard* software mission constants (Phase D)
- Assess onboard software risk likelihood and consequence (Phase D)
- Assess onboard software qualification testing (Phase D)
- Validate resources required for onboard software integration and qualification testing (all phases)

Assess supplier software plans and processes (all phases)

- Assess software plans (all phases)
  - Assess software development plan (all phases)
  - Assess software test planning (all phases)
  - Assess installation and transition to operations planning (preparation for Phase D)
  - Assess transition to maintenance planning (preparation for Phase D)
- Assess software processes (source selection and contract monitoring for all phases)
  - Assess software management processes (source selection and contract monitoring for all phases)
  - Assess software requirements and design processes (source selection and contract monitoring for all phases)
  - Assess software implementation and test processes (source selection and contract monitoring for all phases)
  - Assess software support processes (source selection and contract monitoring for all phases)
- Assess performance of software development processes (period of process execution for each development increment)
  - Assess software management process performance (all phases)
  - Assess software requirements and design process performance (period of process execution for each development increment)
  - Assess implementation and test process performance (period of process execution for each development increment)
  - Assess software support process performance (all phases)

Assess supplier software development products (at product delivery in all phases)

* Onboard includes both the spacecraft (i.e., bus) and payload software.

Assess software management products (at product delivery in all phases)
Assess software requirements and design products (at product delivery in all phases)
Assess software implementation and test products (at product delivery in all phases)
Assess software support products (at product delivery in all phases)
Assess software test and installation activities (in all phases incorporating test and installation activities)

Appendix A4
List of Government Products for Assessment

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Pre KDP A Government Products

The following list, not all inclusive, of government products should be available for review before the KDP A milestone. The product review should provide insight into the software portion of the proposed acquisition effort, and aid in the understanding of the scope, use, and function of the software segment(s), and any related assumptions, constraints, and risks.

- Initial capability document
- Initial capability development document
- System-level CONOPS document
- DOD architecture framework views (OVs)
- Analysis of alternatives results
- Proof-of-concept studies/models results
- Software cost model estimates
- Integrated program summary (IPS)
- Technology readiness assessments
- Test and evaluation strategy

Pre KDP A Modeling and Analysis

The following is a partial list of potential modeling and analysis tasks, applicable to both ground and flight segments, that the program office may choose for the acquisition effort. The sample tasks listed can be undertaken to either help develop or to assess the government's proposed acquisition concept and costs to ensure that both adequately address software.

- Proof-of-concept studies/models
- Software cost model estimates
- Aerospace's Concept Design Center
- Technology readiness assessments

Phase B and C Government Products

The following is a partial list of government products that should be reviewed before the applicable, KDP B or -C milestone. The product review allows for the verification that government plans and products are continually being updated as needed, especially in the area of software, to provide the additional detail required to effectively begin the next acquisition phase. This list is to be tailored to reflect the acquisition needs of the JPO/SPO at a particular acquisition phase.

- Capabilities description document
- System-level CONOPS document
- DOD architecture framework views (OVs, TVs, and SVs)
- Government reference architecture
- Analysis of alternatives results
- Technology readiness assessments
- Technical requirements document
- IPS
- TEMP
- Capability production document
- Government cost and schedule baseline
- RFP
- SOW
- Contract

Appendix A5
Checklists for Assessing Supplier Software Processes and Products

NOTE: To conserve space, the following section does not include definitions along with the first mention of any given acronym. For acronym definitions, please refer to Appendix A2.

Process and product assessments need to be done by staff experienced in the pitfalls and risks of large scale software development in the domain of the contracted system. Assessment of supplier software development processes and products requires the use of an orderly, organized review approach, assessing against recognized process and/or product standards and best practices. The most comprehensive and complete method of process assessment is to conduct a SCAMPI^{SM} assessment [SEI01, SEI02, SEI05]. If that method is not used, processes should be informally assessed by experienced external reviewers at program initiation and regularly during execution of the program.

The process areas listed below do not map directly to those defined in the CMMI appraisal method; however, they do cover, for the most part, the CMMI process areas of concern. The checklists within each section below constitute recommended assessment activities, and are not all inclusive.

Checklists for Assessing Software Development Processes

This appendix addresses four major groupings of software development process areas: software management processes, software requirements and design processes, software implementation and test processes, and software support processes. Common to all four groupings are the following assessment activities:

- Verify that all the software development processes the supplier has defined and identified as being used in the program under assessment are implemented and are being used.

- Assess all software development processes in use to determine if they are disciplined, documented, and adequate to effectively accomplish required activities and complete required products.

- If the supplier has tailored company standard processes, verify that the tailoring is appropriate for the current program needs.

- Verify that the supplier has implemented documented robust and sound systems engineering and software systems engineering approaches and

processes to support the activities comprising the supplier's software development effort.

Software Management Processes

The quality and completeness of the supplier's planning for managing software development is critical to mission assurance since poor planning leads to poor software quality in addition to cost and schedule delays. Please refer to Table A5-1 for the checklist associated with assessing these processes.

An important component of the management plan is a robust metrics and TPM plan that will be effective in identifying deviation from the plan early, and provide information to base timely corrective action. Assuming the software development is a component of a larger acquisition, the program EVMS will apply to software also. A candidate EVMS standard that could be put on contract is ANSI/EIA standard 748 EVMS [GEI01].

Processes applicable to software management include:

- Configuration management
- Management reviews
- Measurement
- Process improvement
- Project planning
- Project tracking and control
- Quality assurance
- Quantitative project management
- Risk management
- Subcontractor management

Table A5-1, Software Management Process Assessment Checklist

- Verify the metrics and process for analysis of metrics are described (or referenced) in the supplier's SDP.
- Verify that the supplier's project planning process is documented and provides for planning changes and mid-course correction that result from the corrective action decisions.
- Verify that the supplier's data collection methods and timelines for metrics and TPMs provide insight into problems early enough to apply effective corrective action.
- Verify that the supplier's process improvement procedures are documented and collect meaningful process metrics, identify needed process changes, and require timely action to modify processes.
- Verify that the supplier's IMP and IMS have adequate detail and milestones for software components and that the supplier has a documented process for updating the IMP and IMS as need requires.
- Verify the WBS content is sufficient to provide adequate visibility for progress on software. (NOTE: Particular attention should be given to areas where software is an embedded component of a hardware component. Those software development tasks need to be identified and tracked.)
- If there are subcontractors developing software items, verify that both the supplier's and subcontractors' processes are both documented and adequate to effectively integrate subcontractor-developed software, collect effective metrics, identify accurate status, and apply corrective action. (NOTE: Particular attention should be given to prime contractor processes for assessment and verification of the adequacy of subcontractor software development processes.)
- Verify that supplier's software configuration management processes are both documented and adequate to manage large software items in multiple baselines and to control changes on multiple baselines.
- Verify there are documented supplier processes for configuration management and managing deliveries between multiple contractors, if applicable.

Software Requirements and Design Processes

The processes for building quality software start with analyses and trade studies, requirements analysis, software architecture, and software design. Sometimes preliminary demonstrations and/or prototypes are developed early on. Please refer to Table A5-2 for the checklist associated with assessing these processes.

Processes applicable to software requirements and design include

- Analyses and trade studies processes
  - Performance analysis
  - Resource allocation and utilization analysis
  - Trade studies

- Demonstration and prototype processes
- Requirements definition and management processes
  - System requirements definition
  - System requirements management
  - Software requirements definition
  - Software requirements management
- Operations concept development processes
- Architecture development processes
  - System architecture development
  - Software and computer hardware architecture development
- Design development processes
  - System design development
  - Software and computer hardware design development
- Specialty engineering processes
  - Information assurance
  - Safety
  - Dependability, reliability, maintainability, and availability
  - Human systems integration

Table A5-2, Software Requirements and Design Process Assessment Checklist

- Verify that the methods and tools chosen by the contractor, including any early demonstrations and/or prototypes, have proven effective when previously used by the contractor on developments of similar size and complexity.
  - If the methods and tools chosen have not been proven in actual use on similar programs by the supplier, verify that technology maturity levels were determined and factored into the program risk and related risk mitigation plans, and adequate cost and schedule reserves were allocated.
  - If technology maturity levels have not been determined, verify that there is a documented process in place to ensure the determination of technology maturity levels and associated risk, and to support the factoring of this risk into the appropriate plans, cost(s) and schedule(s).
- Verify that the development staff assigned to the program is trained and experienced with the methods and tools chosen.
- Verify that there are rigorous peer review processes defined, documented and in place in addition to more formal reviews, and that these processes define appropriate points of insertion of peer reviews.
- Verify that there is a process defined, documented and in place to control and keep current changes to requirements (including specialty engineering requirements), operations concepts, relevant plans, architecture, design, and data.
- Verify that a process is defined, documented and in place to ensure changes to requirements and operations concepts have been reflected in project plans, activities and work products.
- Verify that a process is defined, documented and in place to ensure traceability of requirements from customer to product to product component.

Software Implementation and Test Processes

Processes applicable to software implementation and test include:

- Validation processes
- Requirements validation
- Implementation processes
  - Coding
  - Unit test
- System and software development and test environment processes
  - Software development support processes
  - Software systems administration
  - Database administration
- Integration and test processes
  - Software-software integration and test
  - Software-hardware integration and test
  - COTS integration and test
  - Software qualification test
  - System/segment integration and test
  - System qualification test
- Verification processes
  - Requirements verification
  - Test environment verification
- Transition to operations processes
- Transition to maintenance processes

Please refer to Table A5-3 for the checklist associated with assessing these processes.

Table A5-3, Software Implementation and Test Process Assessment Checklist

- Verify that the supplier code development processes are disciplined, and follow documented programming practices, procedures, standards and conventions that are consistent with good industry standards and practices.
- Verify that there are documented coding standards, specific to each programming language in use.
- Verify that there are documented rigorous code peer review processes.
- Verify that the test processes are orderly, complete, and account for the complex, multi-level testing necessary on a large-scale development.
- Verify that the test processes fully verify completion of test processes at each level so the transition from one test level to the next is orderly, and readiness for the next test level can be confirmed.
- Verify early on the program timeline that the software acceptance processes are sufficiently detailed and are adequate for the government to accept the product.
- Verify that the transition processes (for both operations and maintenance) are sufficiently detailed and are adequate to enable the government to approve the transition.
- Verify that the government roles and procedures in the acceptance process are detailed, clear, and understood by both the government and the supplier.

Software Support Processes

Software support activities provide needed services to the other development activities, and are important for successful software development. Please refer to Table A5-4 for the checklist associated with assessing these processes.

Processes applicable to software support processes include:

- Software configuration management and charge control
- Decision analysis and resolution
- Software quality assurance
- Corrective action
- Infrastructure administration
- Infrastructure development and maintenance
- Training processes
  - Management training
  - Development training
  - Maintenance training
  - Operations training

Table A5-4, Software Support Process Assessment Checklist

- Verify that the software configuration management processes are being implemented in accordance with the software configuration management plan, including the operation of the software configuration control board.
- Ensure that all elements of a complete configuration management processes are both documented and in place, including configuration identification, configuration change control, status accounting, and configuration audits.
- Verify that the software quality assurance process is documented, organized and managed so that there is organizational independence from the software development organization.
- Ensure that there are independent audits of software development processes and products.
- Ensure that the processes provide rigorous tracking, follow-up and reporting of corrective actions.
- Verify that decisions are made in accordance with a documented decision analyses and resolution process, using defined decision criteria.
- Verify that personnel are trained, as applicable, in the appropriate processes: management, development, maintenance, operations, infrastructure, configuration management, etc.
- Verify that processes are defined and documented and are in place to ensure the administration and maintenance of the system(s) and infrastructure needed for software development and test.
    - Verify that these processes are planned to meet development loads and schedules and they provide for preventative maintenance and responsive corrective action for failures.
    - Verify that needed vendor support agreements and plans are in place and that response agreements are consistent with development team needs.
        - Verify that they are staffed with qualified, trained people.

Checklists for Assessing Software Development Products for MA Activities

Assessment of contractor software development products requires experienced reviewers, using an orderly, organized review approach, assessing against recognized product standards and best practices. For product descriptions (and DIDs) refer to [OWE04]. As a minimum, the assessment needs to verify that the products meet contract requirements as described in the SOW, compliance standards, and CDRL items, including the DIDs as tailored for the contract. General guidance for assessment is described in each product group.

The products below are grouped as follows:

Software management products: describe the planning, scheduling, and budgeting of all activities from initial requirements analysis to transition of the completed software to operations and maintenance, including all support activities.

Software requirements and design products: describe the analysis, definition, decomposition, and tracing of software requirements and describe the architecture and design that implement the requirements.

Software implementation and test products: describe the coding, integration, and testing of the software items.

Software support products: describe the plans and activities of several critical functions that support the software development processes.

Software Management Products

The quality and completeness of planning for software development is critical for success. Equally important is recognition that a large-scale development will encounter unplanned technical and developmental problems, so there must be adequate provision for risk management, problem discovery, and rework time.

Products applicable to software management include:

- SDP, IMP, IMS, risk management plan
- Software test plans: There will be several plans, one for each level of testing for each major component, and plans for the planned increments, spirals, builds, etc. These may be separate documents, or sections in unified plans
- Software installation plan
- Software transition plan

Please refer to Table A5-5 for the checklist associated with assessing these processes.

Table A5-5, Software Management Products Assessment Checklist

• Verify plans are suitable for the required degree of MA.
• Verify plans are complete, feasible to execute, and describe all activities necessary to complete and deliver the required software items.
• Verify plans have been updated to reflect changes as they occurred.

Software Requirements and Design Products

Products applicable to software requirements and design include:

- Operational concept description
- Requirements products
  - System specification
  - Segment specifications
  - Software requirements specifications
  - Interface requirements specifications
  - Requirements traceability matrix (separately maintained or part of specification)
  - Requirements verification matrix (separately maintained or part of specification)
- Architecture and design products
  - System/segment design description
  - Software architecture description
  - Software design description
  - Interface design description
  - Database design description
- Software engineering analysis products
  - Performance analysis products
  - Resource utilization products
  - Trade study products

Please refer to Table A5-6 for the checklist associated with assessing these processes.

Table A5-6, Software Requirements and Design Products Assessment Checklist

- Verify system, segment, software and interface requirements are correct, complete, consistent, feasible, verifiable, and clearly and unambiguously stated.
- Verify requirements tracing is complete, and all requirements are completely and correctly traced to parent and child requirements.
- Verify requirements validation plan is complete and that appropriate stakeholders have participated.
- Verify requirements verification plan is complete, and all requirements will be completely and correctly tested or otherwise verified.
- Verify that design products describe complete, feasible designs for all software items needed to meet requirements specifications.
- Verify that the architecture products are complete, feasible and implement the requirements.
- Verify that the operational concept is complete and up to date, and that it will be implemented by the architecture and design.
- Verify that the design products reflect the architecture.
- Verify that the engineering analysis products are complete, that the methods used to produce the analyses were applied appropriately, and that the analysis results support architecture and design decisions.

Software Implementation and Test Products

Products applicable to software implementation and test include:

- Implementation products
  - Code
  - Unit test plans, procedures, and results
  - Software development files
- Integration test products
  - Software integration and test plans, procedures and results
  - COTS integration and test procedures and reports
- Qualification test products
  - System/segment test plan(s), procedures and reports (system/segment test description, system/segment test report)
  - Software test plan, procedures and reports (software test description, software test report)
- Software maintenance products
  - Software product specification
  - Software version description (or version description document)
  - Maintenance manuals
  - Computer programming manual
  - Firmware support manuals

- Operations products
  - Recommended operating procedures
  - Automated operating procedures
  - Software user manual(s)
  - Computer operations manual

Please refer to Table A5-7 for the checklist associated with assessing these processes.

Table A5-7, Software Implementation and Test Products Assessment Checklist

- Verify that the supplier's code is developed in accordance with good coding processes and approved coding standards for the program.
  - Participate in selected contractor code reviews (peer reviews).
  - Examine selected critical code visually and with automated code metrics to assess code quality.
- Verify that the supplier's unit tests are conducted in accordance with the program's SDP and software work instructions (e.g., the program's SSPM).
- Periodically verify that unit test plans, procedures, results, and analysis of results are complete and up-to-date, accurate, and provide complete coverage, as specified in the [ADA05, paragraph 5.7.2].
- Periodically verify that SDF contents for the applicable software unit or component are complete and up-to-date, accurate, and are maintained in accordance with the supplier's SDP or other accepted standards.
- Verify that the supplier system and segment integration tests are conducted in accordance with the program's master test plan.
- Verify that the supplier's software-software and software-hardware integration tests are conducted in accordance with the SDP, software work instructions (e.g., the program SSPM), and the software integration and test plan..
- Periodically verify that supplier's integration test plans, procedures, results, and analysis of results are complete (up-to-date with recorded test progress), accurate, and provide robust testing of allocated end-to-end functions and requirements, under nominal and worst-case off-nominal conditions, and satisfy the test coverage requirements in the [ADA05, paragraph 5.8.1].
- Verify timely update of TPM status with information from test data, and timely reporting of erosion of TPM margins.
- Verify that the supplier's software qualification tests are conducted in accordance with the SDP and the software test plan.
- Periodically verify that the supplier's software qualification testing uses the software test description for test cases and procedures and the software test report for results, and satisfies the test coverage requirements in the [ADA05, paragraph 5.9.3].
- Verify that the supplier's operations products are complete, accurate, up to date and, if applicable, feasible to execute.
- Verify that the supplier's software maintenance products are complete, accurate, and up to date.

Software Support Products

These products describe planning for activities that provide support services to the other development activities. These services are critical to successful software development programs. Please refer to Table A5-8 for the checklist associated with assessing these processes.

Products applicable to software support include:

- Software configuration management plan
- Minutes from change control board
- Software quality assurance plan
- Results from software quality assurance audits
- Program or organization training plan
- Architecture descriptions of development and test environment
- System administration plans and procedures

Table A5-8, Software Support Products Assessment Checklist

• Verify that an adequate qualified software configuration management staff is in place to identify, organize, and control change to the software baseline.
• Verify that configuration management includes configuration identification, configuration change control, status accounting, and configuration audits.
• Verify that change control boards are operating in accordance with the software configuration management plan.
• Verify that change control board minutes are adequate and are distributed in a timely manner.
• Verify that the software quality assurance plan provides adequate surge staff for increased software quality assurance audit activity at milestones and heavy test periods.
• Verify that non-compliance reports from software quality assurance audits are being resolved and tracked to closure.
• Verify development environments and test environments represent the target operational environment as much as possible and are at a high enough fidelity to foster early discovery of software defects.
• Verify test environments have sufficient surge capacity for testing to maintain schedules during rework and retest cycles.
• Verify that system administration plans and procedures to support the infrastructure are complete, feasible to execute and describe all activities necessary to support completion and delivery of the required software items.
• Verify that the program or organization training plan is complete, feasible to execute and describes all the training necessary to support the completion and delivery of the required software items.

References

[ADA05] Adams, R. J., et. al., *Software Development Standard for Space Systems*, Aerospace TOR-2004(3909)-3537B, 11 March 2005

[OWE04] Owens, et. al., *Recommended Software-related Contract Deliverables for National Security Space System Programs*. Aerospace TOR-2006(8506)-5738, in press

[SEI02-1] Software Engineering Institute, *Capability Maturity Model® Integration[SM], Version 1.1, CMMI® for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI®-SE/SW/IPPD/SS, V1.1), Continuous Representation*, Carnegie Mellon University, (SEI-2002-TR-011), March 2002

[SEI02-2] Software Engineering Institute, *Capability Maturity Model® Integration[SM], Version 1.1, CMMI® for Systems Engineering, Software Engineering, Integrated Product and Process Development, and Supplier Sourcing (CMMI®-SE/SW/IPPD/SS, V1.1), Staged Representation*, Carnegie Mellon University, (SEI-2002-TR-012), March 2002

[SEI05] CMU/SEI-2005-HB-005, *Handbook for Conducting Standard CMM®I Appraisal Method for Process Improvement (SCAMPI) [SM] B and C Appraisals*, Version 1.1, December 2005