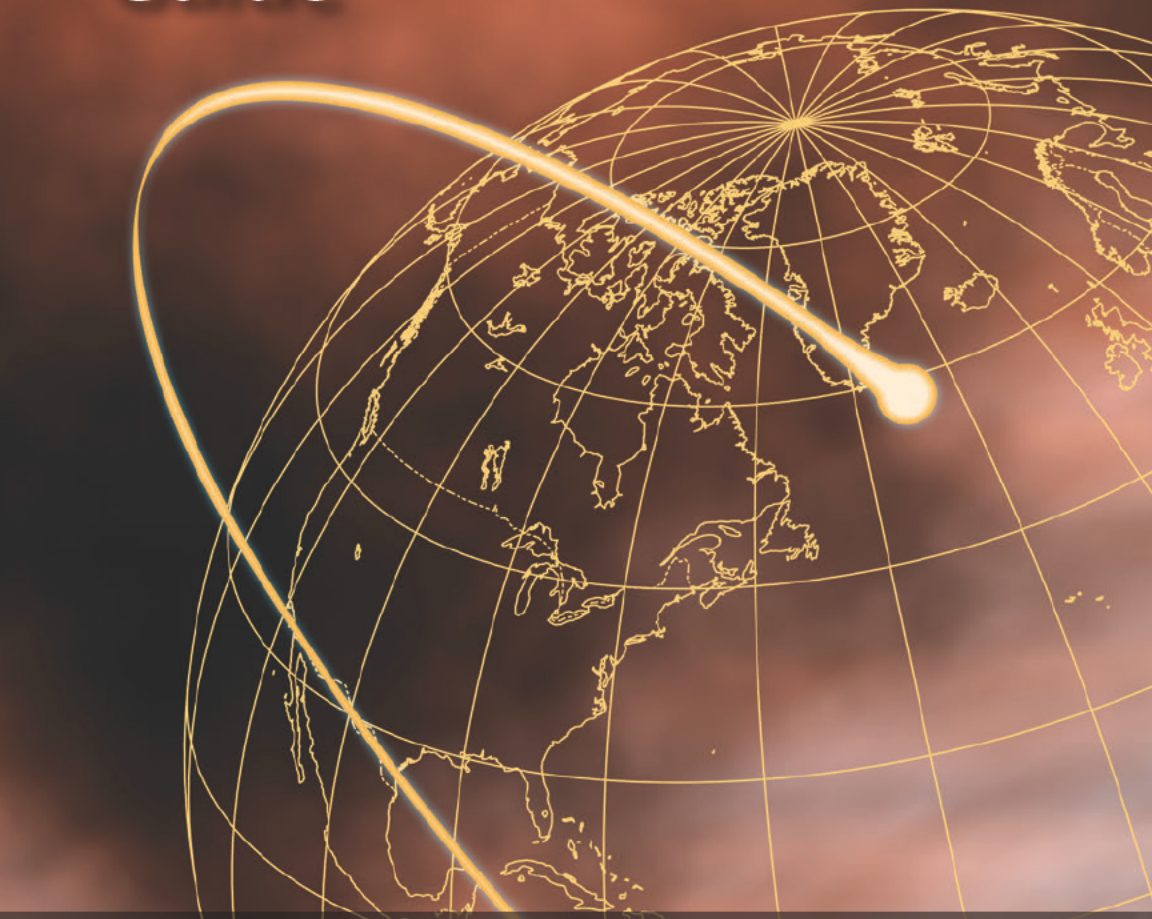
Mission Assurance Guide



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

APPROVED FOR PUBLIC RELEASE

AEROSPACE REPORT NO.
TOR-2007(8546)-6018
Revision B

MISSION ASSURANCE GUIDE

Edited by

S. B. GUARRO, G. A. JOHNSON-ROTH, and W. F. TOSNEY

June 1, 2012

Systems Planning, Engineering, and Quality
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 initial document and Gail Johnson-Roth coordinated the updates and revision to this document, Rev. B. 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 initial guide. The contributing authors are acknowledged in Table I and at the beginning of their respective chapters.

Table I. Contributing Authors

William D. Bjorndahl	Mission Assurance Subdivision
Kenneth R. Childers	Satcom Operations Support
George G. Cuevas	Space Electronics Vulnerability Office
Manuel De Ponte	National Systems Group
Roland J. Duphily	Acquisition Risk and Reliability Eng Department
Colleen M. Ellis	Computer Applications and Assurance Subdivision
Suellen Eslinger	Software Engineering Subdivision
Daniel P. Faigin	Information Assurance Technology Department
Rand H. Fisher	Systems Planning, Engineering, and Quality
John G. Gebhard, III	Retired
James B. Gin	AWTR Systems Engineering
Sergio B. Guarro	Systems Engineering Division
David J. Gorney	Space Systems Group
Dan W. Hanifen	GEOINT Development Office/Payload
Lawrence I. Harzstark	Space Electronics Vulnerability Office
Thomas C. Hecht	System Integration and Test Office
David P. Helgevold	Product and Process Assurance Department
Paul H. Hesse	Directorate L Spacecraft Integration
Leslie J. Holloway	Software Engineering Subdivision
Andrew Y. Hsu	Acquisition Risk and Reliability Eng Department
Gail A. Johnson-Roth	Acquisition Risk and Reliability Eng Department
Jeff B. Juranek	Product and Process Assurance Department
May M. Kwan	Product and Process Assurance Department
Norman Y. Lao	Engineering Data Analysis & Integration Department
David Lutton	Computers and Software Division
Richard C. Maynard	Retired
Arthur L. McClellan	Space Electronics Vulnerability Office
Mark M. Oleksak	DMSP – Spacecraft and Operations
Karen L. Owens	Software Acquisition and Process Department

Eric S. Richter	Product and Process Assurance Department
Steven R. Robertson	Space Electronics Vulnerability Office
Wade Y. Sakauye	Cost, Schedule, and Requirements Department
Abraham A. Santiago	Cost, Schedule, and Requirements Department
Brian E. Shaw	Engineering and Integration Division
Gary D. Shultz	Retired
Mark M. Simpson	Electronics and Power Systems Department
Dana J. Speece	Product and Process Assurance Department
Joseph Statsinger	Retired
Lucio U. Tolentino	Systems Effectiveness, MILSATCOM
William F. Tosney	Corporate Chief Engineering Office
Linda J. Vandergriff	Expl Phen and Analysis Department
Michael R. Ware	Developmental Planning and Architectures
Julia D. White	Corporate Chief Engineering Office
Howard Wishner	Retired

Foreword

Although the past few years of National Security Space (NSS) activity have seen unprecedented mission success in terms of launch and on-orbit operations, delivering critical capability to meet national security needs, our assets have been subject to an unacceptable increase in the number of preventable system integration and 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 predominates; instead, these anomalies seem to be imputable to a combined weakening of systems engineering (SE) and mission assurance (MA) practices, with roots in attempts (beginning in the 1990s) to reduce NSS acquisition costs. Authoritative studies such as the *Tom Young Report*[1] 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 quality problems, process deficiencies, SE concerns, and impacts on mission performance.

It is in the context of the concerted efforts by the NSS community to revitalize disciplined SE and MA programmatic activities that the development of this *Mission Assurance Guide (MAG)* has been initiated and executed, with the encouragement of Dr. Wanda Austin, president and chief executive officer (CEO) of The Aerospace Corporation (Aerospace); Dr. William Ballhaus (former Aerospace president and CEO); 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.

[1]DSB/AFSAB, Acquisition of National Security Space Program, May 2003.

Introduction

Sergio B. Guarro
Systems Engineering Division
Gail A. Johnson-Roth
Acquisition Risk and Reliability Engineering Department

The primary purpose of the *Mission Assurance Guide (MAG*) is to provide practical guidance to personnel of The Aerospace Corporation[2] (Aerospace) and, in general, National Security Space (NSS) program office (PO) personnel, who are responsible for executing mission assurance (MA) functions that are key to achieving program and mission success.

The Aerospace PO, 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, the content was 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. MA functions that are typically carried out by the production entity (i.e., the prime contractor responsible for developing and executing the NSS system design and production activities) are not included in this guide. 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 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 the system concept and user requirements, whereas the prime contractor is

[2]The Aerospace Corporation may also be referred to as Aerospace in this guide.

responsible for interpreting and decomposing requirements into system design specifications, and for executing the design into the manufacture, integration, and verification plans and processes leading to 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, ensuring the prime contractor applies proven and effective processes and practices in developing the system, and, ultimately, 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. These contractors are often referred to systems engineering and technical assistance (SETA). 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 and integration 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, or as it may be applied to different acquisition risk strategies, the guide is intended to be tailored, in scope and/or depth of application, as deemed appropriate by the acquisition organization designated as the organization primarily responsible for MA execution.

The *MAG* defines an overarching MA framework that describes processes, disciplines, and associated executable tasks that are recommended for and applicable to all NSS programs. Aerospace supports that technical oversight role for the organization responsible for the acquisition. This MA framework

includes “best practices” guidance that Aerospace PO, 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 a 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 framework akin to a work breakdown structure (WBS). Chapter 1 introduces the core MA principles, processes, and disciplines. Chapter 2 is an MA planning and verification roadmap that provides a PO the approach to adapting and tailoring the structured hierarchy and organization of tasks, which relates them to the appropriate CMPs, SMDs, program phase, and system framework. Chapter 3 discusses MA methods for assessment and standardized evaluation of MA task plans and executions, which can be carried out utilizing the Mission Assurance Baseline (MAB) as a benchmark.

The MAB is a configuration-controlled set of tasks performed to increase confidence toward the goal of achieving mission success for a satellite system and associated ground systems. The set represents activities for all space vehicle mission types across all acquisition and mission phases. This set is based on mission success guidance found in specifications and standards, policy and other guidance, subject matter expertise, industry best practices, and lessons learned. Tasks in the MAB are intended to be relevant, actionable, and tailorable. Not all tasks are applicable to all programs and some tailoring will be required to meet the unique needs of each program. The MAB is managed as a stand-alone database and is designed to be integrated with a verification management tool suite, the integrated Mission Assurance Tool (iMAT); or can be used as a stand-alone database tool. iMAT is an Aerospace-supported asset for tracking, reporting, and verifying MA accountabilities and assessments. The tool is intended to be used in support of all of Aerospace’s customers in the areas of planning (accountabilities, resource allocation, and task coverage), progress

tracking, risk assessment, and reporting and communication of MA-related activities to various stakeholders.

Chapters 4 through 16 individually cover each of the CMPs and SMDs. Each chapter includes an example of related MA tasks. The guide also includes separate appendices for definitions, acronyms, and a sample of one of the task database outputs.

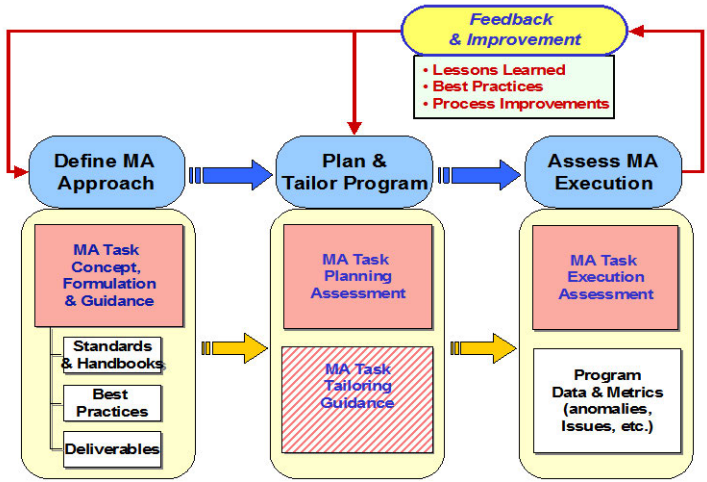


Figure I-1. Mission Assurance Guide within Broader MA Execution Context

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 products 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 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 life cycle and at the start of every new acquisition phase within the life cycle.

Although in terms of system framework or configuration, the primary focus of this guide is the space vehicle (comprising 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 that have been added to the MAB or may be contained in the Launch Vehicle Matrix (LVM), which is an MA verification management tool used for the launch segment. On the other hand, certain aspects of MA related to the performance or replenishment of an entire space vehicle constellation 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 at this particular writing.

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 processes and disciplines in this handbook are properly pursued, the likelihood of mission success will be as reasonably high as we are likely to attain given our present state of experience. For the pursuit of this objective, the guide and the MAB also identify, as appropriate, MA resources available to the Aerospace 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 MAB 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

Mission Assurance Specifications, Standards, Policies, Handbooks, and Best Practices

Gail Johnson-Roth
Acquisition Risk and Reliability Engineering Department
Brian Shaw
Engineering & Integration Division

This section contains a compendium of specifications and standards commonly used as contractual compliance documents, which provide the basis for a disciplined mission assurance (MA) program applicable to national security space (NSS) programs. Additional documents listed in this section include handbooks and best practices that provide guidance in planning and executing MA requirements for NSS programs. These documents offer lessons learned and include collaboration efforts by government, academic, and industry subject matter experts who were assembled to address high-priority common challenges faced by the U.S. space community as they strive to address the challenges to achieving 100-percent mission success.

Specifications and Standards

These specification and standard documents are commonly used as contractual compliance documents and should be evaluated for customer/agency and program applicability, tailored as necessary, and implemented as contract-compliant requirements. The list is current as of the Mission Assurance Guide (MAG) publication date and has a stable heritage, but may evolve as standards are updated or modified. The Aerospace Corporation (Aerospace) recommended set of specifications and standards (highlighted in the list with an asterisk) comprises those standards deemed necessary to adequately support and guide the successful implementation of proven engineering and program management practices in U.S. space programs, in order to achieve mission success while at the same time minimizing any unwarranted and costly impacts to system performance and program schedule.

Contamination Control

*ASTM E 1548	Standard Practice for Preparation of Aerospace Contamination Control Plans, 10 May 2009

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

Electrical/Power

*AIAA S-111-2005	Qualification and Quality Requirements for Space Solar Cells, 26 September 2005
*AIAA S-112-2005	Qualification and Quality Requirements for Space Solar Panels, 26 September 2005
*AIAA S-122-2007	Electrical Power Systems for Unmanned Spacecraft, 5 January 2007
*TOR-2004(8583)-5, Rev 1 [also published as SMC-S-007 (2008)]	Space Battery Standard, 1 April 2005
*TOR-2007(8583)-1 [also published as SMC-S-018 (2008)]	Lithium Ion Batteries for Spacecraft Applications, 30 June 2007
*TOR-2007(8583)-2 [also published as SMC-S-017, (2008)]	Acquisition Standard for Lithium Ion Batteries for Launch Vehicle Application Batteries, 15 January 2008
*TOR-2008(8583)-8492, Rev A [also published as SMC-S-020 (2009)]	Wiring Harness, Space Vehicle, Design and Testing, 28 March 2008

Electromagnetic Compatibility/Electromagnetic Interference

*MIL-STD-461F	Requirements for the Control of Electromagnetic Interface Characteristics of Subsystems and Equipment, 10 December 2007
*MIL-STD-1542B	Electromagnetic Compatibility and Grounding Requirements for Space System Facilities, 15 November 1991
*TOR-2005(8583)-1, Rev A [also published as SMC-S-008 (2008)]	Electromagnetic Compatibility Requirements for Space Equipment and Systems, 1 January 2008

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

Environmental

*NAS 411	Hazardous Materials Management Program, 19 January 1995
*NASA STD 8719.14, with Change 4	Process for Limiting Orbital Debris, 14 September 2009
*TOR-2006(8583)-4474, Rev A [also published as SMC-S-015 (2010)]	Requirements for End of Life Disposal of Satellites Operating at Geosynchronous Altitude, 18 August 2009
*TOR-2007(8506)-7164 [also published as SMC-S-022 (2010)]	Requirements for End of Life Disposal of Satellites Operating in Orbits with a Perigee below 2000 Kilometers, 19 September 2007

Human Factors

*ANSI/HFES-100-2007	Human Factors Engineering of Computer Workstations, November 2007
*COE UIS 4.3, CM Reference 74323	Common Operating Environment (COE) User Interface Standard (UIS), Version 4.3, 31 December 2003
EIA HEB-1A	Electronic Industries Alliance Engineering Bulletin – Human Engineering – Principles and Practices, 1 December 2005
*ISO 9241	Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs), 1 June 1997
ISO 13407:1999	Human Centered Design Processes for Interactive Systems, 1999
*MIL-STD-1472F	DOD Design Criteria Standard—Human Engineering, 23 August 1999
MIL-STD-1472F, Change Notice 1	MIL-STD-1472F – DOD Design Criteria Standard – Human Engineering, Notice 1, 5 December 2003

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

TOR-2010(8591)-3 Vol. 2	Human Computer Interface (HCI) Design Criteria, Volume 2, Display Conventions for Space System Operations, 8 December 2009

Integrated Logistics Support

MIL-PRF-29612B	Training Data Products, 31 August 2001
MIL-PRF-49506	Logistics Management Information, 11 November 1996
MIL-STD-130N	Identification Marking of U.S. Military Property, 17 December 2007
MIL-STD-1366E	Transportability Criteria, 31 October 1989
*MIL-STD-1367A	Packaging, Handling, Storage, and Transportability Program Requirements for Systems and Equipments, 2 October 1989
MIL-STD-1538	Space Parts and Support of Space and Missile Systems Undergoing RDT&E, 11 April 1973
MIL-STD-1545	Optional Spare Parts, Maintenance and Inventory Support of Space and Missile Systems, 15 June 1977
MIL-STD-2073-1E	Standard Practice for Military Packaging, 23 May 2008
TM-86-01/N	Air Force Technical Manual Contract Requirements, 24 February 2010

Interoperability

ANSI/GEIA 836-2002	Configuration Management – Data Exchange Interoperability, 2002
*DISR 12-1.0	Defense Information System Standards Registry (DISR) Standards, 14 March 2012

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

DODAF V2.0, Vol 1	Department of Defense Architecture Framework (DODAF), V 2.0 Volume 1 and Promulgation Memo, 28 May 2009
*DODAF V2.0, Vol 2	Department of Defense Architecture Framework (DODAF), V 2.0 Volume 2, Final 2009-05-28, 28 May 2009
DODAF V2.0, Vol 3	Department of Defense Architecture Framework (DODAF), V 2.0 Volume 3, Final 2009-05-28, 28 May 2009
DTC/03-05-07	Telemetry and Telecommand Data Specification, 2003
ISO 11754:2003	Space Data and Information Transfer Systems – Telemetry Channel Coding, 2003
ISO 12171:2002	Space Data and Information Transfer Systems – Telecommand – Channel Service, 2002
ISO 12172:2003	Space Data and Information Transfer Systems – Data Routing, 2003
ISO 12173:2003	Space Data and Information Transfer Systems – Telecommand – Command, 2003
ISO 12174:2003	Space Data and Information Transfer Systems – Telecommand – Architectural Specification for the Data, 2003
ISO 13419:2003	Space Data and Information Transfer Systems – Packet Telemetry, International Organization for Standards, 2003
ISO 15396:1998	Space Data and Information Transfer Systems – Cross Support Reference Model, 1998
MIL-STD-2401	DoD World Geodetic System 84(EGS84), 11 January 1994

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

Maintainability

*MIL-STD-470B	Maintainability Program for Systems and Equipment, 30 May 1989

Manufacturing

*MIL-STD-1528A	Military Standard Manufacturing Management Program, 1 September 1986

Mass Properties

*AIAA S-120-2006	Mass Properties Control Standards for Space Vehicles, 1 December 2006
TOR-2008(8583)-7560	Tailoring Instructions for AIAA S-120-2006, Mass Properties Control for Space Systems, 29 February 2008

Mechanical Assemblies

*AIAA S-114-2005	Moving Mechanical Assemblies for Space and Launch Vehicles, 28 October 2005

Ordnance

*AIAA S-113-2005	Criteria for Explosive Systems and Devices Used on Space and Launch Vehicles, 10 November 2005

Parts, Materials and Processes

ANSI/AIAA R-100A-2001	Recommend Practice for Parts Management, 16 August 2011
*TOR-1998(1412)-1, Rev B [also published as SMC-S-011 (2008)]	Parts, Materials, and Processes Control Program for Expendable Launch Vehicles, 1 July 2008
*TOR-2006(8583)-5235, Rev A [also published as SMC-S-009 (2009)]	Parts, Materials, and Processes Control Program for Space and Launch Vehicles, 2008

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

*TOR-2006(8583)-5236, Rev A [also published as SMC-S-010 (2009)]	Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles, 30 September 2008

Pressurized Hardware

*AIAA S-080-1998	Space Systems—Metallic Pressure Vessels, Pressurized Structures, and Pressure Components, 1 September 1988
*ANSI/AIAA S-081-2006	Space Systems—Composite Overwrapped Pressure Vessels (COPVs), 24 July 2006
*TOR-2003(8583)-2895 Rev. 1 [also published as SMC-S-006 (2008)]	Solid Rocket Motor Case Design and Test Requirements, 22 December 2004
*TOR-2003(8583)-2896, Rev A [also published as SMC-S-005 (2009)]	Space Systems—Flight Pressurized Systems, 15 June 2007

Product Assurance

*ISO 9001	Quality Management Systems—Requirements, 15 December 2000
ISO 14300-1:2011	Space Systems – Program Management – Part 1: Structuring of a Programme, 8 July 2011
ISO 14300-2:2011	Space System Programme Management – Part 2: Product Assurance,12 September 2011
*SAE AS 9100C	Quality Management Systems—Aerospace—Requirements, 15 January 2009
*TOR-2005(8583)-3859 [also published as SMC-S-003 (2008)]	Quality Assurance Requirements for Space and Launch Vehicles, 1 December 2005

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

Program Management

ANSI/EIA 649B [Related standard: TOR-2008(8583)-1, also published as SMC-S-002 (2008)]	National Consensus Standard for Configuration Management, 29 October 2011
*ANSI/EIA 748B	Earned Value Management Systems, 10 September 2007
IEEE 828-2012	Standard for Software Configuration Management, 2012
*MIL-STD-1528A	Production Management, 9 September 1986
*TOR-2006(8583)-1 [also published as SMC-S-002 (2008)]	Configuration Management, 1 August 2005

Program Protection

AFPAM 63-1701	Program Protection Planning, 27 March 2003
AFPD 63-17	Technology and Acquisition System Safety Protection Programs, 26 November 2001
DCID 6/3	Protecting Sensitive Compartmented Information within Information Systems, 11 December 2003
DOD 5220-22M	National Industrial Security Program, 28 February 2006
DOD-8510.01	DOD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007
DODI 8500.2	Information Assurance Implementation, 6 February 2003

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

DODM 5200.39-M	Procedures for Critical Program Information (CPI) Protection Within the Department of Defense, 1 January 2008
ICD No. 503	Intelligence Community Directive Number 503, 15 September 2008
TOR-2007(8583)-6702	Information Assurance Handbook for DOD space Systems: Guidance on Application of DOD 8500.1/8500.2 IA Controls, 31 August 2007

Reliability

MIL-STD 785B	Reliability Program for Systems and Equipment Development and Production, Note 1, 31 July 1986
MIL-STD-785B	Reliability Program for Systems and Equipment Development and Production, Note 2, 5 August 1988
*TOR-2007(8583)-6889 [also published as SMC-S-013 (2008)]	Reliability Program for Space Systems, 10 July 2007
TOR-2009(8591)-13	Space Vehicle Failure Modes, Effects, and Criticality Analysis (FEMCA) Guide, 15 June 2009
TOR-2009(8591)-14	Effective Fault Management Guidelines, 5 June 2009

Risk Management

*ISO 17666	Space Systems—Risk Management, 1 March 2003

Software

IEEE 828-2012	Standard for Software Configuration Management Plans, 2012
IEEE 1012-2004	Standard for Software Verification and Validation, 1 January 2005

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

IEEE 1028-1997	Standard for Software Reviews, 1 January 2008
IEEE 1471-2000	IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, 21 September 2000
*ISO/IEC STD 15939	Software Engineering—Software Measurement Process, 11 July 2007
TOR-2004(3909)-3405	Metrics-Based Software Acquisition Management, May 2004
*TOR-2004(3909)-3537, Rev. B [also published as SMC-S-012 (2008)]	Software Development Standard for Space Systems, 11 March 2005

Structures

*AIAA S-110 2005	Space Systems—Structures, Structural Components, and Structural Assemblies, 12 July 2005
ATR-2009(9369)-1	Critical Clearances in Space Vehicles, 31 October 2008
*TOR-2003(8583)-2886 [also published as SMC-S-004 (2008)]	Independent Structural Loads Analyses of Integrated Spacecraft/Launch Vehicle Systems, 22 August 2003
TOR-2003(8583)-2894	Space Systems – Structure Design and Test Requirements, 2 August 2004

Survivability

ASTM F 1892	Standard Guide for Ionizing Radiation (Total Dose) Testing of Semiconductor Devices, 1 July 2006
*TOR-2008(8583)-8164, Rev A [also published as SMC-S-014 (2010)]	Survivability Program Management for Space, 19 July 2010

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

System Safety

*AFSPCMAN 91-710	Range Safety User Requirements Manual, 1 July 2004
	Vol. 1—Air Force Space Command Range Safety Policies and Procedures
	Vol. 2—Flight Safety Requirements
	Vol. 3—Launch Vehicles, Payloads, and Ground Support Systems Requirements
	Vol. 4— (Classified)
	Vol. 5—Facilities and Structures
	Vol. 6—Ground and Launch Personnel, Equipment, Systems, and Material Operations Safety Requirements
	Vol. 7—Glossary of References, Abbreviations and Acronyms, and Terms
*MIL-STD-882C	System Safety Program Requirements, 19 January 1993

Systems Engineering

AIAA-S-117-2010	Space System Verification Program and Management Process, 30 June 2010
*ANSI/EIA 632	Processes for Engineering a System, 7 January 1999
MIL-STD-1521B, CN3	Technical Reviews and Audits for Systems, Equipment and Computer Software, 4 June 1985
TOR-2004(3909)-3235	Systems Engineering Charter for National Security Space System Programs, 15 March 2004

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

TOR-2004(8583)-3232	Systems Engineering Contract Data Requirements Selection Guidelines for National Security Space Systems, 20 March 2004
TOR-2004(8583)-3360, Rev 1	System Engineer's Major Reviews for National Security Space Systems, 2 February 2005
*TOR-2005(8583)-3, Rev. B [also published as SMC-S-001 (2010)]	Systems Engineering Requirements and Products, 2009
*TOR-2006(8506)-4732	Space System Verification Program and Management Process, 30 June 2006
*TOR-2007(8583)-6414,Vol. 1, Rev 1 [also published as SMC-S-021 (2010)]	Technical Reviews and Audits for Space Systems, Equipment, and Computer Software, 30 January 2009
*TOR-2008(8583)-7731 [also published as SMC-S-019, Rev A (2008)]	Program and Subcontractor Management, 11 March 2008

Test: Ground Systems

*MIL-STD-810G	Test Method Standard for Environmental Engineering Considerations and Laboratory Tests, 31 October 2008
*MIL-STD-1833	Test Requirements for Ground Equipment and Associated Computer Software Supporting Space Vehicles, 13 November 1989

Test: Launch and Space

*TR-2004(8583) -1 Rev. A [Also published as SMC-TR-06-11 and SMC-S-016 (2008)]	Test Requirements for Launch, Upper-Stage, and Space Vehicles, 6 September 2006

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

Mission Assurance Policies and Directives

DOD systems engineering policy, directives, handbooks, and web resources can be found at: http:www.acq.osd mil, select tab "Policy & Guidance."

SMC systems engineering policy, directives, instructions, and guides can be found on SMC Livelink in the Process Asset Library (PAL), including the following MA-related guidance:

SMC-G-1201	Assurance of Operational Safety, Suitability, & Effectiveness for Space & Missile Systems, 7 Oct 2009
SMC-G-1202	Space Flight Worthiness, 7 Oct 2009
SMC-G-1203	Independent Readiness Review Teams, 13 Oct 2009
SMC-G-1204	Readiness Review Process, 9 Oct 2009

Handbooks and Guides

Handbooks

Listed below are guides and handbooks developed by Aerospace as well as external government agencies (SMC, DOD, NASA) and professional engineering community organizations.

ISBN 1-884989-11-X	Spacecraft Thermal Control Handbook, Volume 1, Fundamental Technologies, 1 January 2002
ISBN 1-884989-14-4 (v. 2)	Spacecraft Thermal Control Handbook, Volume II, Cryogenics, 1 January 2000
ISBN 1-884989-15-2	Space Modeling and Simulation Roles and Application Throughout the System Life Cycle, 1 January 2004
TOR-2006(3904)-1	Digital ASIC/PLD Development Handbook for Space Systems

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, 30 November 2005
TOR-2006(8545)-4591	Space Vehicle Test and Evaluation Handbook; Vol 2, 18 November 2010 and Vol 1
TOR-2008(8506)-8377	Guidelines for Space Vehicle System Late Changes Verification Management. 2008
TOR-2011(8591)-5	Mission Risk Planning & Acquisition Tailoring Guidelines for NSS Vehicles, 13 August 2010

Mission Assurance Improvement Workshop - Best Practices

The U.S. space community (industry, academia, and government) formed the Mission Assurance Improvement Workshop (MAIW) to explore and document best practices and craft a common approach to mission assurance for the U.S. space program. The MAIW is a U.S space program community of practice dedicated to the development and promulgation of proven scientific, engineering, quality, and program management practices related to the U.S. space program's mission success.

ATR-2009(9369)-1	Critical Clearance in Space Vehicles, 31 October 2008
TOR-2006(8506)-4732 Rev A	Space System Verification Program and Management Process
TOR-2009(8546)-8604	Reuse of Hardware and Software Products, 27 January 2010
TOR-2009(8583)-8545	Guidelines for Space Systems Critical Gated Events, 9 May 2008
TOR-2009(8591)-11	Design Assurance Guide, 4 June 2009
TOR-2009(8591)-12	Suggested Checklist to Improve Test Performance in the System Test Equipment Area, 21 May 2009
TOR-2009(8591)-13	Space Vehicle Failure Modes, Effects, and Criticality Analysis 2009 FMECA Product, 15 June 2009

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

TOR-2009(8591)-14	Effective Fault Management Guide, 5 June 2009
TOR-2009(8591)-15	Space Vehicle Checklist for Assuring Adherence to Test-Like-You-Fly Principles, 20 June 2009
TOR-2010(8591)-6	Test Like You Fly: Assessment and Implementation Process, 18 January 2010
TOR-2010(8591)-16	Space Vehicle Testbeds and Simulators Taxonomy and Development Guide, 30 June 2010
TOR-2010(8591)-17	Guidance for Space Program Modeling and Simulation, 30 June 2010
TOR-2010(8591)-18	Mission Assurance Program Framework, 30 June 2010
TOR-2010(8591)-19	Objective Criteria for Heritage Hardware Reuse, 30 June 2010
TOR-2010(8591)-20	Flight Unit Qualification Guidelines, 30 June 2010
TOR-2011(8591)-18	Supplier Risk Evaluation and Control, 1 June 2011
TOR-2011(8591)-19	Failure Review Board Guidelines Document, 10 June 2011
TOR-2011(8591)-20	Space Segment Software Readiness Assessment
TOR-2011(8591)-21	Mission Assurance Guidelines for A-D Mission Risk Classes
TOR-2011(8591)-22	Space Segment Information Assurance Guidance for Mission Success, 10 June 2011

(*) Indicates Aerospace recommended specification or standard to be considered as a compliance document for any NSS acquisition.

Chapter 1
Core Mission Assurance Principles, Processes, and Disciplines

Sergio B. Guarro
Systems Engineering Division
Dan W. Hanifen
GEOINT Development Office
Gail A. Johnson-Roth
Acquisition Risk and Reliability Engineering Department
William F. Tosney
Corporate Chief Engineering Office

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.

1.2 Definitions

Mission success[3] **(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. MS is typically evaluated after operational turnover and according to program specific timelines and criteria, such as key performance parameters (KPPs). MS assessments include operational assessments and user community feedback.

Mission assurance[4] **(MA)** is defined as the disciplined application of proven scientific, engineering, quality, and program management principles towards the goal of achieving mission success. MA follows a general systems engineering (SE) framework and uses risk management (RM) and independent assessment as cornerstones throughout the program life cycle.

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

[3]In contrast, acquisition success can be defined in terms of performance, cost, and schedule.
[4]2009 Mission Assurance Summit Strategic Intent: 2010 Mission Assurance

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 (PO) Federally Funded Research and Development Center (FFRDC)-SE and technical assistance (SETA) team,[5] where The Aerospace Corporation (Aerospace) performs that FFRDC role for national security space (NSS) systems.

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 MS in terms of directly attributable positive consequences.

A **core MA process (CMP)** is an SE process that is defined and applied to support MA goals.

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.

1.3 Mission Assurance Tenets

NSS MA requires the application of effective MA tenets throughout all phases of the life cycle of a program to ensure MS.

1.3.1 Mission Success is "Job 1"

Today we are developing systems of greater complexity with inherently more potential defects and limited and constrained resources. This requires a more disciplined strategy, one that takes a risk-based approach to MA early on in the life cycle, and that considers the constraints of limited resources (cost and schedule), allocates resources to the highest-risk areas, and integrates value-added requirements and MA provisions as a plan for MS. The "Defense Science Board Task Force" stated that "cost has replaced mission success as the primary driver in managing acquisition processes, resulting in excessive technical and

[5]Hereafter in this guide known as the "government PO team."

schedule risk." MS must be the overarching principle in acquisition. Every program has the responsibility to plan for MS; this includes organizing, training, and educating our workforce in the ways of MA. It is not one employee's job; it is every employee's job. Our number one priority must be dedication to MS that mandates a unique, high-confidence MA culture.

1.3.2 Bake It In—UPFRONT

Early decisions on the weapons system capabilities and requirements have a large impact on program cost and schedule and should be supported by a rigorous system analysis and SE process involving teams of users, acquirers, and industry representatives. Concept development and refinement occurs before contract award where 75 percent of the cost decisions are made. Once the government program manger has identified the budget for a new space vehicle, the program objectives, scope, constraints, and the environment in which the program is executed are characteristics that will determine the program risk tolerance. A detailed examination to determine the acquisition strategy and subsequent program implementation includes defining key performance parameters, cost goals, schedule, leadership, and resources. The estimated cost of a mission is a significant contributing attribute and may drive the risks in a program, the risk that the government manager is willing to accept. The contractual compliance set of standards and specifications should reflect the current best practices of government and industry and should be appropriately tailored to match the acquisition strategy and relevant risk posture of the program. These contractual requirements serve as the technical baseline for the program. The requirements and mission assurance processes must be integrated across the entire contractor and supplier base. A program management plan should be put in place that clearly defines accountabilities to execute the defined technical baseline. The final Request For Proposal (RFP) and negotiated contract with the appropriate compliance documents and the program management plan provide the mechanisms to ensure MA is baked in upfront.

1.3.3 Assure the Design Is Right

Recent Aerospace studies suggest that design issues account for 40 percent of on-orbit anomalies. The highest payoff from MA happens early in the program life cycle by preventing problems before they happen, rather than fixing problems later. A design assurance process must be put in place to reduce these anomalies by discovering, preventing, and correcting errors or potential escapes early in a system's life cycle where issues are more easily and less expensively corrected. Design assurance is not only the assessment of the design, but also evaluated, through product qualification, manufacturing, and test phases to ensure compliance with the detailed design requirements as reflected in the appropriate specifications and standards. Assessment of the readiness to manufacture hardware (HW) and build software (SW) includes ensuring the

technology is available, the hardware can be manufactured, and the software can be built to meet performance, cost, and schedule requirements. Design assurance encompasses mission design, system design, HW and SW design, and test. On-orbit anomaly investigations should be incorporated to the extent that lessons learned are captured and communicated so necessary improvements are captured for future space programs. Employing in-depth design audits with a rigorous in-depth process is essential to ensure the design is the *right* design.

1.3.4 Assure Process Discipline

An iterative set of planning, analysis, test, and inspection processes should be performed from concept to preliminary to detailed design stages to improve the probability that space, launch, and ground systems will meet their intended requirements through all operating conditions and through the design life. The most critical processes should be identified with a special mission assurance emphasis. Acquisition risks should be managed to an established baseline by adhering to highly disciplined, gated processes used in MA.[6] Program risk should be systematically identified and managed at a sufficiently high level, especially during the critical early acquisition phases of a program, to ensure appropriate decisions are made based on the risk acceptance and needs of the program.

1.3.5 Rely on Rigorous Verification Methodologies

NSS systems have characteristics that require a rigorous MA process to maximize confidence in MS**{** XE "MS" **}**. They 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 environments, are not serviceable in operation, are not reusable (except for ground systems), and must satisfy unique requirements for nearly every mission. 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 to ensure that verification management plans and processes are in place that are both effective and disciplined. A pedigree of all delivered HW and SW configuration items (CIs) is essential as well as test-like-you-fly principles to test components and systems in as-flown configurations. SE experience and practice show that the primary focus of mission and systems design activities is the achievement of performance, whereas MA places additional effort and attention on the further objective of ensuring such a performance over time with high levels of confidence and reliability.

[6] "Guidelines for Space Systems Critical Events," TOR-2009(8585)-8585, 9 May 2008.

1.3.6 Leverage Independent Assessment

NSS MA**{** XE “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 independent of the normal activities performed by the prime contractor and subtier contractors/suppliers. In some cases, independent means that a separate technical team is established to conduct a technical or readiness review or audit, to certify launch or mission readiness. Independent technical analysis and evaluation may include the application of specialized tools and subject matter expertise; or, in the case of technology assessments or anomaly investigations, specialized laboratory research. In other cases, the independent nature of MA is manifested within the government PO 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. Assessments serve as an independent process check and verification to ensure that the engineering processes, quality assurance processes, and management processes are being implemented. Executability assessments should be conducted to ensure the program is executable and capable of achieving the mission requirements on time and on schedule. 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.

1.3.7 Integrated Application

Different HW and SW 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 in viewing the system as a whole. 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.

1.3.8 Management and Technical Expertise

MA includes the planning, implementing, and reporting of PO MA activities performed in support of a program. Planning should document the program’s risk posture consistent with the program’s mission (i.e., operation or experimental), identify MA technical command media (i.e., tailoring of required

specifications and standards) as contractual requirements, and clearly communicate PO accountabilities and define MA responsibilities.

The program implementation strategy should evaluate the government resources required over the life cycle to execute the program to ensure the government has access to the talent needed to manage the program. 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 the 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 MS benefits within the constraints of the program.

1.3.9 Reporting Channels

Government PO and contractor PMs 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 decisionmakers if MS 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 MS 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 Mission Assurance Processes and Disciplines

MA can be viewed as a set of programmatic and engineering processes organized together toward the goal of MS. 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.

1.4.1 Mission Assurance Processes

CMPs treated in this guide are:

- Program Assurance
- Requirements Analysis and Validation
- Design Assurance
- Manufacturing Assurance
- Integration, Test, and Evaluation
- Operations Readiness Assurance (ORA)
- Operations, Maintenance, and Sustainment
- 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.

1.4.2 Mission Assurance Supporting Disciplines

SMDs treated in this guide are:

- Risk Assessment and Management
- Reliability Engineering
- Configuration Management (CM)
- Parts, Materials, and Processes (PMP) Management
- Quality Assurance (QA)
- Systems Safety Assurance
- Software Assurance
- Information Assurance (IA)

SMDs tend to span across the entire program life cycle. Because of 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 CMPs. 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, ORA is a CMP, which is articulated for the majority of its composing tasks within Mission Assurance Guide (MAG) Phase D of the NSS acquisition cycle. Risk assessment and management, on the other hand, is an SMD, as it focuses on evaluating risks to MS that may originate in any of the acquisition and operation activities. In fact, some form of risk assessment is used in Phase A to support the MA ORA planning process, and in another program phase to support a different MA process. Thus, this guide classifies risk assessment as an 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.

1.4.3 Mission Assurance from a System Engineering Perspective

A CMP is an SE process that is defined and applied to support MA goals. Figure 1-1 illustrates the CMPs in a graphic based on the standard SE V-Model, the life systems development model illustrating the sequence of steps in a project life cycle. This standard SE process for space systems development emphasizes a requirements-driven design and testing. All design elements and acceptance tests must be traceable to one or more system requirements and every requirement must be addressed by at least one design element and acceptance test. The associated CMP MA tasks detail the independent assessment by a program for each of the SE steps and are closely aligned with the phase of the product development. Just as the engineering disciplines span across the program life cycle, the MA tasks associated with the SMDs (listed in the center of Figure 1-1) also span across the program life cycle.

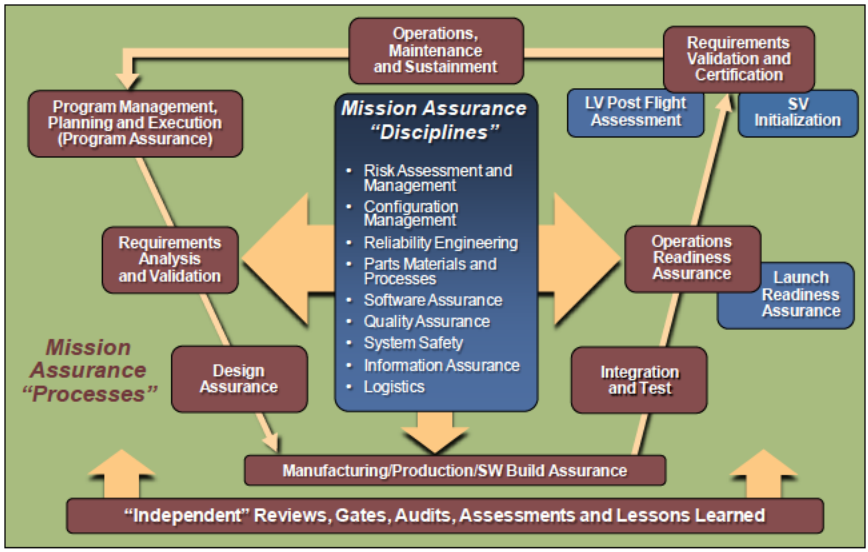


Figure 1-1. MA from an SE Perspective

1.4.4 Development Engineering and Science Disciplines Used to Support Mission Assurance

The ultimate foundation of MS 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. SE 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 to successfully translate allocated requirements/specifications and performance into initial paper designs, performance predictions, breadboards, and/or prototypes and the final design. 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

1.5 Key Lessons Learned

1.5.1 Apply Mission Assurance Principles Early

The most important program decisions, those that influence the total life-cycle costs, are made at Milestone A. The majority of the costs are actually incurred after Milestone C. Figure 1-2, adopted from the Defense Acquisition University graphic, illustrates the system life-cycle acquisition and deployment phases to emphasize the need to apply MA principles very early in the program life cycle. The application of SE and MA principles is critical to ensure an executable program. High-quality pre-Milestone A activities certainly contribute to later positive outcomes. Added requirements and criteria for demonstrated, rigorous SE/PM/MA to Milestone A review are essential to ensure successful acquisition programs are delivered on time and on budget.

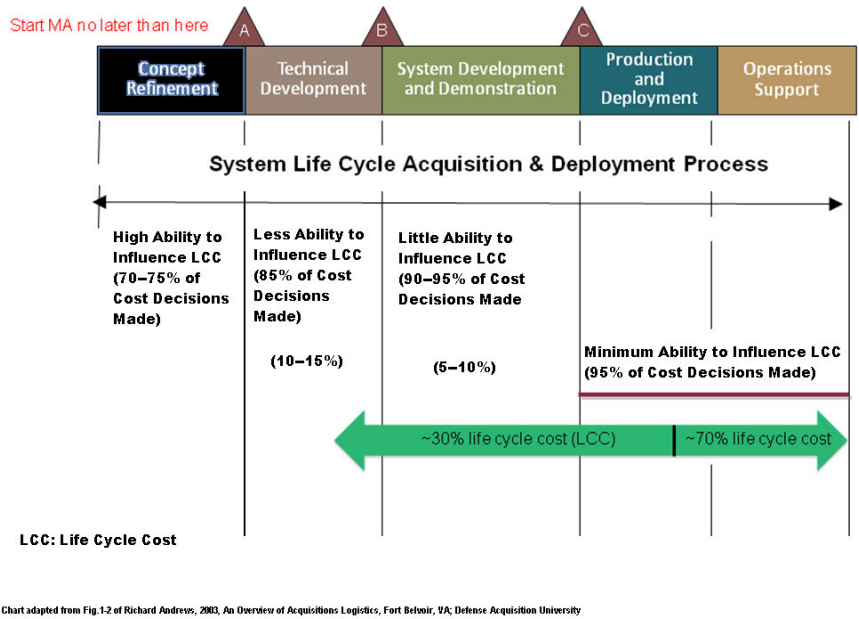


Figure 1-2. System Life Cycle Acquisition and Deployment Process

1.6 Mission Assurance Objective by Life Cycle

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 1-3 summarizes the major acquisition phases (as defined in the Department of Defense [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. Milestones are points in the acquisition timeline of a space program where the program maturity is evaluating to determine readiness to proceed to the next acquisition phase. Note that while acquisition and MA life cycle phases share common terms, specific tasks that occur for MA are unique to furthering MS. Specific MA objectives and tasks are summarized by MA life cycle phase following Figure 1-3.

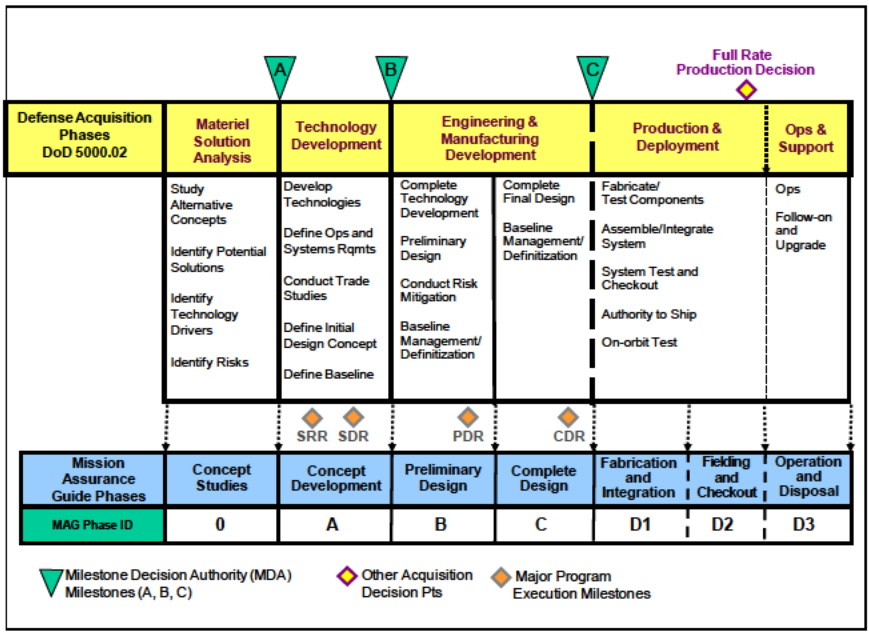


Figure 1-3. MA vs. Space Acquisition Life Cycle Phases[7]

1.6.1 Phases 0 and A – Concept Studies and Early Concept Development

In Phases 0 and A, the primary MA objective is to ensure 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.

[7]Based on DODI 5000.02, 8 December 2008.

Phase 0 and early Phase A MA tasks ensure 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 the government PO establishes the policies, procedures, and contractual language within the SOW or objectives, CDRLs, and DIDs, so the contractors provide the data for MA evaluations.

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

1.6.2 Phase A – Concept Development

MA tasks in Phases A, B, and C 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.

MA tasks in Phase A typically verify and validate concept development and trade studies, system architecture development, threat assessment and protection measures, technology development and technology maturity assessments, risk reduction, requirements development, test and evaluation master plan development, initial design supporting functional baseline development, and industrial capability assessments for key technologies and components. Milestone B determines the program's readiness to begin the preliminary design development activities.

1.6.3 Phase B – Preliminary Design

MA tasks verify and validate the Phase B preliminary design development activities. Phase B increases confidence in the selected system alternatives by assessing the estimated risk levels and projected performance at a detailed engineering level. Critical technology should be tested in relevant environments.

Milestone C determines the program's readiness to begin the final design development activities.

1.6.4 Phase C – Complete Design

MA tasks verify and validate the design development activities. Phase C further increases confidence in the selected system alternative(s) by assessing the estimated risk levels and projected performance at a more detailed engineering level. Phase C provides critical inputs to support build approval, which is the authorization to conduct acquisition-related activities associated with fabrication, testing, and supporting operations that constitute Phase D. Phase C may also be referred to as **critical design** as this phase culminates as the critical design review (CDR).

1.6.5 Phase D1 – Fabrication and Integration

In Phase D1, the primary MA objective is to ensure product and system integrity.

MA seeks to verify that system components and elements are manufactured, programmed (SW), 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. For the ground segment, the description **implementation and integration** is more typically used for Phase D1. It also includes the verification and certification of flight/mission readiness and the assessment of performance risk.

1.6.6 Phases D2 and D3 – Fielding and Checkout and Operations and Disposal

During Phases D2 and D3, the primary MA objective is to ensure 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 ensure 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 Phase D3. 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 CMPs, as illustrated in Figure 1-4. Within the CMPs, tailored sub-processes from a set of SMDs are also integrated as appropriate, as shown in Figure 1-5. 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 1.4.4) applied during detailed technical design processes and analyses. A full discussion of the interrelation of MA processes and disciplines is provided in Sections 1.4.1 and 1.4.2. For the practical implementation of MA, each program will have to conduct a deliberate and focused tailoring activity (as illustrated conceptually by Figure 1-5), 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. For the ground segment, the description **deployment** is more typically used for Phase D2, and **operations** for Phase D3.

1.7 Current SMC Mission Assurance 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."

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 (AFPD) 63-12, AF Instruction (AFI) 63-1201, and AF Material Command Instruction (AFMCI) 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.

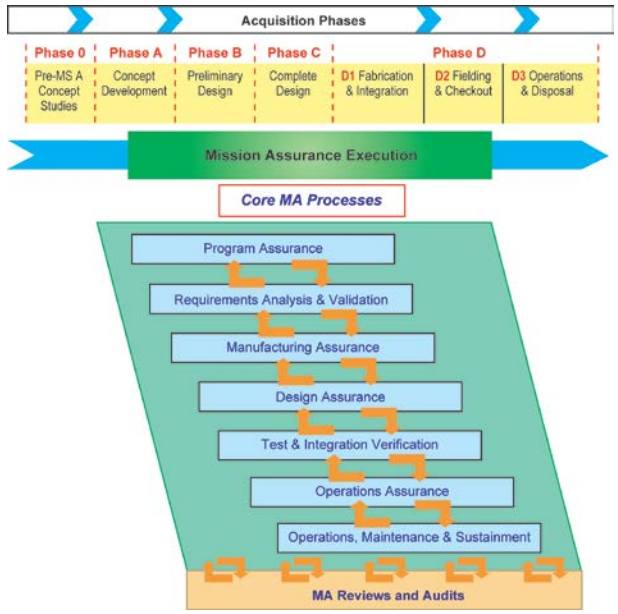


Figure 1-4. MA Execution via CMPs

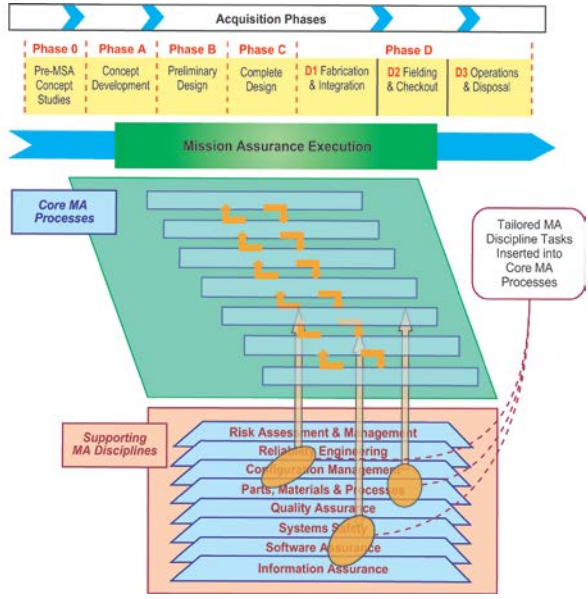


Figure 1-5. Relationships between CMPs and SMDs

Space flight worthiness is determined according to Space and Missile Systems Center Instruction (SMCI) 63-1202 USAF (Space Flight Worthiness), which implements the requirements contained in AFPD 63-14, USAF Flight Worthiness. Space flight worthiness measures the degree to which a spacecraft, launch vehicle (LV), 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 (FRR).

1.8 Mission Assurance Implementation Overview

1.8.1 Organizational Roles and Interactions

Figure 1-6 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 PO, with Aerospace as the program FFRDC support; and Defense Contract Management Agency (DCMA) as the delegated in-plant support. Primary Aerospace MA functions generally reside within the government PO team, but involve all the participants to ensure MS. 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 MA 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 PO team.

The DCMA team typically provides a program integrator (PI) as a focal point for the government PO 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, and 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 general system engineering and integration (GSE&I) tasks executed by Aerospace, are assigned in accordance with the SMC FFRDC Users Guide[8] 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

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

government team in support of the system PO. However, Aerospace has a unique MA role providing independent and objective technical assessments reported through the Aerospace President to the SMC Commander.

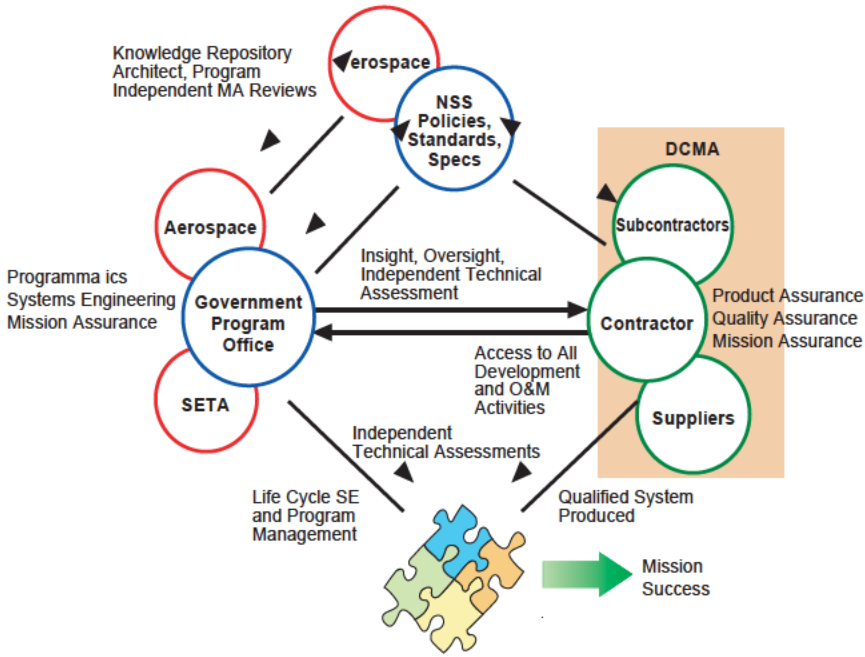


Figure 1-6. Distributed and Complementary MA Responsibilities[9]

1.8.2 National Space Security Mission Assurance Model

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. The NSS model shown in Figure 1-7 defines an effective, consistent, repeatable, single, enterprise-wide MA baseline process to apply to all programs. 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. The 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.

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

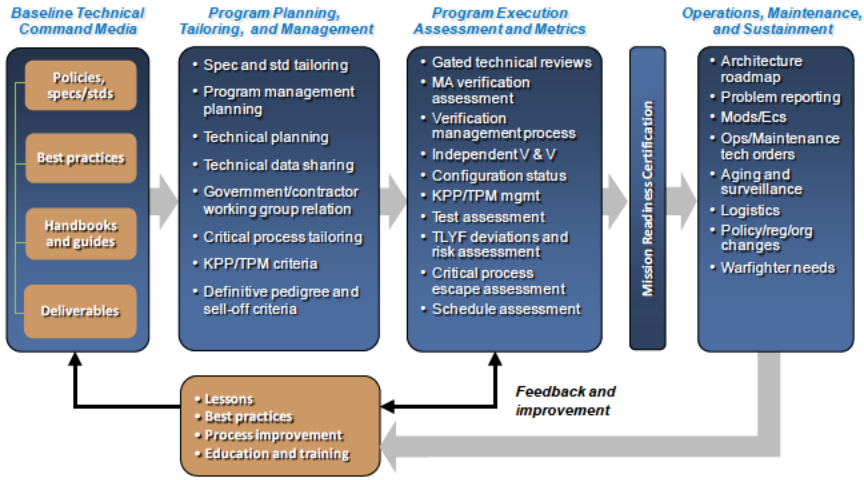


Figure 1-7. Mission Assurance Model for National Security Space

A complete MA process identifies phase-dependent core processes and specialty disciplines. Program planning, tailoring, and management of those tasks are consistent with the program objectives.

Since CMPs and engineering disciplines 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 greatest MA value for the program
2. Threads these tasks together in an execution flow that, in depth and timing, is compatible with the program goals and resources

MA task execution is conducted periodically, and before critical milestones. This information should be documented concerning task closure criteria and satisfaction in execution to enable an assessment of residual risk to the program. The residual risk information is used as part of the overall program assessment, readiness, and launch certification process to determine whether the level of risk in any particular area is acceptable, or whether additional assurance activities are warranted. Task closure and evidence of verification by responsible engineers culminates in the final gates (Aerospace Presidents Review and/or FRR) prior to mission readiness certification.

Once the program or program segment is declared operational, MA activities shift to the operations and disposal phase (D3). Programs in D3 must continue to

ensure system requirements remain satisfied to the extent possible as assets age and eventually degrade or fail. The depth of MA effort is constrained by available engineering resources and budgets; it must be planned and executed accordingly. The MA tasks are operations oriented to include SW updates, monthly stationkeeping and solar salutes, and anomaly resolution.

The NSS MA model is closed loop in that it is dependent on communication of lessons learned, process improvements, and best practices to improve the technical command media by considering feedback from the execution and operations phases of the programs.

1.8.3 Program-Integrated Mission Assurance Execution

Figure 1-7 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 and 1-5. Core processes, disciplines, specifications and standards, other CDRLs, and government PO and contractor MA programs are all tailored according to program criticality, priority, schedule, and available resources. Specific test and evaluation (T&E) or SE 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.

1.9 References

Policy-Related

AFI 63-1201	Life Cycle Systems Engineering, 12 September 2011
AFI 99-101	Developmental Test and Evaluation, 1 November 1996
AFI 99-102	Operational Test and Evaluation, 1 July 1998
AFMCI 63-1201	Implementing Operational Safety, Suitability, and Effectiveness (OSS&E) and Life Cycle Systems Engineering, 11 February 2011
AFPD 63-12	Assurance of Operational Safety, Suitability, and Effectiveness, 1 February 2000

AFPD 63-101	Acquisition and Sustainment Life Cycle Management, 3 April 2009
DODI 5000.02	Operation of the Defense Acquisition System, 8 December 2008
SMCI 63-1201	Assurance of Operational Safety, Suitability, and Effectiveness (OSS&E) for Space and Missile Systems, 16 January 2004
SMCI 63-1202	USAF Space Flight Worthiness, 16 January 2004
SMCI 63-1203	Independent Readiness Review Teams, 16 January 2004
SMCI 63-1204	SMC Readiness Review Process, January 2004.

Handbooks

DOD-HDBK-343 (USAF)	Design, Construction, and Testing Requirements for One-of-a-Kind Space Equipment, 1 February 1986

Other

DSB/AFSAB Task Force Report	Acquisition of National Security Space Programs, November 2002
GAO-03-98	Major Management Challenges and Program Risks: Department of Defense, January 2003.
TOR-2004(1901)-3101	Recommended Missile Defense Agency Mission Assurance Practices, 17 October 2003
TOR-2009(8583)-8577	Mission Assurance from a Program Life Cycle Success Perspective, 15 November 2008
TOR-2009(8585)-8585	Guidelines for Space Systems Critical Events, 9 May 2008

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

2009 Mission Assurance Strategic Intent: 2010 Mission Assurance

Aerospace's Lessons Learned database

Pre-Milestone A and Early Phase Systems Engineering: A Retrospective Review and Benefits for Future Air Force Acquisitions, Air Force Studies Board, National Research Council, 2008

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

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

SMC FFRDC Users Guide, 20 January 2004

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

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

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

Chapter 2

Mission Assurance Planning and Verification

Gail A. Johnson-Roth
Acquisition Risk and Reliability Engineering Department
Norman Y. Lao
Engineering Data Analysis & Integration Department

2.1 Introduction

This chapter provides an overview of the planning and execution of mission assurance (MA) activities performed in support of a program. The following overarching values should underscore the essence of the MA effort:

- Commitment to mission success
- Commitment to the interest of the national security space (NSS) customer
- Commitment to implement (to include developing and improving) necessary capabilities

Applying MA best practices with dedication to mission success links these values to the work at hand. MA includes the engineering management activities that the government conducts in the context of a program office (PO) to execute acquisition responsibilities (i.e., acquisition strategy, milestone reviews, etc.) and assessment of program risk (technical, cost, or schedule) leading to the timely and effective deployment of space systems.

MA accountabilities include technical review or independent analysis of the work of industrial contractors who are designing or manufacturing spacecraft and launch vehicles to assess the readiness of each vehicle for launch and operation. Dedication to mission success requires taking lessons learned captured in standards and best practices and applying those to the program baseline. MA requires engineering judgment to be objectively applied when assessing risks associated with baseline deviations, providing technical excellence in those assessments, and communicating with integrity the results of those assessments. The challenge is to learn from the lessons of the past as we face the challenges of today.

2.2 Definitions

The purpose of an **MA Plan (MAP)** is to provide a structured and consistent communication of program office support within the PO, customer set, and senior management as well as serve as guidance to the personnel in the PO. MA

includes the planning, implementing, and reporting of PO MA activities performed in support of a program. The MAP should document the program's risk posture consistent with the program's mission (e.g., operation or experimental), identify MA technical command media (e.g., tailoring of required specifications and standards) as contractual requirements, and clearly communicate program office accountabilities and define MA responsibilities. The MAP should also identify those aspects of the program that will not be assessed.

The **Mission Assurance Baseline (MAB)** is the corporate, configuration-controlled set of tasks performed to increase confidence toward the goal of achieving mission success for a satellite system and associated ground systems. The set represents activities for all space vehicle (and ground system) mission types across all acquisition and mission phases. This set is based on mission success guidance found in specifications and standards, policy, and other guidance, ETG expertise, PO experience, industry best practices, and lessons learned. A PO should produce a tailored set of tasks that is believed to be practically executable within the scope and constraints to meet the specific needs of that program.

MA verification, as described in the *Mission Assurance Guide (MAG)*, is focused primarily on the identification, tailoring, and assessment of MAB tasks. MA processes should be applied in accordance with the total risk tolerance of the program, considering the constraints of cost and schedule, and ensure formal reviews validate and document risk mitigation tactics. MA activities should be viewed as an investment to save future dollars—doing smart things up-front to reduce risk and avoid an issue or catch an issue prior to impacting the mission. The identification and tailoring of MA activities have the objective of selecting and refining tasks from the MAB. MA activities must be tracked against the program baseline and red flag indicators put in place to immediately identify baseline deviations to program stakeholders.

MA technical command media is defined by The Aerospace Corporation (Aerospace) as the collection of vetted and configuration-controlled MA guidance recommended to increase the confidence in achieving mission success. Command media is a configuration-controlled set of requirements, processes, practices, and policies that govern space system-of-systems (SOS) acquisition, programmatic, and MA activities. The MA technical command media includes recommended specifications and standards; the MAB; handbooks; and applicable policies, practices, and instructions.

2.3 Acquisition Mission Risk Classification

The early establishment of mission risk acceptance provides the basis for government program and project managers to effectively communicate the

acceptable level of risk to develop and implement appropriate contractual requirements and risk management strategies. Recently published guidelines define criteria for four mission risk classification levels (i.e., A, B, C, and D) as a function of several parameters.[10,11] The same documents also provide tailoring guidance for a recommended minimum set of specifications, standards, and processes that should be placed on contract for any national security space vehicle acquisition. The development of tailored specifications and standards for a specific contract is intended to ensure a cost-effective space system acquisition consistent with the risk tolerance, policies, and constraints in the establishment of the technical baseline requirements.

Acquisition planning requires defining requirements for contractual application to represent the best balance between cost, schedule, performance, and risk. Specifications and standards define the developing system design, manufacturing, test, and safety requirements. Although every requirement in a specification or standard may be appropriate for some programs, every requirement does not make sense for every program. The set of applicable requirements for the identified applicable specifications and standards is established through an integrated and iterative approach based on the analysis of cost/technical drivers and risk, and serve as the baseline for that program. Program characteristics (i.e., risk classification level) are the primary influence on the decisions made during the requirements tailoring process. Tailoring the standards and specifications is the responsibility of the government in consideration of the mission risk profile and other program characteristics. The collective set of tailored requirements should be evaluated to ensure that the MA profile is in agreement with the risk posture and needs of the program.

The PO MAP should describe the methodology that will be applied to the program based on the accepted mission risk. The resource planning and allocation should match the tailoring approach of the awarded contract. The tailored contract requirements will drive the PO activities to include approval of deliverables and required presence with review and approval at technical meetings and major milestones. PO MA oversight should be executed in accordance with the mission risk established for that program.

2.4 Mission Assurance Plan

MA planning of support to programs is fundamental to the commitment to mission success, working to improve effectiveness for space operations and end user communities and contributing to acquisition success. Government organizations may produce a MAP for the program or have other program

[10]TOR-2011(8591)-5, Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles, 13 September 2010.
[11]TOR-2011(8591)-21, Mission Assurance Guidelines for A-D Mission Risk Classes, 3 June 2011.

documentation that satisfies recommended elements as described in this chapter. MAPs can be produced at the program or at the **mission area level**.

The Aerospace program office is responsible for establishing, maintaining, and executing a MAP for Aerospace support to a program. The Aerospace PO communicates and coordinates the MAP with the customer and ensures that the portion of the MAP describing Aerospace support is consistent with applicable technical objectives and plans. A MAP is defined and implemented at inception of Aerospace support for a new program, at a significant upgrade to an existing system, or at any point in system development that Aerospace support is initiated. The customer organization for the program may have a MAP or other program documentation. The MAP for Aerospace support to the program may reference the customer program documentation to address the required elements supplemented with an addendum to address Aerospace accountability

2.4.1 Purpose of a Mission Assurance Plan

The MAP should provide a structured and consistent communication of PO accountabilities in the planned execution of that program. These contributions contribute to achieving mission success; work to improve effectiveness for space operations and end user communities; and reflect MA to meet the program's needs and constraints. The MAP considers agreements and tasking by the relevant customers, articulates scope of effort, and identifies aspects of the program that will be assessed. In some cases, the MAP may be generated by the government organization for the entire PO effort, or be more limited in scope to address Aerospace support to a particular customer. The goal of a MAP is to facilitate communication of PO roles, responsibilities, and accountabilities. The communication should be dynamic and the MAP should be updated periodically to address different program phase priorities, significant changes in allocated resources, or program re-plans.

2.4.2 Establishing a Mission Assurance Plan

A MAP is defined and implemented when the PO is established, at a significant upgrade to an existing system, or at any point in the system development that is appropriate to document PO roles, responsibilities, and accountabilities. A timeline for putting a MAP in place for a program, to include level of effort and support organizations, should be established at plan inception. The MAP should include the set of reporting points for formal periodic MA assessments. The reporting points are agreed-upon times when program assessments will be reported out to stakeholders, and which are typically aligned with major program milestones.

The first step to creating a MAP is to perform an initial program assessment to ensure that all relevant information is considered. This step requires PO

communication and discussion of customer policies and practices and contractual documentation in place. Discussions should include, but are not limited to, the established mission risk with consideration of the compliance specifications and standards, mission type, program phase, mission duration, contract partners, technology readiness, supply chain, CONOPS, cost goals schedule, and contract type. A technical assessment of program risks should further be completed that at a minimum considers the following: previous lessons learned, contractor experience, new mission area vs. existing, design complexity, and if development is a first article (first of fleet) or production. Understanding and documenting the PO needs and requirements is required to efficiently and effectively dedicate program office resources—to include Aerospace capabilities and commitments that are detailed in the SMC Federally Funded Research and Development (FFRDC) Users Guide[12] and the manpower allocations for a specific program. The MAB is also a useful resource to do preliminary assessment of typical MA tasks that may be conducted in execution of PO accountabilities. Figure 2-1 illustrates this initial program assessment.

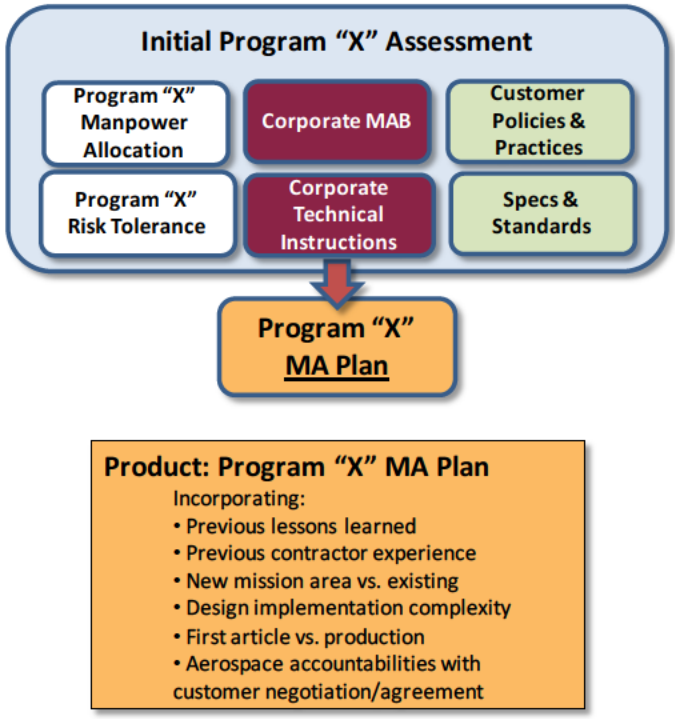


Figure 2-1. Initial Program Office Assessment

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

The MAP should capture existing processes in place. Applying MA processes to a program begins with the MA technical command media baseline established for the program. The MA technical command media baseline is tailored to a program's specific needs and constraints to define the MA approach of the program. Monitoring and assessment of MA activities continues throughout the program life cycle and across all segments for which the program is accountable. This approach is consistent with the MA model previously discussed in Chapter 1 and reproduced here in Figure 2-2 for reference. The MA technical command media baseline serves as the basis of the MA tasks that will be planned and executed by the program.

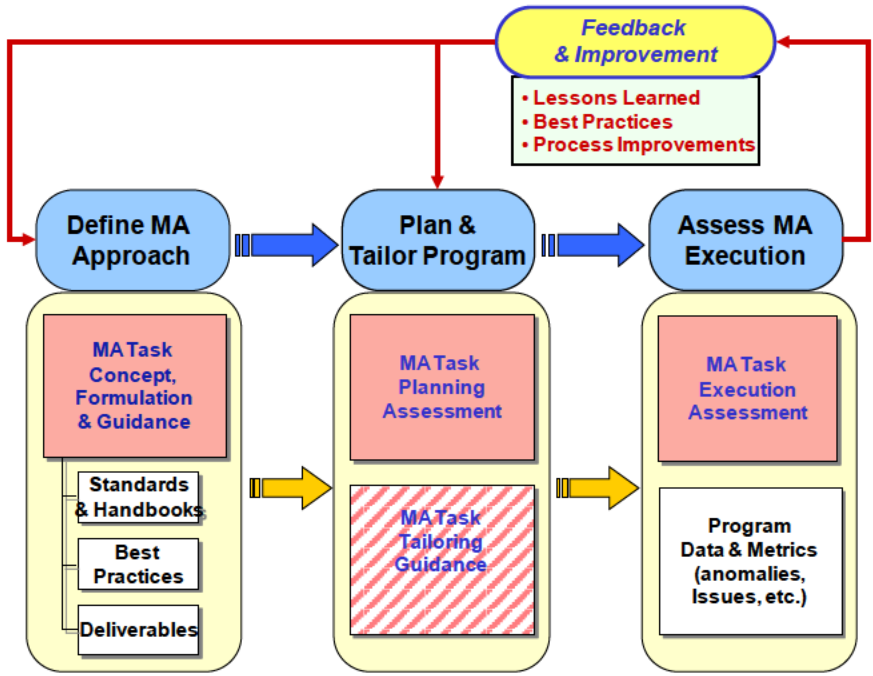


Figure 2-2. National Security Space Mission Assurance Model

2.4.3 Mission Assurance Verification

MA for a particular PO is the process that the program uses to verify that the system developed is able to perform the intended mission. An integrated engineering-level assessment of analysis, production, verification, validation, operation, maintenance, and problem resolution process is performed over the life cycle of a program by which an acceptable level of risk is determined in the delivery of the intended capability in an intended environment. The objective of the assurance process is to identify and mitigate design, production, and test

deficiencies that could impact mission success. Aerospace has created the MAB as a tool/resource to be used for this process. As described in Section 2.2, the MAB is a configuration-controlled set of tasks performed to increase confidence toward the goal of achieving mission success. This "super-set" of MA tasks includes all the MA core processes and supporting disciplines detailed in this guide as well as tasks derived from specifications and standards, lessons learned, best practices, government instructions, and other baseline technical command media. The MAB is itself considered baseline technical command media and can be used as a tool while doing a program assessment of risk.

Each PO should produce a tailored set of tasks that is believed to be practically executable within the scope and constraints to meet the specific needs of that program. Tailoring includes eliminating those tasks that are not applicable to that particular acquisition (e.g., non-applicable payload) and/or not consistent with the particular phase of the program. A particular program then creates a customized set of PO tasks. The task plan could be included as an appendix or supplement to the MAP. The customized PO task plan is then used to do program assessments and assess MA risk (see Figure 2-3). Lessons learned and changing technology are examples of feedback that may drive updates to the MA Baseline (MAB) or appropriate specifications and standards in a controlled continual improvement process.

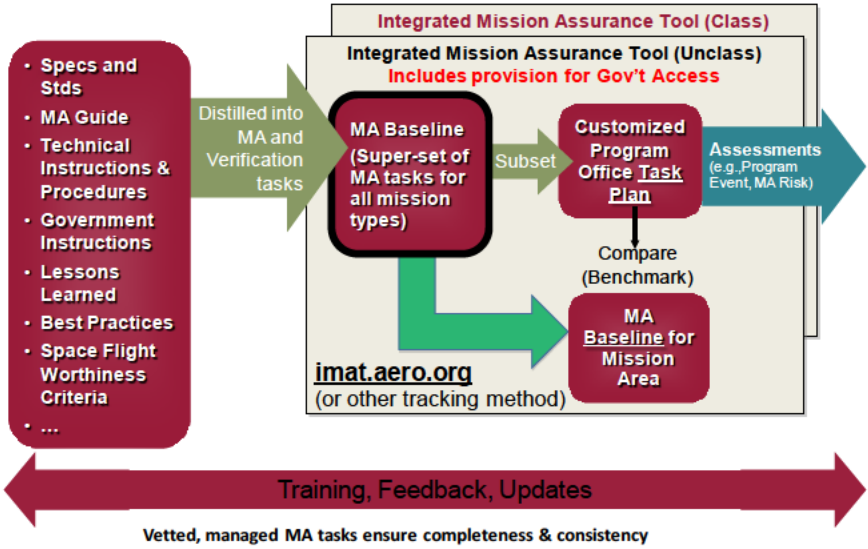


Figure 2-3. Mission Assurance Verification

The PO, with engineering matrix support, selects and tailors tasks from the MAB within program constraints. Justification for tailoring and acceptance of residual risk should be documented. The program-specific tasks are then assigned to responsible engineers for execution, establishing accountability on a task-by-task basis. Accountabilities accepted by Aerospace relative to the specific space program, launch campaign, or grounds system fielding and the activities to be conducted by the PO with engineering matrix support in the execution of those accountabilities can be documented using this approach. The integrated Mission Assurance Tool (iMAT), described in Section 2.3, or other another database tool may be used to track execution and completion of tasks.

The program task plan should be consistent with allocated program office resources, the documented risk tolerance, and agreements with the customer. The PO should also revisit the required reporting points detailed in the MAP to ensure appropriate and adequate resources are in place to execute in accordance with the documented plan. As the MA program is executed, and the MA tasks are worked off and closed, an assessment of closure should be conducted to qualitatively describe any residual risk associated with that task execution/closure that may be associated with the level of MA oversight, the risk acceptance, and/or the remaining technical risk. Evidences that support the task closure are recommended to be stored in a central records retention area for the PO.

2.5 Mission Assurance Execution in the National Security Space Acquisition Cycle

The execution of PO activities can be managed through the use of the iMAT. iMAT serves as host to the codified MAB that spans the entire program life cycle. The most current version of MAB serves as a benchmark to programs executing their own tailored versions. iMAT is intended to enhance the consistency of MA application and, where applicable, verification as well as facilitate appropriate consideration of risk in decisionmaking. The tool enables appropriate customizing per level of MA accountability, mission type, and vehicle class. Identification of content for life cycle readiness assessments for significant program events and resource distribution are key features in the tool. iMAT is not intended to perform program management functions in terms of program schedules, cost, or auto-calculate manpower levels. The tool does not replace or constrain necessary sound engineering judgment required in the course of executing MA tasks. The primary goal of the tool is to facilitate communications and transparency, accommodating participation by all the relevant stakeholders and collaborating organizations.

2.5.1 Acquisition Cycle Phases

Section 2.5 provides an introduction of the NSS system and program acquisition phases that define the broad context within which the execution of MA is articulated. Basic sequential MAG phases cover the full acquisition cycle of an NSS system and correspond to phases defined in current DODI 5000.02[13] as detailed below. These basic program acquisition phases are identified in Table 2-1 and are listed below for ready reference. The MAG phases were originally established in 2007 and baselined in Aerospace curriculum. In parallel the MAB was developed and MA tasks were defined in accordance with the MAG phase definitions. The phases as defined present unique MA tasks that are phase specific.

Table 2-1. Mapping of MA and Technical Program Phases to DOD Acquisition Phases

Program Technical Phase	Within-Phase Program Execution Milestones	Concluding Program Execution Milestone	MAG Phase	DOD Acquisition Phase	Within DOD Phase Acquisition Milestones	Concluding Milestone Decision Authority Milestone
Requirements and Concept Definition/ Acquisition Planning	N/A	N/A	**Phase 0 Concept Studies**	Material Solution Analysis	N/A	Milestone A
			Phase A Concept Development	Technology Development	N/A	Milestone B
System Definition	SRR	SDR	**Phase A Concept Development**	Technology Development	N/A	N/A
Design and Development	PDR	CDR	**Phase B Preliminary Design**	Engineering and Development	N/A	N/A
			Phase C Complete Design	Engineering and Development	N/A	Milestone C
Production, Integration and Test	N/A	N/A	**Phase D1 Fabrication and Integration**	Production and Deployment	N/A	N/A
Deployment, Test and Checkout	N/A	N/A	**Phase D2 Fielding and Checkout**	Production and Deployment	Full-Rate Production Decision	N/A
Operations and Sustainment	N/A	N/A	**Phase D3 Operations and Disposal**	Operations and Support	N/A	N/A

- **Phase 0**, Concept Studies (corresponds with Pre-Milestone A, Materiel Solutions Analysis.)

- **Phase A**, Concept Development (corresponds with Pre-Milestone B, Technology Development. Includes program requirements and concept

[13]DODI 5000.02, Operation of the Defense Acquisition System, 8 December 2008.

definition in the acquisition planning stage of system definition that incorporates system requirements review program execution milestones)

- **Phase B**, Preliminary Design (corresponds with Engineering and Manufacturing and ends after satisfaction of completion of the preliminary design review)

- **Phase C**, Complete Design (corresponds with Engineering and Manufacturing and ends after satisfaction of completion of the critical design review)

- **Phase D1**, Fabrication and Integration (corresponds with Production and Deployment)

- **Phase D2**, Fielding and Operation (corresponds with Production and Deployment phase and may include a full-rate production decision)

- **Phase D3**, Fielding and Operation (corresponds with Production and Deployment phase)

NOTE: The Defense Acquisition System was created in 1971 by Defense Secretary Packard and defined in DOD 5000.1. This instruction established the Defense Systems Acquisition Review Council that defines decision point and phases as applied to major program acquisitions. The policy has changed 16 times in the past 40 years to include as few as two milestone decision points (1982 to 1985) to as many as seven milestones (2008). As of October 2011, there are three milestone decision points (A, B, C) and five phases (Material Solution Analysis, Technology Development, Engineering and Manufacturing Development, Production and Deployment, and Operations and Support). The relationship between the acquisition phases and system milestones (SRR, SDR, PDR, CDR) has also changed numerous times. The acquisition policy has changed twice since the MAG phases were originally defined in 2007 (intended to align with then DOD policy).

2.5.2 Program Office Technical and Mission Assurance Guide 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, Table 2-1 provides a mapping of traditional technical and MA execution phases into the acquisition phases referred to in DODI 5000.02.

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 MAB task database.

2.5.3 Phase-Dependent Organization of Mission Assurance Tasks

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

2.5.3.1 Organization of Core Mission Assurance Processes Tasks

The core mission assurance processes (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 MAB task database, with a 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.

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 Table 2-2.

Table 2-2. Core Mission Assurance Processes

Core MA Processes	Chapter
Program Assurance	4
Requirements Analysis and Validation	5
Design Assurance	6
Manufacturing Assurance	7
Integration, Test, and Evaluation	8
Operations Readiness Assurance	9
Operations and Sustainment	10
MA Reviews and Audits	11

The program phase dependence of an 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 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 Phase B (preliminary design) and 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 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 Mission Assurance 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 framework activity areas. These, at the top level, are intended to group together tasks that pertain to the following types of activity:

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

- **Systems Engineering.** The systems engineering group defines those tasks within a given CMP intended to ensure the integrity of requirement, design, and operation provisions that address SOS 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 standard tasks that originally have been defined and functionally organized under the parallel framework of supporting MA disciplines (SMDs).

- **Hardware/Software Product Oriented.** 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 framework structure. The generalized framework used in this guide is, for the practical purpose of defining product-oriented subtasks, not developed further than the subsystem level (i.e., the level directly above the unit level).

Figure 2-4 illustrates the space segment hierarchical organization of tasks within a generic CMP and acquisition phase, reflecting the above discussion. The definition of generalized framework levels depicted in the table is partly modeled after MIL-STD 881C, “Work Breakdown Structures for Defense Material Items.”

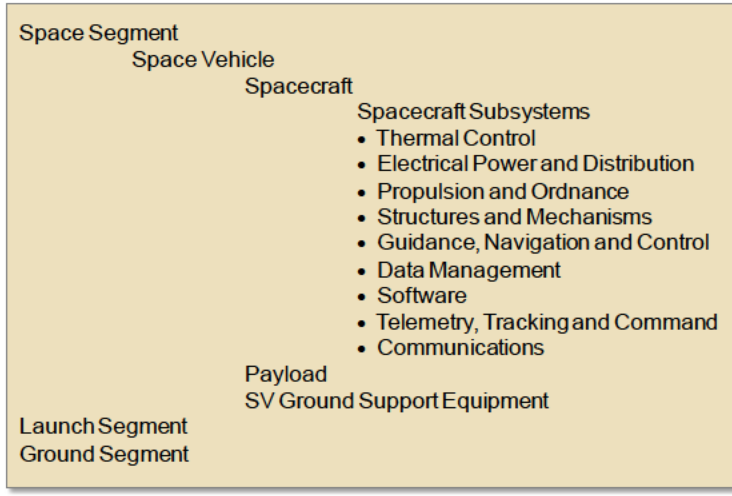


Figure 2-4. Hierarchical Organization of Task within a Generic MA Process and Phase

2.2.3.2 Organization of Supporting Mission Assurance Disciplines Tasks

As discussed 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 SMDs included in the MAG task structure are listed below:

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

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 interrelated, contexts:

- 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 Supporting Mission Assurance Discipline Tasks in Standalone Mission Assurance 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 subprocesses 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 Supporting Mission Assurance Discipline 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.

Generally speaking, and according to the established practice of the aerospace industry, the MA discipline tasks will usually be inserted under the systems engineering task header (see Figure 2-4). 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 framework 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.

2.5.4 Government and Contractor Input to Mission Assurance Tasks

A significant fraction of the tasks documented in the MAB task database concerns assessment, validation, and/or verification by Aerospace and other MA-dedicated (e.g., systems engineering and technical assistance [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.

2.5.5 Tailoring of Mission Assurance Process Executions

The definition of MA processes in terms of the task structures documented in the MAB is intended to be as comprehensive and as general as possible. The MAB will always 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 MAB task database that support program-specific tailoring can be found in Section 2.6.1.

The MAB is applicable to all space mission types across all acquisition and mission phases. The MAB is based on mission success guidance found in specifications and standards, policy and other guidance, PO experience, subject

matter expertise, industry best practices, and lessons learned. The MAB is comprised of MA tasks that include review of contractor products, assessment of contractor and government products and process, and performance of independent analysis. The baseline is relevant, actionable, and customizable, but not all tasks are applicable to all programs, therefore tailoring is required.

The MAB provides a common set of MA tasks that all programs can draw from, providing for better consistency in application of MA practices across the enterprise. Each program is required to tailor the complete set of MAB tasks based on their mission type, risk posture, level of mission assurance accountability, and other factors at the decisionmakers' discretion, all which should be captured in the MAP.

2.6 Use of the Mission Assurance Baseline Task

Besides being a comprehensive repository of MA process and task guidance and information, the MAB serves two complementary practical uses:

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

The practical use of the database is made possible by the associated software tool, iMAT. After the user enters the database using the associated software tool, there are several choices for viewing the organization of tasks and associating them with specific elements in a program framework structure. The association of SMD tasks with CMP tasks, and of either type with the programs defined framework elements is then considered as part of the tailoring process.

2.6.1 Mission Assurance Baseline Framework and Task Structure

The MAB framework is the hierarchical structure (which can be also thought of as a tree or folder structure) around which the MAB tasks are organized. Tasks are populated within and throughout the various folders of the framework. The MAB is organized as such so that programs can readily identify MA tasks that may be applicable to their program. Rather than use the MAB framework for tracking MA task execution, programs are encouraged to establish their own framework in terms of what makes sense to organize the functions, activities, and business processes unique to their program. Some areas of the framework may not be applicable to a particular program due to the mission or phase of that program. Figure 2-5 is an example of an excerpt of the framework from MAB Version 2.3.

A MAB task is defined as an MA activity that is performed by the PO or engineering. The task is performed to enhance the overall likelihood of mission

success, and may actually be performed by Aerospace, the government, another FFRDC, or a support contractor. In general, a MAB task itself is not performed by the contractor.

MAB tasks are organized in a basic hierarchy as "Level 1" and "Level 2" tasks. Level 1(L1) tasks are high-level overview assessment tasks. The following are examples of L1 tasks: Assess Attitude Control System (ACS) Design; Assess ACS Verification Planning; and Assess ACS Analyses. Level 2 (L2) tasks are more detailed, actionable tasks that are used to ensure completion of a particular L1 task.

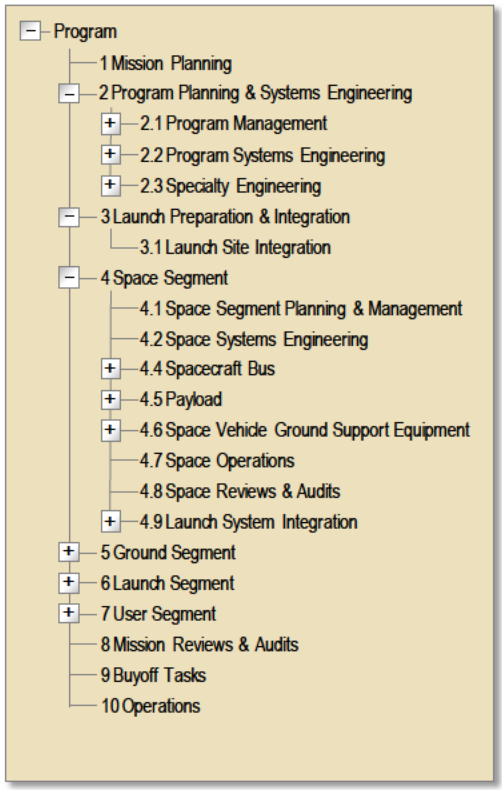


Figure 2-5. Framework Excerpt from MAB V 2.3

For example, in order to “Assess the ACS Design” (L1 task), there are a number of L2 tasks that would need to be completed. Listed below are just two of 21 L2 tasks that ensure completeness of L1 task (Assess the ACS Design):

- “Ensure that the safe mode design satisfies criteria established and that test plans are in place to verify the fault protections”
- “Ensure ACS pointing error budget and margins are established with adequate detail to track performance for each operational mode”

Although more detailed than the L1 tasks, the L2 tasks are not intended to be entirely standalone or comprehensive in detail. The MAB tasks are not a how to guide or a substitute for a particular specification or standard, but are intended to be a reminder of the set of activities that need to be completed to ensure comprehensive and consistent MA practices are applied.

Phase information indicates the acquisition life cycle where the task should be performed and completed. The phases in the MAB directly reflect the phases as defined in this Guide: 0 (Concept Studies), A (Concept Development), B (Preliminary Design), C (Complete Design), D1 (Fabrication, Build, and Integration), D2 (Fielding and Checkout), and D3 (Operation and Disposal). The task description field is often included to provide additional information that describes specific attributes of the task and/or briefly describes the different activities expected to be performed at the different phases or milestones. A task reference field is similarly populated to include one or more source references that a user can consult for further information. The references may include policies, practices, handbooks, specifications, standards, or reports.

Figure 2-6 provides an example of the L1 and L2 task hierarchy for a particular L1 task, “Assess ACS Design.” This particular L1 task is comprised of 21 separate L2 tasks (four are shown in the graphic). The graphic also shows how the phase information, the description, and the reference areas are captured for L2 tasks.

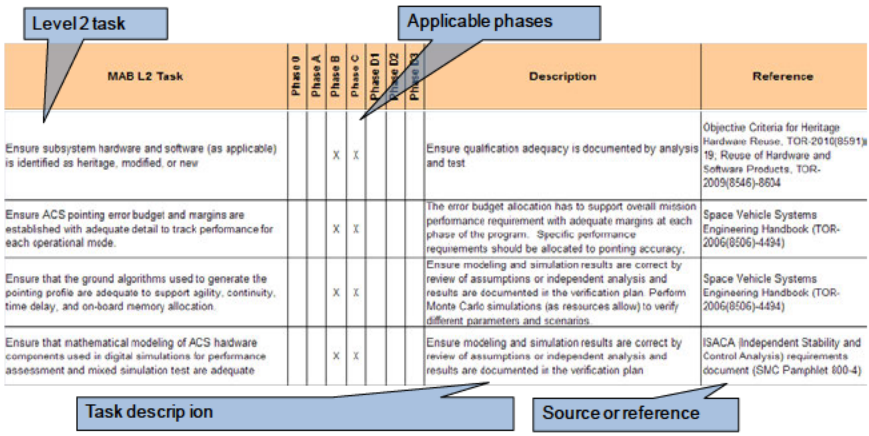


Figure 2-6. Level 2 Task Details in the Mission Assurance Baseline

2.6.2 Mission Assurance Baseline Tailoring Methodology

There are essentially four major steps to creating a program-unique task plan. The first step is to collect, review, and create appropriate program MA documentation. Step 2 (develop a program framework), step 3 (develop a task plan by tailoring the MAB tasks), and step 4 (deploy in software tool to track and monitor task completion) are described in more detail in this section.

2.6.2.1 Review and Create Program Mission Assurance Documentation

Existing program documentation should be reviewed, assessed, and referenced during the planning process. The program document of most interest is the MAP that details the risk posture, compliance documents, resource, and accountability agreements with the customer. Applicable policies, instructions, and other command media (the MAG) should be reviewed to ensure the best way forward to meet program requirements.

2.6.2.2 Develop the Program Framework

As indicated in the previous two sections, the MAB is composed of: (1) the framework and (2) the tasks. The MAB framework is a generic structure intended for task organization, and is often not suitable for effective program execution for a particular program.

The first step to create a unique program instance, a program-specific MAB or task plan, is to create a framework that best represents the program. The program framework may be a tailored version of the MAB, or a tailored version

of the contractor's work breakdown hierarchy, or other. Best practices today by programs have found a combination of the MAB framework in consideration of the PO's organizational structure works best to organize and assign tasks within that PO. The organization should consider the management functions and accountabilities within the staffing of the PO.

2.6.2.3 Develop a Task Plan (Tailored Mission Assurance Baseline)

This step is best approached by first surveying the baseline to assess relevant tasks for the program. The actual task tailoring is best achieved on the spreadsheets. A recommended best practice is to note the reason why certain sections of the MAB are excluded from the program baseline. For example, the tasks may not be considered for the following reasons: Not applicable to this phase of the program (i.e., program may be in Phase C of the program and tasks in 0, A, B are not applicable); non-mission area (i.e., non-applicable payloads). Tailoring at this level is conducted at a top level with little required resources.

Once the initial filtering of the MAB is complete, the final tailoring can be conducted. Considerations include resolution of perceived overlap of accountabilities with other functional areas as specific task responsibilities are assigned to specific organizational areas. Equally important is the consideration of accountability for specific sets of tasks (i.e., is Aerospace accountable?), and if there are adequate resources to execute. Again, a recommended best practice is to capture with a short note why MAB tasks are not included in a specific program's tailored task plan (i.e., outside defined accountability; not funded; or not consistent with risk posture of program). Once L1 tasks are accepted there may be additional tailoring of the L2 tasks to include addition of unique program tasks. A final review should be conducted of the task plan in consideration of the program milestones and definition of internal evaluation/review dates of the selected tasks. Experience has shown that the tailoring process must include the entire program's management staff to ensure appropriate accountabilities are assigned to the applicable PO functions.

2.6.2.4 Deploy the Program Task Plan

Implementation of the task plan should include deployment that includes a way to track and monitor completion of tasks as accepted by the PO. The iMAT tool provides that ability and as well as many other functionalities such as creating unique reports. Part of the deployment process will be to determine the appropriate evaluation points (e.g., Aerospace President's Review) for the mission. Engineers perform assessment of the task, and manager's review and concur on task closure. This is a continual process as products are developed and delivered.

2.6.3 Assessment of a Mission Assurance Baseline Task

Initial planning for MAB task use and assessment is considered in concert with the MAP. The MAB tasks will reflect the accountability of the program with an initial resource plan. The initial resource plan should indicate if the task is planned to be performed, which will reflect the accountability for those tasks and at what level in terms of man hours. Furthermore, the planned effort should include a rating (green, yellow, or red) as to sufficiency of the planned vs. the funded effort. This resource plan should be revisited as the MAP is updated to reflect levels of effort consistent with that plan.

At the core of assessment usage of the MAB task is the responsible engineer's participation in an individual task. The iMAT tool specifies six different levels of participation (depth of effort) planned for their execution within a given program execution plan: none; maintain awareness; review and comment; review and analyze; analyze and assist; and full and independent analysis. This participation should reflect the assigned accountability for the MA task and is considered in the final residual risk assessment prior to task closure.

The combination of the MAP, the resource plan, and planned participation ratings produces a set of "MAP risk" ratings that serve as MA verification of the tailored set of tasks related to core MA processes and supporting MA disciplines. The process considers the total risk of the program, considering the constraints of cost and schedule, and ensures formal reviews validate and document risk-mitigation tactics. In this use of the database, "MAP risk" signifies the potential for future impact on program execution that may result from the participation 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 "MAP risk" ratings can be used to negotiate and adjust the programmatic level of effort planned for the execution of Aerospace MA tasks and activities. MA activities must be tracked against the program baseline and red flag indicators put in place to immediately identify baseline deviations.

Additional detail regarding evaluation of residual program risk using the MAB is offered in the next chapter of this handbook.

2.7 Summary

The MAB database is expected to evolve over time. Thus, the examples provided here are to be considered notional illustrations.

2.8 References

Policy-Related

DODI 5000.02	Operation of the Defense Acquisition System, 8 December 2008

SMC FFRDC Users Guide, 20 January 2004

Specification and Standards

MIL-STD-881C	Work Breakdown Structures for Defense Materiel Items, 3 October 2011

Best Practices

TOR-2011(8591)-5	Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles, 13 September 2010
TOR-2011(8591)-21	Mission Assurance Guidelines for A-D Mission Risk Classes, 3 June 2011

Other

ATR-2012(9041)-1	Mission Assurance Baseline Version 2.3, 30 April 2012

Chapter 3
Mission Assurance Evaluation and Assessment

Sergio B. Guarro
Systems Engineering Division

3.1 Introduction

The preceding sections of this guide introduced the basic principles and tenets of mission assurance (MA) and the associated MA Baseline (MAB) task database, providing an overview of the overall framework and associated 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, is under the general heading of MA evaluation and assessments, tackles the subject of measuring and assessing the quality of MA planning and program execution.

The ultimate and most objective metric of successful MA planning and execution is the degree of mission success achieved by an organization over the years and over a range of acquisition programs. Unfortunately, this is not a headlight metric and thus provides information with an intrinsic time lag. This makes it difficult, if not altogether impossible, to use such information to make effective corrections to achieve MA improvements before it is too late to influence the outcome of a specific acquisition program. It also limits its usefulness for shaping and evaluating MA plans that are in the process of being formulated for upcoming programs.

Because of the above, the estimation of the effectiveness and quality of MA plans and program execution must often rely on projections and indications that are supported by incomplete information and, by necessity, rely on some significant degree of subjective judgment on the part of the assessor. Despite this, any metrics used in the evaluation process should still be chosen to be as objective as possible in their formal definition. That is, any such metrics should be selected on the basis of the correlation value they are believed to have with respect to the MA quality dimension that is being evaluated or predicted, even though the actual assessment of such metrics may ultimately rely to a significant extent on the subjective judgment and experience of the assessor.

The sections that follow explain the basic nature, logic, and practical foundation of metrics that may be used for assessment of the MA planning and program execution activities addressed by this guide. The focus of a program office (PO) user is most likely to be on the practical application part of the materials provided in the following. To provide the foundation for a successful practical

implementation of the related guidance, it is useful, however, to precede the related topics with discussion that defines the objectives and technical principles of typical MA assessments that are of interest in a program context.

According to the above, and to facilitate the reader's comprehension and use of the subjects discussed in the chapter, these are organized according to the following order of presentation:

1. Types of MA assessments that are typically included in national security space (NSS) program objectives (Section 3.2)

2. Key concepts applicable to the use of risk metrics in MA assessments (Section 3.3)

3. Guidance applicable to execution of MA assessments of interest to NSS programs (Section 3.4)

3.2 Types of Mission Assurance Assessments

In the context of the national security space (NSS) program MA activities that The Aerospace Corporation (Aerospace) supports, all MA assessments support the ultimate objective of mission success. However, not surprisingly given the time and scope of most NSS acquisition programs, these assessments may, at different points of development and execution of a specific program, take different forms and have somewhat different immediate purposes. From a practical point of view, a simple classification that reflects the practices implemented by most Aerospace program offices can be based on two basic elements that characterize the objectives of an assessment:

1. **Phase discriminator.** A differentiation of the MA assessment on the basis of whether it is carried out for MA planning purposes or execution assessment purposes.

2. **Object discriminator.** A differentiation of the MA assessment on the basis of whether the object of the MA assessment is the evaluation of an MA task (or set of tasks defining a super-task or process), or the evaluation of the MA attributes of a given system-item (such as a spacecraft component or subsystem).

A discussion of the types of MA assessment that reflect these characteristics is provided in the subsections that follow. Before delving into the related details, it is appropriate to point out that:

- The nature of an MA assessment is usually determined by combination of the two characteristics identified;

- Many MA assessments can also be hybrid with respect to the object discriminator. For example, an MA execution assessment may seek to assess both a task-set in terms of their MA process attributes, and a system-item or group of items in terms of their MA product attributes.

3.2.1 Mission Assurance Plan and Execution Assessments

From the point of view of the evaluation objectives associated with the early vs. later phases of an NSS program (with reference to what has been referred to above as an MA phase discriminator), an MA assessment may be sought for planning purposes, or for the purpose of evaluating the quality of execution of MA tasks once they are completed. These two types of assessments are respectively referred to in the following as an MA plan assessment (MAPA) or an MA execution assessment (MAEA).

A MAPA evaluates the projected effectiveness of a program's planned set of tasks prior to execution, primarily on the basis of the planned breadth and depth of manpower support to execute the tasks. The objectives of this type of assessment are as follows:

- Evaluating the breadth and depth of resources allocated in the MA program plan toward the execution of different types of MA tasks and activities, with the underlying objective of ensuring that highly important (i.e., critical) areas and items receive sufficient support and dedicated resources.

- Establishing and documenting the program-tailored baseline of allocated MA resources, so that both the federally funded research and development center (FFRDC) providers of MA services and their government customers recognize an agreed-upon level of effort in each MA area of interest.

An MAEA is conducted upon or after the completion of MA program tasks, on the basis of the technical and specific indicators of the quality and thoroughness of the actual execution (e.g., the satisfaction of task closure and the resolution of any technical issues). The practical objectives of this type of assessment include the following:

- Evaluating the thoroughness and quality of MA task execution and ensuring that highly important (i.e., critical) areas and items have received sufficient support and technical attention.

- Assessing the level of residual risk remaining in the 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)].

MAPA and MAEA assessments will be addressed again in Section 3.4, from the perspective of recommendations that are applicable in practical contexts, consistently with the technical principles and guidelines that are discussed in Section 3.3.

3.2.2 Mission Assurance Task and Product Assessments

As mentioned in Section 3.2, the other principal factor by which an MA assessment can be characterized is whether its focus is on evaluating MA tasks on the basis of their process attributes, or more specifically the MA attributes of a system product (i.e., the attributes of an actual component or subsystem of the system designed to execute a NSS mission). This distinction must not be interpreted as being one of mutual exclusion (i.e., to imply that a task-oriented evaluation must necessarily exclude any consideration of the resulting system product[s], or vice versa). MA tasks are applied for the purpose of achieving MA goals related to the resulting attributes of a system item. The evaluation of such tasks from a process perspective is usually just the first step of an MA assessment which is to be completed by the evaluation of the product attributes of that item.

While the above remains generally true, the object discriminator distinction is nevertheless useful in practical terms, because many MA tasks are initially defined in the MAB and in associated software tools in non-product-specific terms. Such tasks are defined as processes applicable within broad program areas and, as such, their definition is not provided in terms of a specific application to a particular system component or subsystem. Given the broad nature of such tasks, in certain contexts, and especially in the early planning stages of MA program definition, a related evaluation may be conducted from a broad perspective, and not necessarily be focused on the attributes of system products to which the tasks are eventually applied.

3.3 Risk as a Metric for Mission Assurance Assessments

The MAB supports the expression of MA quality in terms of risk, and a risk statement is the preferred way of summarizing an MA assessment carried out by an Aerospace PO. Somewhat different types of MA-related program or mission

risk evaluations can be pursued, depending on the phase and focus characteristics of the MA assessment.

Reflecting the MA phase discriminator distinction, two typical kinds of assessment that are articulated in risk terms are:

- A MAPA risk evaluation is the assessment of the level of risk that can be predicted, on the basis of the level of MA resources and activities that are planned by a program, relative to the standard represented by the full set of MA tasks identified by the MAB.

- An MAEA residual risk evaluation is an assessment of the residual level of program and mission risk that may remain, after the execution of the planned MA tasks and activities, as a result of issues in the execution of such tasks and/or the occurrence of adverse factors.

The above two basic types of risk and any associated metrics will be referred to as “MA plan risk” (MAPR) and “MA residual risk” (MARR).

The distinction between plan risk and residual risk only provides a partial definition of an assessment. This is because the nature of the risk to be used as an MA metric remains undefined if a corresponding identification of the type of outcomes that are of concern to a stakeholder and/or assessor is not provided first. For example, an assessment of risk in terms of potential mission execution impact will be different, qualitatively and quantitatively, from an assessment in terms of potential program cost or schedule milestone impact. This is further discussed in Section 3.3.1, and then again in Section 3.4 in the context of the guidance provided for execution of different types of MA assessments.

3.3.1 Outcomes and Events Defining Mission Assurance Risk

From an evaluation perspective, most assessments of risk are based on the complementary dimensions and composing factors of likelihood and severity of consequences. In more fundamental qualitative terms, risk always refers to the possibility that certain events may occur with outcomes bearing negative consequences for certain affected stakeholder(s). Thus, an evaluation of risk cannot be carried out or communicated meaningfully without first identifying and defining the specific negative outcomes that are of concern. Once this is accomplished, risk ratings and formulations based on the likelihood and consequence parameters can be applied (i.e., risk can be rated in terms of the likelihood of a certain type of outcome of concern and of the severity of the negative consequences directly associated with that outcome).

In the NSS context the program stakeholders are concerned with program and mission outcomes, thus risk-relevant events and consequences of concern here are those that may negatively affect a program or mission execution. Mission success is the primary goal of MA activities, and any possible shortfall with respect to the desired level of mission performance constitutes an undesirable outcome and a corresponding MA risk. At the same time, MA issues may also have cost and timeliness effects of high concern to an NSS program, thus these programmatic dimensions of risk may also be an important part of an MA plan or execution assessment.

When applied in the quantitative domain, and when the type of consequence of concern to stakeholders is clearly identified and defined, the risk concept is translated into the evaluation of a probability of occurrence and a magnitude of consequence severity for the outcome(s) of concern. The combination of these metrics provides a measure of risk that can be defined in objective terms and is, at least in principle, quantifiable. The discussion of MA-related risk in this guide follows these standard tenets. The MA risk terminology and formulation may, where necessary, be adapted to the partially qualitative nature of the context within which MA-related risk is to be assessed, and of the related information.

While the principles just discussed for the use of risk metrics as indicators of MA quality are generally valid, differences also arise when considering risk in contexts that cover the range spanning from the assessment of tasks to that of products and system components. These differences can be better understood by defining in more precise terms the type of risk to which an assessment refers, or, more specifically, the nature of the unfavorable outcomes and consequences that are to be prevented by the application of MA tasks and measures.

The negative events of concern may be generically described as events that produce shortfalls or deficiencies in key attributes of the object of the assessment, regardless of whether the latter is an actual system component or an MA task process. Types of negative events that are of utmost concern in the overall MA context are those capable of producing a shortfall in mission performance as a direct consequence. In a risk evaluation, the immediate effects of most MA shortfall events, and especially of those events concerning tasks and processes rather than actual system components, are usually quite removed from an actual mission impact. The occurrence of one of these events indicates that a mission impact is perhaps a step closer than if the event had not occurred, but the observation of such an occurrence cannot by itself be directly equated with high risk. Accordingly, the presence of task attribute shortfalls, and even of system component ones, can be viewed as a symptom of risk, but is not a direct indicator that the risk level is high in mission impact terms.

3.3.2 Mission Assurance Task Relation to Mission Risk

Risk in terms of mission execution impact (i.e., mission underperformance or failure consequences) is used for illustration of the technical principles introduced in this section, given the generally understood relevance of a mission risk metric to MA goals and objectives. The risk-modeling concepts illustrated via the mission risk scenario example in Figure 3-1 remain largely valid if an MA task assessment is conducted from the point of view of cost or schedule milestone consequences, rather than mission performance ones. More direct evidence of this is provided in Section 3.4.

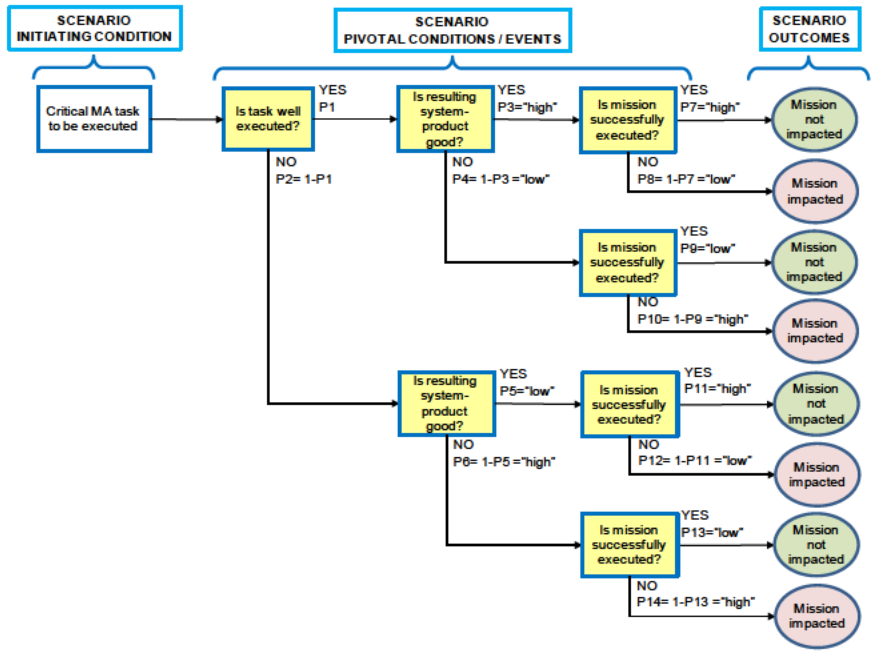


Figure 3-1. Conceptual Model of MA Task-Related Mission Risk

Figure 3-1 depicts an MA task-related risk scenario in a binary logic event sequence format. This representation constitutes a very simplified model of a typically complex actual condition, since it reduces event outcomes that may more realistically be defined as shades of gray to yes or no binary conditions. The whole scenario shown in the figure is driven by an MA task that is depicted as being critical, whereas such a task, like any other MA task, may have a varying degree of criticality and importance towards the achievement of some specific system MA objectives. The next event in the sequence reads "Is task well executed?" and implies again either a yes or no answer. In principle an

actual task outcome may be described on a continuum, within a range varying in value between zero quality and some maximum possible quality.

The simplified binary representations of the figure are a relatively crude model of reality, but illustrate the basic steps of a thought process that an MA evaluator can apply to identify and correctly represent the relation between MA task risk factors and ultimate mission risk. The ability to represent this relation in understandable and defensible terms is particularly important because the format recommended in Aerospace's assessment and reporting of risk in the context of the APR or the Aerospace Senior Management Review (ASMR) uses mission risk and mission performance shortfall as the outcome frame of reference and consequence severity metric. Additional details and discussion of the risk are documented in a supplementing Aerospace Technical Report.[14]

Three MA risk assessment focal points are identified to provide a general perspective to the assessment of MA task risk. These focal points also define a streamlined thought process that an assessor can apply to identify (and communicate) key factors and elements of MA risk.

1. Define Risk

   When using risk as a metric of MA, it is important to correctly identify and define the specific risk scenario outcome(s) with respect to which risk is being assessed. In the past it has been a common practice to refer to the risk of an MA task and give the task a risk rating or color (a green, yellow, or red coloring of the task) to express associated risk. The use of such a practice without further specifics is not recommended because the risk ratings produced in such a fashion refer to risk outcomes that remain undefined and often subject to incorrect interpretations.

   This can be understood by referring to Figure 3-1 and noting that, although the outcome of a critical task not being well-executed is not a desirable event and is a legitimate MA concern, other downstream events determine whether an actual program or mission impact will result. Whenever using a risk statement or metric for MA assessment or other related purposes, it is necessary to provide a clear answer to the question: risk of what? Any risk statement and associated metric should be formulated and defined in a way that makes clear what risk outcome they refer to. An assessment of MA risk in terms of mission performance defines a context that is distinct from that of an assessment in terms of program execution milestone impacts such as

[14]"Mission Risk Assessment Process and Techniques for APR," ATR-2012(9012)-1, Version 1.0, October 16, 2011.

cost or schedule. Besides being distinct from one another, any type of macro-level risk, such as the risk of mission performance impact or of program cost or schedule milestone impact, is very different even in mere qualitative terms from the risk of unsatisfactory output of a single MA task.

2. Identify Key Risk Factors and Events

Once the risk outcome(s) of concern are identified and defined, it is equally important for evaluation or assessment purposes to identify the principal factors and/or events that are deemed to have a significant effect on the likelihood and severity of such an outcome. The nature and definition of these events and factors is strictly related to the nature of the risk that is of concern. The risk scenario events in Figure 3-1, which correspond to basic risk questions that need to be answered to assess the likelihood of mission impact outcomes, would be different if the objective were to be an assessment of the risk of program cost or schedule milestone impacts.

Figure 3-1 identifies a risk sequence format with key events and factors that, given the execution of a critical MA task, determine whether or not a mission will be successful. Depending on the nature of the assessment, the qualitative definition of such events and factors can be accompanied by an associated identification of likelihood or probability. In the binary world depicted in Figure 3-1, the scenario events correspond to the questions of (a) whether or not the task is well executed and (b) whether or not the resulting system product is good. Formally decomposing a risk scenario into key factors or events logically connected by cause-effect relationships, whose interaction determines the outcome of concern, serves the purpose of understanding and evaluating the associated risk with as much objectivity as possible.

3. Understand Conditioning Effects

Once the key risk factors that are relevant to a certain outcome are identified, the final key step is for the assessor to develop a basic understanding of how these factors affect one another in terms of likelihood and magnitude of associated effects. Even in the simplified scenario depiction of Figure 3-1 it is relatively easy to understand that the likelihood of certain factor/event outcomes may be higher or lower depending on the outcome of a preceding event. For example, the likelihood of the task of interest resulting in a good system product is clearly higher if the task is well executed. This is indicated in the figure by the qualitative statements P_3 = High and P_5 = Low, or in quantitative

terms by the assertion that $P_3 > P_5$. In a specific sequence of events or cause-effect factors which are part of a given risk scenario, each event or factor may only occur if the event/factor that precedes it in the sequence has already occurred and is true. In probabilistic language this means that the probability associated with each event is a conditional probability whose value depends on how the sequence of events has unraveled up to that point. Using again an example from Figure 3-1 and more specifically referring to the scenario sequence branching from the "YES" answer to the question "Is task well executed?" it is reasonable to assume that a positive cause-effect relation exists between quality of MA task execution and quality of the resulting system product, "Is resulting system-product good?" If this assumption is correct, the probability of a good system product outcome from the corresponding event represented in that specific risk scenario branch may also be assumed to be relatively high, and in any case higher than the probability of a similar outcome in the risk scenario branch downstream of the "NO" answer to the "Is task well executed?" event question.

The assessor decides how detailed the conceptual depiction of a risk scenario or sequence needs to be to enable a reasonable judgment of the associated risk. For example, in the depiction of Figure 3-1 one may leave out the factor/event that pertains to whether the system product is good or not. This, however, implies that in evaluating the risk of mission failure one would directly judge whether a good or bad MA task execution would translate in a high or low likelihood of mission success. Such a direct judgment or evaluation may generally be more difficult to execute without giving thought to whether a good or bad product may be produced, and without gathering information relative to the likelihood of the task resulting in such product characteristics.

A good evaluation requires careful consideration of the factors and events that may strongly influence outcomes and associated likelihoods and probabilities, and also an appreciation of the conditioning effects that some events may have on other events that are downstream in a scenario cause-effect chain. Without identifying these factors and relations, and evaluating them at least in qualitative terms, it is unlikely that a realistic conceptual model and assessment of the risk can be formulated. A brief discussion of risk attributes of MA tasks and products that are relevant in a practical assessment is provided in Section 3.4.2.

This section can be concluded with a final caveat concerning the depiction of risk scenario presented in Figure 3-1. The oversimplified binary representation adopted in the figure was for the purpose of illustrating the concepts and points discussed. In general, and depending on the level of insight and fidelity sought in the evaluation of certain risk scenarios, one may or may not be able to use

binary tree models of similar formal structure. Outcomes of events may often fall in a continuum in their measurable effects. Depending on the nature and level of fidelity sought in the evaluation of an MA-related risk metric, the evaluator may have to determine whether a qualitative awareness of the conditioning factors is sufficient for a realistic judgment, or whether a form of logic model approximation, or multi-valued and more complex, is appropriate for a specific purpose. A discussion of more complex models, such as influence diagrams and belief networks is beyond the scope of this guide. The interested reader is encouraged to consult with the cognizant experts and to refer to the abundant technical literature on these subjects.

3.4 Program Execution of Mission Assurance Assessment

The full evaluation or assessment of MA tasks in the context of an NSS program is a major endeavor for which no single detailed formula or prescription of general validity can be provided. For this reason, in seeking to provide guidance for program execution of MA assessments of a pragmatic nature, this section focuses on the discussion of (a) basic process steps that can be recognized as being generally applicable to the possible assessment objectives and contexts, and (b) technical elements of assessment that can be identified and used by Aerospace PO and engineering support personnel in a typical NSS program environment.

3.4.1 Recommended Mission Assurance Assessment Steps

The discussion addressing the use of risk metrics for MA assessment was carried out in Section 3.3 in general terms.

The major points on use of risk metrics discussed in Section 3.2 can be used in the formulation of basic steps for practical execution of an assessment contextual to more specific program needs. In this formulation, some steps (e.g., Steps 1 and 2) represent a definition and clarification of objectives and as such are of straightforward execution. The other steps usually require further definition choices to be made by users, as well as the execution of analytical activity of varying depth and complexity, in order to be carried out in a specific programmatic context.

Step 1 – Definition of MA Assessment Purpose. The objective of this step is to determine and establish the planning or residual risk nature of the MA assessment. A program will in its early phases define an MA plan by selecting and tailoring a subset of MA tasks extracted from MAB. A MAPA is then executed as a part of, and necessary complement to, this process, to provide insight into the adequacy of the MA plan and associated program-tailored set of tasks, and identify possible weaknesses and any needed adjustments. Programs

should document the accepted risk incurred by the tailoring of tasks as part of the program specific mission assurance baseline.

Step 2 – Definition of MA Risk Focus. This step consists of the determination of the mission risk and/or program risk orientation of an assessment and should be practically parallel to the completion of Step 1. While it may appear obvious that a definition of what type of risk MA tasks are to be evaluated against is necessary from assessment onset, it still occurs that generic discussions of task risk are sometimes carried out, and risk ratings even derived, before a clear definition of the actual risk outcomes of concern is formulated and established. The confusion and miscommunication resulting from this ambiguity in the use of risk language is easily avoidable if a risk focus is firmly established and defined early on. This includes the parallel pursuit of a dual focus (e.g., if a program wants to assess a formulated MA task plan from both the potential associated mission risk perspective and from the program execution perspective of potential cost and schedule milestone impact). While it is possible and useful to keep both perspectives, it should be clear that different risk factors and metrics would be of concern for the two types of assessment.

Step 3 – Identification of Risk Scenario Elements. This step involves the construction of a risk model by identification of the primary events, factors, and associated questions that are judged by the assessor to be important in determining the occurrence or non-occurrence of risk scenario outcomes. The risk model can take a formal event sequence diagram shape as in Figure 3-1, or, for situations that can be evaluated in more streamlined fashion, that of an informal list of relevant risk questions to be considered and correlated.

Step 4 – Estimation of Risk Scenario Likelihoods and Severities. Once a risk model is formally defined or informally delineated, the elements can be individually evaluated to arrive at an estimation of the likelihood and severity of the risk outcomes. These, after consolidation across the risk scenarios associated with a given set of MA tasks or products, provide the metrics by which such tasks and products can be assessed for level of quality and/or compliance with program milestones. The term likelihood includes the meaning of probability, with the caveat that the latter term is usually intended to signify a more rigorous process of assessment (estimations of likelihood are generally inclusive of judgment processes that are less formally rigorous than those applied when obeying the axiomatic logic rules of probability theory). The complexity and rigor of the estimation techniques applied in this step are at the discretion of the assessor, although of course the overall goal is to match them to the importance of the desired assessment output. At one end of the spectrum, for example, the direct judgment of whether the likelihood of a certain mission or program-milestone impact of a given group of planned MA tasks is expected to be low, significant, or high. At the other end would be the estimation and logic

aggregation of individual event probabilities concatenated by cause-effect in detailed risk scenario sequences.

Regardless of the modeling and estimation level of detail applied, the following considerations/substeps are recommended in the execution of Step 4:

1. Identification of key event likelihoods and impact severities to be estimated.

2. Identification of correlations among the above that affect the estimation of overall scenario risk.

3. Evaluation of the quality attributes of the MA tasks and or products being assessed, with respect to an MAB that corresponds to negligible risk, and of the effect that the quality level of these attributes may have on the likelihood and severity factors that pertain to the risk scenarios of concern and associated events. A discussion of what tasks or product attributes may be relevant in this regard and what general correlations that may have with the actual likelihood and severity components of risk is the subject of Sections 3.4.2 and 3.4.3.

3.4.2 Mission Assurance Baseline and Risk Scenario Elements

In the identification of MA-related risk the concept of deviation from baseline is commonly applied with regard to both tasks and products. A more precise definition is necessary to avoid possible confusion arising from different interpretations of its meaning in a practical context. For the purpose of the MA evaluations, the following definitions are adopted and assumed valid for both MA tasks and MA products.

MA Task or Product Baseline. The MAB is the ensemble of quality attributes of a task (or combination of tasks at any level), or of a product (or functional assembly of products at any level), which the responsible organization considers necessary to provide high assurance that overall system quality and mission success are not adversely impacted.

Deviation from Task or Product MA Baseline. A deviation from the MAB is a degradation in the quality attributes of an MA task or product—or combination thereof at any level, which the responsible organization judges potentially capable of resulting in an objectively measurable negative impact on overall system quality and mission performance.

The assessment of MA task and product risk can therefore be linked to the assessor's observation or projection of deviations from baseline deemed capable of producing negative system and mission impacts with non-negligible

likelihood. A deviation from a task or product MA baseline becomes a symptom or indicator of potential system quality and mission performance risk. An observed or projected deviation from MAB represents the first observable or assumed condition or event that may be followed, with non-negligible likelihood, by other conditions leading to an actual system and mission impact. An illustration of this, still simplified and presented at the level of thought process aid, is provided, for initial conditions by the risk scenario templates in Figure 3-2 and Figure 3-3, for deviations from a task and product MA baseline, respectively.

The key observation to make with regard to the two figures is that the condition questions identified in the corresponding risk sequences, downstream from the baseline deviation initiating conditions, are examples of the thought process that a risk assessor may follow to identify the additional conditions and events that represent a link between those initial indications of risk and an actual system and mission impact. In an actual scenario for a given program a full answer to the generic questions presented may require the identification/definition of more specific questions or events. The general objective would remain to identify at some level of credible definition the logic cause-effect link between an observed deviation and an actual system and mission effect.

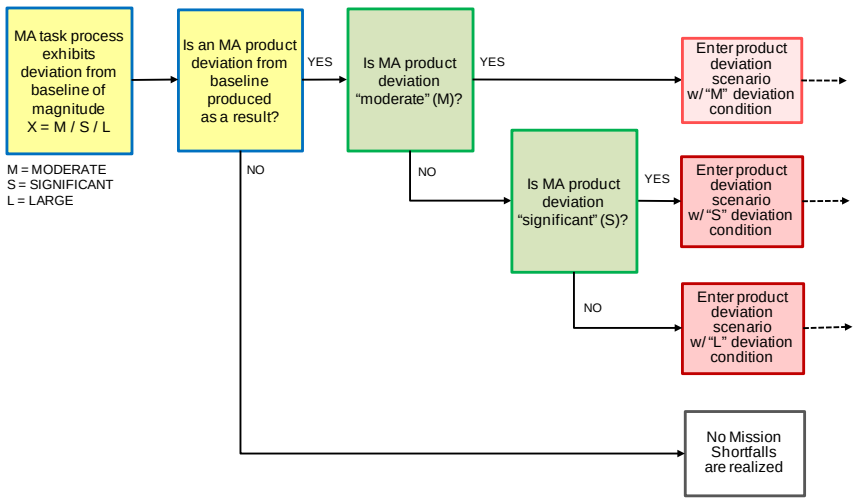


Figure 3-2. Mission Risk Scenario Template for Deviation from Task MA Baseline—Initiating Condition

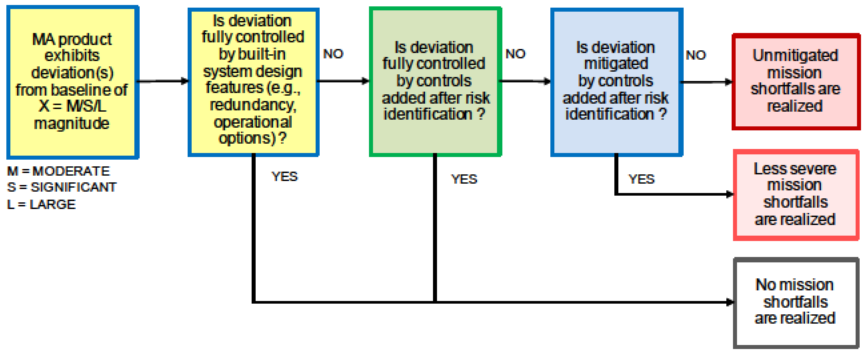


Figure 3-3. Mission Risk Scenario Template for Deviation from Product MA Baseline—Initiating Condition

If the expression of risk is intended to remain limited to less critical impact dimensions than those of mission impact, or to concern impact dimensions that are different (e.g., program schedule), this should be clearly defined and communicated. A different type of risk scenario thought process may be applicable for the assessment of MA risk in such different terms of impact, and the standard mission performance shortfall versus probability risk-map/matrix[15] would not be applicable as a risk reporting instrument.

For illustration purposes, a simple risk scenario template for a cost and schedule milestone type of impact is depicted in Figure 3-4.

The figure refers to a program milestone risk potentially related to an MA task, that may actually represent a group of related tasks, and related MA product(s). For simplicity, the example template does not break down the sequence branches according to deviation severity, although this could be done if deemed useful for the purpose of an actual assessment. The main point of this example is not to prescribe the details of a specific risk scenario representation, but to illustrate the underlying thought process. More specifically, in this case the objective is to show how the nature of the risk questions to be answered and of the associated events to be considered depends on and changes with the risk focus (e.g., mission versus program-milestone impact) of the assessment. The figure also illustrates some of the correlations that may be assumed to exist among risk parameters that appear in the scenario. For example, in the risk sequences that correspond to an assignment of insufficient resources ("NO" answer to the questions of whether MA task or product resources are sufficient) the likelihood/probability of the program milestone schedule being met without delay may be assumed to be low.

[15] "Mission Risk Assessment Process and Techniques for APR," ATR-2012(9012)-1, Version 1.0, October 26, 2011.

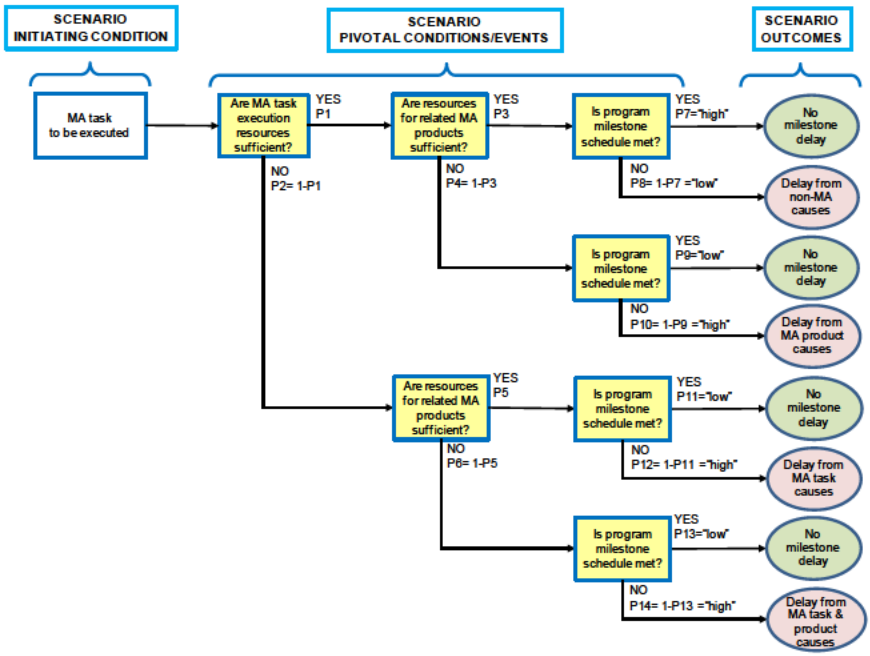


Figure 3-4. Risk Scenario Template for Cost and Schedule Milestone

No attempt will be made here to prescribe or define in detail the MAB attributes against which deviations are to be identified or measured for MA risk evaluation purposes. A corporate-level MAB in terms of tasks is defined and maintained in a database intended to constitute a general reference super-set from which individual NSS programs can derive their own tailored, program-specific baselines of MA tasks to be planned and executed. Moreover, when referring to products and system components, attributes defining quality baselines at lower levels of indenture are obviously system and mission dependent. If a lower-level definition of an MA baseline is deemed necessary to execute a specific type of assessment, a program should identify the key defining task and product attributes and associated criteria in terms of which possible deviations with respect to such a baseline are identified and assessed. To provide guidance towards this objective, Section 3.4.3 discusses some key aspects of the problem that are context-independent and yet significant for the purpose of identifying the potential relation between MA task or product attributes and risk outcomes of concern in a given assessment.

3.4.3 Mission Assurance Task and Product Attributes

It is difficult, when projecting task outcomes far into the future of an actual space mission execution, to accurately predict and describe in all details the possible evolutions of a risk sequence. An evaluation of potential mission outcomes and risk associated with MA task activities, even in qualitative form, cannot be correctly framed without a basic understanding and consideration of the principal factors that define relations of cause and effect between MA task attributes and resulting product and system attributes. This is true regardless of whether a risk assessment is conducted for MA planning purposes (i.e., a MAPA is being conducted) or MA execution evaluation purposes (i.e., an MAEA is being carried out). In the case of an MAEA, however, the availability of direct product and system quality evidence such as the results of product inspections or tests (not usually available in the planning phases when a MAPA is conducted) may make the identification and representation of cause-effect relations and correlation somewhat easier.

The considerations presented below on the potential risk-relevance of certain MA observable task and product characteristics are general in nature. They are not intended to be applied as rigid rules but simply to provide a basic reasoning aid for the wide variety of assessment that may arise in the risk evaluation of MA plans or MA execution.

- 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 usually proportional to the importance of that task. This is referred to as the task criticality, which may in turn be assessed with an associated level of criticality. For example, 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. The implications of this type of attribute with respect to risk are that the higher the level of task criticality is with respect to a desired program or mission outcome, the larger would also be any adverse consequences resulting from a poor execution of the task. This cannot be considered as a proven fact across the board in any given assessment, but should be evaluated in light of the actual type of risk being considered and expressed in terms of likelihood of various postulated levels of outcome severity.

- The likelihood of an MA task or group of tasks having the desired positive outcome and effect on program or mission is positively correlated, when evaluated at MA plan time and referring to MAPA, to the planned breadth and depth of task execution and, when referring to MAEA, to the actual breadth, depth, and quality level of task execution.

For simplicity of terminology, the former will be referred to as the task planned depth, and the latter as the task execution quality.

It should also be considered that, for evaluation purposes, a task planned depth is usually directly correlated with:

– The level of program resources allocated to the task in the task planning stages—or, in administrative language, to the staff time equivalent (STE) level planned for the task (or group of tasks)—relative to the standard level of resources believed to be necessary to execute the task correctly and successfully.

Also for general evaluation purposes, a task execution quality, as assessed after the task has been closed out, may be assumed to be directly proportional to:

– The level of effort actually applied in the execution of the task.

– The degree to which all task closure and exit criteria technically and programmatically applicable to the task (and which have been identified as such) are satisfied.

– The quality attributes (e.g., inspection or test results, if any) of the system products associated with the task.

- The level of risk that can be estimated in MAPA or MAEA terms should account for the following considerations:

  – When estimating MAPA risk level, a significant imbalance between task criticality level and task planned depth of execution is an indication of potential risk. For example, a task assessed as being highly critical for which the level of planned resources is too low would typically suggest a high MAPA risk level.

  – When estimating MAEA level, a significant imbalance between task criticality level and task execution quality is an indication of residual risk. For example, if a task assessed as being highly critical has experienced for whatever reason a low quality of execution, possibly made evident by quality shortfalls in the associated system product(s), this would typically suggest a significant level of residual risk.

3.5 Summary and Conclusions

The discussion and guidelines presented in this chapter have covered the basic principles that can be applied to enable the use of risk metrics in MA assessments. The chapter has emphasized the following important notions:

- Risk metrics can provide a flexible framework for the assessment of MA plans and MA execution.
- The basic formulations of risk models and metrics that may be applied are generally determined by the type of program or mission outcomes of concern.
- The level of risk model detail used in MA assessments can vary greatly, but no valid assessment can be executed without identifying and evaluating as objectively as possible the key elements that determine mission and program outcomes of concern.
- Useful indicators for the identification and assessment of MA related risk are provided by the evaluation of MA baselines and any possible or observed deviations of MA plans, tasks, or products from these baselines.
- MA task and product quality attributes that may serve as indicators of risk are in large part program and context dependent, however some risk-significant characteristics of such attributes are general and have been identified for consideration and evaluation in actual assessments.

In closing, it is noted that for assessments related to later-stage residual mission risk and related assurance activities the reader should compare the contents of this chapter with the more specific and detailed discussion and illustration examples contained in ATR-2012(9012)-1, “Mission Risk Assessment Process and Techniques for APR.”

3.6 References

Best Practices

ATR-2012(9012)-1, Version 1.0	“Mission Risk Assessment Process and Techniques for APR,” October 26, 2011

Chapter 4
Program Assurance

Manuel De Ponte
National Systems Group
Rand H. Fisher
Systems Planning, Engineering, and Quality
David J. Gorney
Space Systems Group

4.1 Introduction

The goal of program assurance is to establish and control a program delivering the required capabilities within the allocated budget and schedule at acceptable risk. In simple terms, program assurance is aimed at appropriately balancing desired/required technical performance within cost, schedule, and risk constraints. In this sense, it expands the meaning of "mission success (MS)" to include meeting cost and schedule objectives in addition to on orbit performance. Since 75–80 percent of a program's budget is determined early in its life cycle, decisions made in these early phases should be adequately informed by rigorous systems analysis, with the involvement of teams of users, acquirers, and industry representatives.[16] Government and industry need to work together to develop and explore solutions to arrive at an optimal systems solution that meet cost, schedule, performance, and risk goals.

This chapter has been added to the Mission Assurance Guide (MAG) as a result of studies and experience that emphasize the critical importance of early program acquisition activities. The results of independent program assessments (IPAs) show that failure to adequately address key elements of program assurance and systems engineering in the program leads to design escapes and parts problems that do not emerge until later in integrated testing, which then contribute to significant schedule delays, cost growth, and increased risk.[17] For The Aerospace Corporation (Aerospace) program office (PO), engineering and laboratory personnel that routinely perform mission assurance (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, this chapter is intended to provide useful, important context and insight into complex

[16]Space Acquisitions: DOD Faces Substantial Challenges in Developing New Space Systems, GAO-09-705T, 20 May 2009; Report of the Defense Science Board/Air Force Scientific Advisory Board Joint Task Force on Acquisition of National Security Space Programs, May 2003; Space Capabilities Development: Implications of Past and Current Efforts for Future Pro-grams, M. Hura, et al., RAND, September 2007; Pre-Milestone A and Early-Phase Systems Engineering, A Retrospective Review and Bene-fits for Future Air Force Systems Acquisition" by National Research Council, 2008.
[17]TOR-2011(8591)-5, Evaluation Guide for Independent Program Assessments.

decisions made by government program managers (PMs) who must balance technical and programmatic risks. Additionally, as the corporation continues to transition its focus to perform more "front-end" architecture, systems integration, and engineering work, this chapter will serve as a useful guide.

This chapter aims to familiarize National Security Space (NSS) PO personnel with program assurance elements, which include program management acquisition activities and system engineering (SE) activities. These program assurance elements tend to be non-technical in nature and include program staffing, independent cost estimates, acquisition program baselines (APB), acquisition/contract strategy, source selection, and programmatic metrics. They become even more important in defining, acquiring, and delivering program capabilities that are integral parts of larger, generally networked systems (i.e., system of systems [SOS]). A useful reference in this regard is the recently developed The MITRE Corporation/Aerospace "Critical Factors for Acquisition Success Checklist" which defines three "horizontal tracks"—Program Management, System Engineering, and Acquisition.[18]

NSS programs must be properly established with sufficient resources (experienced personnel, infrastructure, funding, and technology) and schedule to manage risk effectively. Program assurance has an ongoing role during program execution to assess technical, schedule, and cost information to identify trends, issues, and risks to understand unfavorable impacts to the program's established performance, schedule, cost, and risk baselines. Stakeholder expectations should be addressed by continuously providing objective program status. This chapter describes practical program assurance tools and practices to establish and manage an executable program, delivering the best value system given the budget, schedule, and mission targets.

4.2 Definitions

Program Assurance is the set of MA activities systematically executed by the PO through technical assessments of the programmatic practices (cost, schedule, performance, and risk) to ensure the program delivers the required capability for required operations within the allocated budget and schedule for overall mission success.

Acquisition Program Baseline reflects the threshold and objective values for the minimum number of cost, schedule, performance, and attributes (called "key performance parameters [KPPs]") that describe the program over its life cycle. Cost values reflect the life cycle cost estimate, scheduled dates include key activities such as milestones (MSs) and the initial operational capability (IOC),

[18]Critical Factors for Acquisition Success Checklist, Version 3.1, The MITRE Corporation and The Aerospace Corporation, 5 June 2012.

and performance attributes reflect the operational performance required for the fielded system. Since programs rarely progress as expected, a low-level re-tuning of the baseline may allow the program to steer clear of major APB breaches, which require notification to Congress.[19]

Earned Value Management (EVM) is the discipline of managing projects successfully. It is the planning and controlling of authorized work to achieve cost, schedule, and technical performance objectives. Special emphasis is placed on efficiency and effectiveness in the execution of work through the development and operation of an EVM system to consider the application of people, systematic processes, and innovative tools and techniques. EVM helps project managers and their teams operate more effectively in the execution of risky high-dollar and complex programs.[20]

Independent Cost Estimates (ICE) is a life-cycle cost estimate for Acquisition Category I (ACAT 1) programs prepared by an office or other entity that is not under the supervision, direction, or control of the Military Department, Defense Agency, or other Component of the Department of Defense (DOD) that is directly responsible for carrying out the development or acquisition of the program, or if the decision authority has been delegated to a Component, prepared by an office or other entity that is not directly responsible for carrying on the development or acquisition of the program. An ICE attempts to capture a program's full costs and associated risks to establish a "will-cost" position for the program that tests the reasonableness of the advocated program cost estimate.[21]

Integrated Master Plan (IMP) is an event-driven plan that documents the significant accomplishments necessary to complete the work and ties each accomplishment to a key program event.[22]

Integrated Master Schedule (IMS) is an integrated and network multi-layered schedule of program tasks required to complete the work effort captured in a related IMP. The IMS should include all IMP events and accomplishments and support each accomplishment closure criteria.[23]

Integrated Product Team (IPT) is a multidisciplinary team composed of representatives from appropriate functional disciplines working together to build successful programs, identify and resolve issues, and make sound and timely recommendations to facilitate decisionmaking. Program-level IPTs focus on

[19]Defense Acquisition University ACQuipedia, https://acc.dau mil/CommunityBrowser.aspx?id=275159
[20]Ibid.
[21]Ibid.
[22]Ibid.
[23]Ibid.

program execution and may include representatives from both government and industry after contract award.[24]

Key Performance Parameters (KPPs) are those attributes or characteristics of a system that are considered critical or essential to the development of an effective military capability. A KPP normally has a threshold, representing the required value, and an objective, representing the desired value.[25]

4.3 Objectives

The primary objectives of program assurance are to ensure that system performance is well defined, and program execution meets required performance, with management of requirements, risk, performance, schedule, and cost throughout the program life cycle. **Simply stated, Program Assurance objectives are cost, schedule, performance, and their associated risks**. PMs must plan and manage every phase of a program life cycle with objective and rigorous knowledge-based criteria with emphasis on program MS tasks and deliverables. Programs should organize for success but also develop contingency plans that allow for deviations from the plan. This strategy applies to both technical management and programmatic management planning and execution phases. A PO should organizationally allocate resources and document roles, responsibilities, and accountabilities to manage to the established performance, cost, and schedule baselines. The development of a viable acquisition strategy that results in a clear, concise Request For Proposal (RFP) and subsequent contract award is essential. Additionally, the choice of contract type, with appropriate controls and deliverables is important in managing programmatic constraints and decisions. In this regard, planning should detail the program assurance oversight responsibilities associated with the contractor as well as government accountabilities (responsibilities dictated by policies and instructions) to ensure acquisition success.

4.4 Program Assurance Core Activities

Figure 4-1 depicts program assurance core activities in the context of a typical DOD acquisition life cycle.[26] The activities are sorted along three primary disciplines: program management, SE, and acquisition. Each of these tracks contains a set of activity areas across the life cycle, for a total of 15 activity areas. Although the principal focus of this chapter is the program management

[24]Ibid.
[25]Ibid.
[26]DOD Technology Readiness Assessment Deskbook, July 2009.

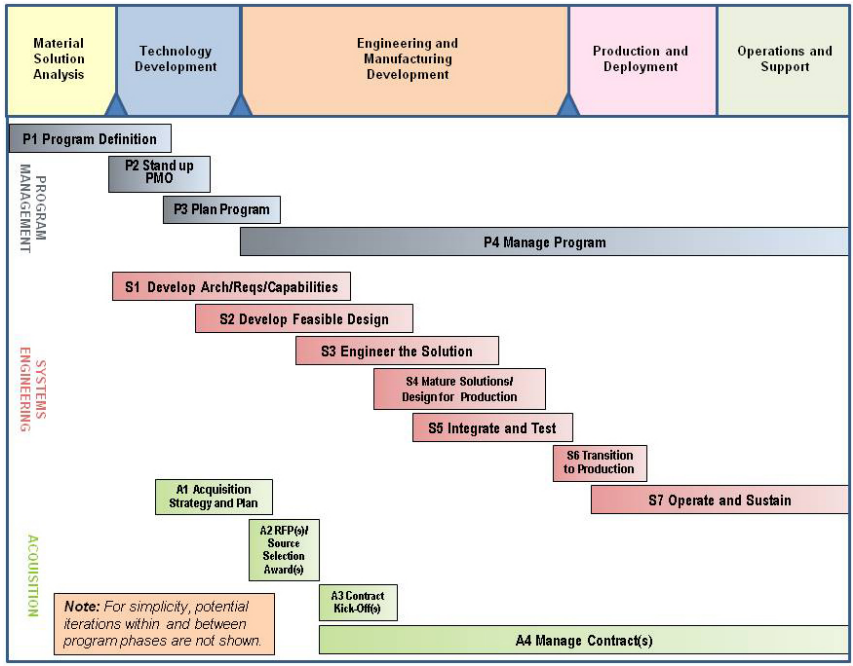


Figure 4-1. Program Assurance Core Activities

and acquisition tracks, program assurance activities also intersect with SE.[27] Specific MA activities for core processes and supporting disciplines that follow the SE framework are further detailed in the remaining chapters.

The accelerating development of information technologies and focus on network enabled/connected systems adds a layer of significant complexity to many programs—that of "SOS" integration. A key element to consider in planning and executing a program strategy using these program assurance core activities is the tiered and iterative nature of program acquisitions that have multiple segments and that span multiple organizations. When developing a strategy to ensure that a program will be successful (i.e., that a program will be executed that delivers all the technical capability required on schedule and within budget), three integration domains should be considered and resourced properly—architectural integration, organizational integration, and programmatic integration.

[27]NASA/SP-2007-6105, Rev. 1, NASA Systems Engineering Handbook, December 2007; GAO-06-776R, Space System Acquisition, June 2006; Guidelines and Metrics for Assessing Space System Cost Estimates, RAND, 2008; Space Vehicle Systems Engineering Handbook, TOR-2006(8506)-4494, W. Englehart, Editor, 20 November 2005; Guidelines for Space Systems Critical Gated Events, W. Tosney, et al., TOR-2009(8583)-8545, May 9, 2008; Federal Acquisition Regulation, Section 2.101, https://www.acquisition.gov/far/

- Architectural integration includes, but is not limited to, defining and managing technical interfaces across major segments of a program that might include space or airborne platforms/sensors, networks, and terminals. Typically, responsibility for segments is distributed among acquisition and user organizations, requirements organizations, decision authorities, operations organizations, and maintenance/sustainment organizations. The government is responsible for these integration tasks and typically forms an industry-led systems integration team, with Federally Funded Research and Development Center (FFRDC) support, coordinating and orchestrating the connections across all of these organizations to allow the acquiring organization to maintain a stable set of requirements and deliver capability on schedule, on budget. A key element in successfully executing complex programs is ensuring appropriate resources for the systems integration team.

- Organizational integration involves coordinating and managing the close cooperation, collaboration, and advocacy across multiple agencies/organizations to ensure proper resourcing and synchronization with multiple programmatic activities, particularly linked to the Program Planning Budgeting System (PPBS) cycle (and activities on the Hill). Again, this is principally a government responsibility since each organization has its own funding authority. Consideration should be given to establishing a senior-level working group to enable the high degree of shared awareness and trust necessary for ultimate program success.

- Programmatic integration is typically the responsibility of the prime contractor and involves a detailed understanding of the industry team and supply chain that must be properly organized and synchronized to build and deliver the "program." The government PO must ensure that the prime contractor, as well as industry partners and supply chain, are properly resourced and incentivized to ensure success. Contract types and how they flow down through the supply chain are important considerations.

4.4.1 Program Definition (P1)

The first activity area in this horizontal track, **Program Definition (P1)**, typically occurs as part of a program's concept development work. Shaping the acquisition initiative into a credible and executable program, laying the foundation for the program, is critical to the success of the subsequent development of a system or capability. As part of this activity, the government should ensure that there is a clear and valid need, expressed by the applicable user communities, which can be met with a practical and cost-effective solution. Equally important to shaping the need is ensuring that the user and sponsor communities back this need and are willing to support it, and that there is a clear champion for the program to help make it a success. This activity area should also highlight the communication vehicles needed, including any necessary

external governance structures, the high-level acquisition strategy, and the most critical risks identified at this early stage of the life cycle.

Reliable cost and schedule analyses are critical to avoiding expensive overruns. Yet, these are often poorly managed. Inaccurate cost estimates often result from lack of clear roles, responsibilities, and emphasis in cost estimating on programs.[28] Key contributors to schedule delays in these complex systems development include: requirements volatility, technology maturity, test failure with resulting redesign, build-up, retest, design challenges, parts quality, launch vehicle (LV) availability, etc. A high-level ICE should be created before contract award and additional independent reviews performed at major MS reviews.

The work in this program assurance area is predominately completed by the government. A Program Management Office (PMO) may or may not exist at this time. Government personnel supporting this early program definition work may or may not ultimately move into the PMO. The primary effort during this activity area is led by the requirements organization, in coordination with the acquisition office and the end users.

4.4.2 Stand Up PMO (P2)

Successfully formulating a program and implementing its solution requires a team of staff with the needed technical and managerial competencies and operational experience. Once the operational need has been sufficiently defined and receives the approval and funding to become a program, the first step is most often to implement this second activity area, **Stand Up PMO (P2)**. Critical in standing up this office is determining the appropriate organizational structure and acquiring the right resources. The most critical of these resources are the PM, Chief Systems Engineer, and Chief Architect. It is also critical that as part of this activity area, the roles and responsibilities of the various PMO entities and external interfaces are clearly defined, including the authorities and accountabilities associated with each. The governance structure and lines of communication also should be defined and the managerial processes and procedures defined. These roles and responsibilities should be revisited as the program progresses through integration and testing phases to adjust program talent as needed. The government should attempt to align the duration of the PM and key personnel assignments with key deliverables and MSs in the program. Finally an initial credible schedule should be established and tied to the funding.

The space community must improve collaboration, particularly to collectively learn lessons, adopt best practice, and capture this knowledge in the appropriate documentation. Standing up a PMO is a government responsibility. Most often

[28]GAO-06-776R, Space System Acquisition, June 2006.

the PMO Manager is selected and then given the responsibility to establish and implement the PMO. As part of standing up the PMO, the government may acquire a program management support contractor to help with the execution of the PM activities. When this occurs, the acquisition horizontal track is concurrently executed to acquire this support contractor.

4.4.3 Plan the Program (P3)

Per the Federal Acquisition Regulation (FAR), Section 2.101, *Definitions*, acquisition planning means "the process by which the efforts of all personnel responsible for an acquisition are coordinated and integrated through a comprehensive plan for fulfilling the agency need in a timely manner and at a reasonable cost. It includes developing the overall strategy for managing the acquisition."[29] The **Plan the Program (P3)** activity area begins by defining a program with realistic objectives that are within the PM's span of control to enable rapid, successful outcomes via acquisitions. Key elements in planning the program include requirements development and management, defining and developing the concept of operations (CONOPS), implementing configuration management control and tracking, tailoring the life cycle to best support the program's needs and outcomes, implementing a strong risk management process, beginning the planning for testing, updating the initial schedule to include more detail, and updating the initial high-level cost estimate, to create a full life-cycle cost estimate (LCCE). The culmination of these efforts is documented in the APB.

The system concept development is the creative technical process that develops a basic approach to a system that achieves the desired outcomes. The goal of the concept studies phase is to refine the initial concept, develop a supporting technology strategy, and define the system requirements. These activities are primarily pre-Phase A, and lead up to a key decision point at Milestone A. The main function performed during this conceptual study phase includes the assessment of alternative concepts, identification of potential solutions, and identification of technology risks. The process details comparing alternative solutions on the basis of operational effectiveness and cost. The time value of the capability should be considered for greater probability of mission and program success. "Each year that a needed capability is delayed has a cost to those who need it, and delays the availability of operational data and experience to guide subsequent improvements."[30] High confidence trades must be clearly articulated that incorporate constraints and boundaries with strong advocacy for an executable result.

[29]Federal Acquisition Regulation, Section 2.101, https://www.acquisition.gov/far/
[30]Space Capabilities Development: Implications of Past and Current Efforts for Future Programs, M. Hura, et al, RAND, September 2007.

A comprehensive understanding of KPPs, technical performance measures (TPMs), and CONOPS details (e.g., system throughput, response time) must be documented and understood by all users, PO personnel, and contractors. These should be developed early in the program planning. The KPPs/TPMs will guide development, demonstration, and testing of the system.[31] Program assurance activities should ensure all major system-level requirements, including all KPPs/TPMs, are defined sufficiently to provide a stable basis for system development. Failure to define system KPPs/TPMs clearly is the first step to requirements instability and subsequent cost and schedule overruns.

The PMO should evaluate the quality of the contractor program execution plan including the staffing plan against the IMP, the IMS, the Program Management Plan (PMP), and the Contractor Delivery Requirements List (CDRLs). The strategy for program plans, schedules, and developments is to organize for success, both technically and programmatically. The contractor should have a plan in place to resource the development of the system with appropriate talent over the life of the program to include a steady stream of tangible successes (e.g., demonstrations of technologies, testing of parts, subassemblies, bread-boards, brass-boards) and overlay this with MS reviews. Contractors often align their efforts based on functions that provide engineering integration across the program life cycle. These functions should be recognized and managed by high-quality PMs and system engineers with high aptitude and extensive experience combined to create high domain knowledge – critical for large complex development programs. The length of the experience, number of programs worked, domain knowledge, and formal training are important evaluation factors for selecting key personnel.

The government should review the contractor's strategy, both technically and programmatically. Frequent clarification of requirements and decisionmaking is required using the most effective communication and coordination practices. Effective communication can best be realized through the establishment of IPTs that include users and stakeholders. The PMO should have access to contractor facilities and data. Contractor counterparts and points of contacts should be identified and a data retention system established with PMO access to that data repository.

4.4.4 Manage the Program (P4)

In the **Manage the Program (P4)** activity area, the PMO begins to implement and execute all of its management processes. One of the most important aspects of effectively managing the program is maintaining the APB, including the technical baseline, using strong configuration control. The PMO must also conduct continuous and active risk management and schedule and cost

[31] DOD Technology Readiness Assessment Deskbook, July 2009.

management, and implement needed program reviews, including tracking and monitoring actions resulting from these reviews. Additionally, the PMO must keep a record of all critical pending and made decisions with the applicable decision briefings. The remainder of this Guide goes into much more detail on the core MA processes and overlapping supporting disciplines in terms of MA activities that the government should be undertaking in an oversight role.

Early program assurance focus on conducting system performance assessments should be to ensure that there are sufficient models, and appropriate simulation environments to validate the selected concept and CONOPS against the KPPs. Performance assessment of large complex programs early may affect maturity of requirements and later performance verification. Program assurance should resist new system requirements and new technologies after Milestone B. The PM should verify requirements and consider future mission growth over the program life cycle. Challenges include developing systems with greater complexity with more potential defects with limited and constrained resources. This requires a more disciplined verification strategy. A strategy that takes a risk-based approach to MA early on in the life cycle. A strategy that considers the constraints of limited resources (cost and schedule), allocates resources to the highest risk areas, and integrates value-added requirements and MA provisions as a plan for MS.

Reliable cost and schedule analyses are critical to avoiding expensive overruns. There are a number of models that offer cost estimates based on preliminary design information and databases of heritage program cost information. Schedule analysis is also based on historical data for mature programs of similar scope and technical complexity. New program starts should scrutinize claims and assumptions linked to cost savings, maturity of technology, funding stability, requirements stability, and achievability of planned schedule. During the program execution phase, the contract tools for assessment are the EVM system for cost analysis, and the IMS. This information ties closely to the contract work breakdown structure (WBS), however there usually are accounting timeline lags and/or the contractor may manage day-to-day activities using a different scheduling system/tool. The government PO must be aware of the tool limitations and frequently communicate with the contractor to realistically assess risk to the cost and schedule baselines.[32]

Program assurance activities should focus on the major cost and schedule drivers, including risk, and plan on reducing these uncertainties. All potential risk is communicated and accepted by all stakeholders. The risk load should be reported in both risk adjusted schedule and risk adjusted cost for a specified confidence level. Assumptions that should be scrutinized include claims and assumptions linked to savings, expected weight growth, maturity of technology,

[32]Department of Defense Earned Value Management Implementation Guide, October 2006.

funding stability, requirements stability, and achievability of planned schedule. Optimistic schedules are a red flag for program executability.

The government is ultimately responsible for this activity area and the PMO leads the implementation and execution of this activity area; however, it is often assisted by a support contractor.

4.4.5 Develop Architecture/Requirements/Capabilities (S1)

During the Program Definition phase the operational needs were defined in a set of high-level requirements. The first activity area in this horizontal track, **Develop Architecture/ Requirements/Capabilities (S1)**, is to refine these into a more detailed set of operational and technical requirements. Although the ultimate responsibility for doing this lies with the PM, to be successful it is critical to involve the end users and stakeholders as well. At this same time, the PMO begins defining the architecture. Alternate architectures should be considered as part of this activity with a focus on creating a standards-based yet flexible architecture that supports agile, performance-based implementation. The key capabilities are also clearly defined as part of this activity area. Finally, the PMO may begin some early prototyping during this phase. The prototyping can be of different architectures or even early candidate solutions.

Functional and product architecture provides portioning of complex systems, often with reduced developmental cost and risk. Program assurance activities should evaluate the mission architecture to verify that the system has been partitioned into segments that can be independently developed and tested. Additionally, there should be a plan in place, prior to Milestone A that addresses the information exchange protocols for the system. Defining the interfaces early reduces interface problems in subsequent development phase, when it may be costly to change or fix.

The government must maintain responsibility for this activity area. The PMO should be the ultimate integrator for the program, and should drive the requirements and architecture development. The Chief Engineer (CE) plays a critical role in performing the activities in this area.

At the onset of Phase A, the contractor is responsible for mission analysis, system synthesis, requirements analysis and allocations, and requirements/specification development and validation activities. The government PMO performs associated independent requirements analysis activities supporting MA. Parallel government and contractor processes require use of 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. These activities are described in more detail in Chapter 5, Requirements Analysis and Validation.

4.4.6 Develop Feasible Design (S2)

It is the PM's responsibility to implement a sound SE approach to translate the operational needs and requirements into the solution. The **Develop Feasible Design (S2)** activity area is where this is done. To make this translation, a preliminary, and then detailed, design is developed. Department of Defense Instruction (DODI) 5000.02 states that "The design approach shall partition a system into self-contained, functionally cohesive, interchangeable, and adaptable elements to enable ease of change, achieve technology transparency and mitigate risk of obsolescence. It shall also use rigorous and disciplined definitions of interfaces and where appropriate, define the key interfaces within a system by widely supported standards (including interface standards, protocols, and data interchange language and standards) that are published and maintained by recognized standards organizations."

A common start for this activity area is gaining a full understanding of the range of possible solutions, including their costs, schedules, performance implications, and ability to satisfy the operational and technical requirements. This is typically done via an Analysis of Alternatives (AOA). The AOA should at least be started in this activity area, even if it isn't completed until the Engineer the Solution activity area.

As part of this activity area, the government may also consider using modeling and simulation (M&S) to help determine early whether the design is feasible. It should also consider using trade-off analyses and prototyping as well. It is critical to ensure that the design can be implemented into a feasible operational and technical solution. Another aspect of this activity area is to develop the test strategy and begin planning for the test environment, and to consider any potential operational constraints that may impact the architecture or design.

Chapter 7, Design Assurance, of this Guide provides key objectives and practices applied to assess the design to evaluate that the design intent is achieved through product qualification, manufacturing, and test phases. The design assurance process, a core MA process, is an iterative set of planning, analysis, test, and inspection activities which are performed from conceptual to preliminary to detailed design stages to improve the probability that space, launch, and ground systems will meet their intended requirements through all operation conditions and throughout the design life. Design assurance encompasses: mission design, system design, hardware (HW), and software (SW) design and test.

4.4.7 Engineer the Solution (S3)

A common start for the **Engineer the Solution (S3)** activity area is planning and developing the Systems Engineering Plan (SEP). This critical engineering

document is used to guide the implementation activities. Also as part of this activity area, performance parameters are identified, security and MA implications associated with the proposed solution identified, and risks associated with the proposed solution addressed. The Operations & Maintenance (O&M) organization should also be engaged as part of this activity area so that it understands the alternative solutions and the proposed solution it would be maintaining, and so that the PMO and development contractor understand any operational environment constraints that could impact these solutions.

Also critical to this activity area is ensuring that the PMO has a clear integration strategy and that as part of this strategy it is has considered the implications with the use of commercial off-the-shelf (COTS) products, especially if they are modified-COTS. Before this activity area is completed, the PMO should have a solid programmatic and technical baseline. The PMO should begin transition planning and continue its test planning with the development of the Test and Evaluation Master Plan being completed as part of this activity area and the beginnings of test scripts created. Prototyping should also continue as part of the early engineering of the solution.

The development contractor generally performs the activities in this area, although the government can do this as well, or have a university-affiliated research center (UARC) or FFRDC help with this, especially with conducting an AOA and prototyping. The PMO should maintain responsibility for integration.

4.4.8 Mature Solutions/Design for Production (S4)

The **Mature Solutions/Design for Production (S4)** activity area is also referred to as implementation. The chosen solution from the Engineer the Solution activity area is fully developed and incrementally tested as it is being developed. The O&M organization should be involved during this activity area as well to continue to understand better what it will take to operate this new system and to continue to identify any possible new constraints in the operational environment. Test scripts should be completed and the associated test environment stood up as part of this activity area. Planning for the transition to production should be completed by this time as well, with a clear and completed Transition Plan.

Manufacturing engineering encompasses the use of available and certifiable materials, parts, and manufacturing process to create products that fulfill documented design requirements. Manufacturing assurance, a core MA process, uses a system of checks and validations (i.e., in process tests, inspections, and analysis) to verify that at each stage of the manufacturing sequence the end product of the process meets the quality standards for that stage of the manufacturing sequence. The development contractor takes the lead for the activities in this area, with the government operating in an oversight and

integration role. Core activities are provided in more detail in Chapter 7, Manufacturing Assurance.

4.4.9 Integrate and Test (S5)

There are a number of different test activities conducted as part of the **Integrate and Test (S5)** activity area. Integration, test, and evaluation 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. Test and evaluation reveals any deficiencies or possible deficiencies in the system, including the inability to meet the operational and technical requirements. The first activity is typically development test and evaluation (DT&E) and the testing usually culminates with the operational test and evaluation (OT&E). Other test activities include security and performance testing as well as any other additional tests needed for the system being implemented. Throughout the set of test activities, results should be documented, lessons learned captured, and reports developed. Chapter 8, Integration, Test, and Evaluation, provides a more detailed treatment of the key MA objectives with respect to an integration, test, and evaluation program.

Most activities associated with the development, integration, validation and verification of system components (units, subsystems, and systems) are formally planned and performed by contractor personnel. Typical PO MA activities include ensuring testing is appropriately planned, performed, witnessed, and documented, and test results are independently evaluated to establish development, qualification, and acceptance status. The government PMO is responsible for evaluating test activities and advising contractor personnel on appropriate test approaches based on best practices, standards, lessons learned, and database experience. Equally important is the government oversight to ensure the solution is fully integrated.

4.4.10 Transition to Production (S6)

Many space system acquisitions do not transition to a production mode because they are one-of-a-kind systems or are acquired in very small quantities (usually less than four). Nevertheless, some commercial communications and imaging satellites are acquired and produced in a “production” mode, generally at lower cost and shorter timelines than in most government space systems acquisitions. The key considerations are the degree of “change” across the acquisition/production enterprise and risk posture—to include requirements, people, materials, parts, and processes.

In considering the transition of space systems to production, a careful assessment should be made regarding overall program stability and risk. It is

important that the implementation of new capabilities into the production environment not disrupt other legacy applications. The planning efforts for the transition should be completed prior to entering the **Transition to Production (S6)** activity area. The PM and CE should oversee and coordinate the transition activities required to fully deploy the solution. The activities conducted in this area include the actual transition, documentation of results, and documentation of lessons learned. A strong connection between those responsible for the operational performance of the system and the acquisition/production team is highly recommended.

4.4.11 Operate and Sustain (S7)

The program or program segment has entered into the mission operations phase has been validated and requirements verified. The responsibility for the execution of the system in the production environment is transferred to the O&M organization. Planning for the O&M phase of the life cycle occurs prior to entering the **Operate and Sustain (S7)** activity area. This activity area is specifically for the operation and sustainment of the new capabilities in the production environment and for the introduction of needed changes or enhancements. The O&M organization often uses a contractor to help execute and maintain the system. This contractor could be the same as the development contractor or may be a different O&M contractor.

MA support focus is on the engineering assessment and changes to the system. Changes to the program/system are an artifact of both external (i.e., changing threats) as well as internal (i.e., anomalies, aging system, usage degradation) initiators. PMO contributing support to operations, maintenance, and sustainment includes support to anomaly operations and recovery from anomalies, sustainment of SW, sustainment of ground segment and user segment, system safety (collision avoidance [COLA] analysis and cyber threat analysis), reliability model updates, and end user support and system effectiveness assessments. More details on these extended MA activities are described in Chapter 10, Operations and Sustainment.

4.4.12 Acquisition Strategy and Plan (A1)

The **Acquisition Strategy and Plan (A1)** activity area, considered by many to be one of the key program assurance activities, establishes how needed capabilities will be acquired and supported throughout the life cycle, from development to operations to retirement. Developing the acquisition strategy, and supporting plan, is most often an iterative process, with updates being made as early uncertainties and risks are resolved through further definition and solution formulation. The strategy is also updated as a result of conducting an analysis of alternative solutions, most effectively done via the involvement of the user and stakeholder communities.

The government must lead this activity area and often may perform the activities in this area solely with government staff. It is not appropriate for any development contractor, or even most PMO support contractors, to assist in this area. The government must ensure that any outside support it receives in this activity area, as well as any of the other acquisition horizontal track activity areas, is free of any possible organizational conflicts of interest (OCI). As such, the government will often use an FFRDC to provide guidance and support in these activity areas.

Key to MS is quality and timely delivery of critical items from the supply chain. The PO should ensure that transparency and quality management systems flow to the supply chain. Additionally important is access for both the prime contractor and the government to supplier facilities and management systems, where applicable. A key program assurance task is to ensure that quality management system requirements are flowed down to the suppliers, and that those requirements are understood and implemented. While there are only a handful of large prime contractors, there are more small prime contractors and subcontractors to the prime. As the prime contractors subcontract more of their units or subsystems, the PO should ensure that meaningful insight and oversight into the activities are conducted at the primes and their subcontractors.

4.4.13 Request for Proposal/Source Selection Award (A2)

The focus of the **RFP/Source Selection Award (A2)** activity area is to develop the RFP and supporting Source Selection Plan and to conduct the actual source selection. The typical procurement activities are conducted at this time. In conducting these activities, the solicitation should address items such as performance-based contracting, incentives and disincentives, protecting the government's data rights, and dependencies on external systems. The PMO must also determine if the development contractor will also be the O&M contractor and ensure that an Independent Government Cost Estimate (IGCE) is conducted. One of the key decisions the PMO, with the support from the Contracting Officer (CO), should make is determining the type of contract vehicle to use and whether it wants to award work to one or more contractors.

The term "contractor" signifies a producer of modules or higher-level items of equipment. A contractor that provides items to another contractor can be identified as a subcontractor. Some system programs have one major contractor identified as the prime contractor, who is responsible directly to the acquisition activity. Other programs may have two or more major contractors, each responsible directly to the acquisition activity, which are known as associate contractors. Major/critical subcontracts are those in which failure would seriously jeopardize successful completion of a program within cost, quality, schedule, and technical performance. Prime contractors should establish processes and procedures to ensure that the technical and program management

requirements are clearly and comprehensively defined and effectively flowed down through the complete contractor structure.[33]

The government is responsible for executing this activity area, with the PM and CO being the primary responsible entities. It is critical that the CO be included as part of the PMO, typically through a matrix support approach, so that the CO is equally responsible for meeting program schedules.

4.4.14 Contract Kick-Off (A3)

The **Contract Kick-Off (A3)** activity area is a fairly short and quick activity to conduct. The primary purpose of the Contract Kick-Off(s) is to ensure that the development contract(s) get off on the right foot. Working the relationship between the PM and its PMO, the CO, and the contractor is critical to effectively executing the contract(s). This is where those relationships are initially established. This is also the PMO's first opportunity to share additional information and documents with the contractor to ensure that the contractor fully understands the need, the environment it will be operating in, and any other government expectations.

The PM and CO lead this activity and are supported by the PMO in setting an agenda, pulling together information to be shared, and preparing briefings to be used, etc. The development contractor(s) also play a role in this activity by participating in the kick-off meeting(s) and being prepared to present on any topics requested by the government.

4.4.15 Manage Contracts (A4)

The **Manage Contracts (A4)** activity area is an ongoing, long-term activity that exists for the duration of the contract(s) under the PMO's control. The PM, and PMO, must balance the amount of contract management and controls it puts in place with the need to execute on schedule and within budget. Yet, at the same time, the PMO must put enough management oversight in place to ensure that it can quickly recognize, and take proactive corrective actions (CAs), when the contractor efforts begin to fall off plan. The PM and CO should keep the contractor focused on achieving the end-to-end performance within the program constraints. Another key aspect of this activity area is to ensure that the needed quality exists in the contractor deliverables. The PO should have access to the contractor facilities and data. A data retention system and government access to that data repository should be established, as applicable.

The PMO should ensure that transparency and quality management systems (QMSs) flow down to the supply chain. Additionally important is access for

[33]"A Beginner's Guide to Program Metrics," C. LeeVan and M. Willard, Thomson/West, June 2006.

both the prime contractor and the government to supplier facilities and data management systems (DMSs), where applicable. A key program assurance task is to ensure that QMS requirements are flowed down to the suppliers, and that those requirements are understood and implemented. While there are only a handful of large prime contractors, there are many more subcontractors to the prime. As the prime contractors subcontract more of their units or subsystems, the PO should ensure that meaningful insight and oversight into the activities are conducted at the prime's and their subcontractors.

The PM and CO must also continually monitor the contract requirements to ensure that any proposed new requirements are really out-of-scope, and must monitor and properly implement the use of incentives and disincentives established as part of the contract.

The CO, supported by a Contracting Officer's Technical Representative (COTR), is ultimately responsible for this area, however the PM and PMO conduct most of the day-to-day oversight. This activity area is an inherent government function.

4.5 Program Assessment Metrics

The measurement of the progress of a program through assessment metrics is a fundamental management tool. A standardized reporting of executability risks (metrics) is required to gauge how the program is doing. Metrics should be readily understood, objective, easily measurable, and intuitive to the user. The challenge for a PM is determining the right set/number of key metrics for the right phase to highlight the risks and issues for their specific program. A developing program is dynamic and therefore the metric suite must be a broad story with a broad set of measures. On any given day any one measure could be a leading indicator, but more likely a combination of metrics and interactions between the technical and programmatic components of the acquisition is more telling. Likewise the program is not a linear model, as the hardest tasks/work packages take a longer amount of time to accomplish and the PM should be wary of those hardest problems and greatest risks. Metrics are a tool the PM can use to uncover the roadblocks and then further discover the chokepoints to successful execution.[34]

4.5.1 Cost and Schedule Assessment

Reliable cost and schedule analyses are critical to effectively managing programs and avoiding expensive overruns. Many factors impact these

[34]Independent Review Process – Overview and Best Practices, N. Nelson, et al., ATR-2009(9369)-20, August 20, 2009; Executability Metrics for SMC Programs, P. Smith, et al., TOR-2004(8583)-3470, 15 June 2006

estimates, including type of contract, amount of change or "newness" involved in the program, and degree of acceptability of risk. Given the inherent optimism of most PMs, ICEs are highly recommended and in many cases mandated.

Cost and schedule management is normally required using the contractually mandated EVM system, maintained by the contractor, to assess technical and schedule progress against the baseline plan. EVM data is formally submitted and reviewed by the government PO (Integrated Baseline Review [IBR]) to include contractor performance plans and budgets to verify the technical content of the performance measurement baseline and the adequacy and consistency of the required resources (budgets) and schedules.[35]Overly optimistic schedules and budgets should be an immediate red flag. A general rule of thumb is about a 15 percent management reserve for both time and money.

In theory, EVM can highlight trouble spots by use of two key metrics: the schedule performance index (SPI), and the cost performance index (CPI). The SPI can be isolated to measure performance against schedule in the current month, the last three-, six-month (or any particular period), and inception to date. Emphasis on a current short time interval can be early indicators of program problems and allow management intervention before significant unfavorable variances occur. Trend analysis is useful as well to possibly predict future variances. Similarly, the CPI can measure cost variances at different time periods. Greater than 10 percent variances in the SPI or CPI is an automatic red flag.

The key to effectively using EVM is that it must correlate well with the program IMS and WBS breakdown. The SPI and CPI tie closely to the IMS – a fully networked schedule containing all the discrete work packages (and planning packages) including criteria for determining the completion of work packages. A metric of delivery of work packages/units over time coupled with the SPI, CPI, and a separate manpower loading would provide a global view of the programmatic baseline. The IMS also identifies critical path items that cannot be delayed without delaying the completion date of the program. The government PO must ensure the IMS is frequently updated (monthly updates as a minimum) and reflect the current program schedule and path for these monitoring tools to be effective.

When used effectively, EVM data can identify early areas of the program performance where cost or schedule growth exists so that CA can be taken. Accurate reporting is dependent on trained staff and early identification of performance problems. Unfortunately, incentives sometimes exist to defer the recognition of unfavorable cost and schedule variances by the contractor in order to maintain good customer relations until some interim objective

[35]Federal Acquisition Regulation, Section 2.101, https://www.acquisition.gov/far/

(preliminary design review [PDR], critical design review [CDR], etc.) is achieved, until follow-on work or authorized change work is negotiated, or to avoid criticism internally. Government personnel must be proactive in analyzing IMS and EVM data to discover unfavorable cost and schedule variances, to consider potential worst-case performance risks, and to develop mitigation and CA plans early on.[36]

4.5.2 Performance Assessment (Technical Baseline)

Early program assurance focus should ensure that sufficient models and appropriate simulation environments exist to validate the selected concept and CONOPS against the KPPs. Early performance assessment of large complex programs may affect maturity of requirements and later performance verification.

4.5.2.1 Requirements

The technical baseline is established by the requirements which must be assessed and understood by the stakeholders. The mission is defined by the requirements to include effectiveness measures decomposed to KPPs and then allocated to the system down to the component level with bidirectional traceability. Requirements must be clearly written and consistent; complete; traceable to the lowest level; and written so that there is at least one verification method per requirement. Metrics should address the maturity, verification, and validation of the mission, KPPs, and technical design of the system. Requirements are under CM, so one useful measure is *the number of changes realized over time* – trends should show a decrease of changes over time with stable requirements defined no later than PDR. Variances/changes from the established baseline are a strong indicator of an unstable program. Chapter 5, Requirements Development, Validation, and Verification Planning, of this Guide provides more detail on the MA activities associated with requirements analysis and validation.

4.5.2.2 Design (Maturity/Robustness)

The first assessments of the design address if the concept is feasible from an engineering viewpoint and if the design is operationally feasible based on the completeness, validity, stability, and consistency of the described design. The effectiveness of prototype demonstrations and verifying that the proposed design meets requirements are practical measures. One significant parameter is the maturity of the technology which can be characterized and measured by the

[36] Ibid.

technology readiness levels (TRLs).[37] TRLs should be monitored to ensure sufficient time and funding is allocated to mature the technology. Technical design parameters every program should measure include those regarding the robustness of the design, i.e., *power and thermal margin sufficiency and dry mass growth*. Spacecraft mass always increases as understanding of the design increases; and the spacecraft mass will grow more quickly than anticipated. The stability and the validity of the design may be assessed by monitoring the mass dry mass growth over time since the inception of the program and "adjustments" of the mass margins. Detailed assessment of mass margins can focus risk management activities based on historical evidence published with recommended margins over the life cycle.[38] Chapter 6, Design Assurance, provides more detail on the MA activities associated with design assurance.

4.5.2.3 Manufacture/Build/Quality

Manufacturing/build assessments must first consider if qualified sources exist – single supplier and foreign sources. Planning documentation must include descriptions of adequate resources and qualified parts; and that the processes are repeatable, sustainable, and capable as executed by trained operators with quality inspections in place throughout the supply chain. Hard evidence should be produced as evidence of decisions and managed based on historical risk. Particular emphasis should be placed on monitoring adherence to critical processes along with the personnel experience and training. Quality indicators and work package completion are important metrics that are strong indicators of the producibility of the design and if the processes are in control. Quality indicators include *the number of nonconformity transactions (discrepancy reports)* to include nonconforming product, operator errors, and nonconformity processing. *Number of work packages completed should be evaluated against planned deliveries to include a correlation of manpower budgeted* for those deliveries. If scheduled deliveries shift/slip, then manpower required should either increase or be the same and not reflect an unrealistic turndown which is sure to bust the baseline. Other important quality index assessments include heritage HW/SW reuse performance and number of waivers issued. Additional detail on associated MA activities may be found in Chapter 7, Manufacturing Assurance, and Chapter 16, Quality Assurance.

4.5.2.4 Integration and Test

Integration, test, and evaluation feasibility and testability should be evaluated early on in concept development. The test and evaluation strategy must consider the needed technology development, HW/SW maturity success criteria, test and evaluation methodologies, required ground support equipment, test facilities and

[37]Defense Acquisition University ACQuipedia,
https://acc.dau mil/CommunityBrowser.aspx?id=275159
[38]Executability Metrics for SMC Programs, P. Smith, et al., TOR-2004(8583)-3470, 15 June 2006.

infrastructure availability, design considerations, interface requirements, prototype(s), and engineering identified and planned. All requirements must be verified by performing the right verification for the right requirements to ensure satisfaction of requirements. The program should plan and execute the pyramid test philosophy and ensure test readiness to ensure build maturity. Unit qualification *completeness* prior to assembly, integration, and test (AI&T) is a measurable indicator of planned test execution. Tests should evaluate adequacy of workmanship and retest considerations. Failure review boards (FRBs) tracking and resolution to root cause is required MA insurance for MS. Metrics for test include all *anomalies for HW and SW analyzed and resolved* with the *number of unverified failures* documented. Chapter 8, Integration, Test, and Evaluation, provides more detail on the MA activities associated with integration and test (I&T).

4.5.2.5 Operations Readiness

Operational certification requires a number of products to be delivered that detail the operational procedures, infrastructure, information assurance (IA), logistics, range safety, and testing. One early readiness assessment should reflect the operational SW readiness for the start of AI&T as an indicator of product maturity. On-orbit testing is the validation that the space vehicle (SV) is operating as designed, the ground systems are ready to support mission operations, and the mission data can be distributed to the planned users. Each phase of testing involves functional checkout, performance assessment, and calibration. Metrics for test include all *anomalies for HW and SW analyzed and resolved* with the *number of unverified failures* documented. Anomalies at this juncture in the life cycle are sure to delay turnover of the system to operational status. Chapter 9, Operational Readiness, provides more detail on MA activities associated with operations readiness.

4.5.3 Risk Assessment and Management

Risk management (RM) is a structured process with the objective to identify and evaluate risk across the program, including the identification and evaluation of specific risk reduction and risk control measures associated with cost, schedule, and performance. RM is a key program function in identifying and communicating threats to MS to decisionmakers and program stakeholders at all levels. The government team should maintain a separate risk process from the contractor to track PO execution requirements. Metrics include *risk exposure (number of risks, probability, and impacts), risk burn-down, and risk handling*. One method to highlight the largest risks is *to monetize the risk impact* for relative comparison. 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. No program is without risk; risk decisions and

acceptance that contribute to the total risk burden of the program should be fully documented.

Program risks (performance, cost, and schedule) should be baselined early in program planning and a management plan established across the program life cycle to mitigate those risks. Risks should be evaluated and continuously tracked at a program level throughout the life cycle. The first step to baseline the risk is to assess the contractor critical design, test, and production processes against industry best practices. Focus on the details and high-risk areas; apply best practices; and adopt realistic modeling techniques for schedule, cost, and contractor performance. The full team should be involved, with mechanisms in place to encourage continuous feedback and communication. Risk integrated product teams should include PO, prime contractor, and critical subcontractors. Accountability should be assigned to the highest risk items. It is recommended that cost and schedule risk areas be evaluated against the identified "Six seeds of program failure: inexperienced leadership, external interface complexity, system complexity, incomplete requirements at Milestone B, immature technology, and high reliance on new software."[39]

4.5.4 Staffing and Skills (Organizational Maturity)

A stable and mature organization is required to plan development and execute to plan in the acquisition of a complex space system. The program implementation strategy should address the staffing plans for the contractor as well as the government team. The government program management plan should describe an organizational construct to include identifying FFRDC and SE and technical assistance (SETA) needed, with accountabilities detailed. A program may be assessed based on the organization, management policies, staffing numbers, experience level by skill, productivity, overtime, attrition, morale, hiring, training, and leadership ability. The life cycle of the system should be considered in terms of the types of talent needed and available for the different phases of the program life cycle—sufficient experienced program and system engineers with seasoned leaders is critical to maintaining focus and discipline aligned with key deliverables and MSs in the program. *Skill trends* are metrics that should be tracked over the life cycle of the system, along with *attrition and hiring*.

4.5.5 Independent Review Teams

An independent review is a process by which a program is assessed by a team of people with pertinent skills, but who do not have a day-to-day involvement with program execution. The assessment may be used to redirect the program or to

[39]Report of the Defense Science Board/Air Force Scientific Advisory Board Joint Task Force on Acquisition of National Security Space Programs, May 2003.

affirm its current progress. Independent reviews may be broad or narrow in scope. They add value to a program in several ways, most obviously by bringing a "fresh set of eyes" to plans, schedules, cost estimates, technical design, development and test, and technology maturity assumptions of a program. Independent review teams (IRTs) may have experienced and overcome difficulties similar to those the reviewed program is encountering. They may bring unique knowledge about a specific technology, or novel test ideas. They also provide an impartial "sounding board" for individuals or groups to discuss issues or concerns that have not yet reached formal problem status.[40] Chapter 11, Mission Assurance Reviews and Audits, of this Guide provides more detail on IRTs as well as other applicable MA reviews and audits.

Readiness reviews provide a formal mechanism that supports the decisionmaking process by forcing a careful examination of all elements of the system at key maturity MSs relative to final integration, testing, and operation proficiency, including outstanding problems or liens, in preparation for launch. Key MSs include the decision to ship the launch and/or SV from the factory; the decision to proceed with vehicle erection on launch pad; ground system certification; and the decision to proceed with launch after successfully completing launch integration and processing, successfully demonstrating end-to-end mission connectivity, and successfully demonstrating personnel proficiency through rehearsals. These critical reviews are led and performed by the government with technical recommendations supported by FFRDC and SETA staff. These types of readiness assessments are described in more detail in Chapter 11, Mission Assurance Reviews and Audits.

IPAs are the assessment of the government PMO readiness to proceed into the next acquisition phase. IPAs are conducted before each MS, prior to the post-system design review, and whenever directed by the Milestone Decision Authority (MDA). They are independent, comprehensive, systematic views of the major functions and duties that any PMO must complete, in a step-by-step manner, to have a successful acquisition. Failure to adequately perform these steps could result in essential details not being addressed, possibly resulting in hidden cost overruns, schedule slips, or performance reductions later. IPAs not only provide readiness assessments to the MDA but also mentor PMOs on how to resolve deficiencies to successfully meet MS review boards.[41]

4.6 Practice Task Application Example

When assessing program assurance on a program, the first step is to determine what is the phase of interest to determine the PO program assurance activities and plan resources accordingly. The PO may use this chapter as a guide in

[40]Executability Metrics for SMC Programs, P. Smith, et al., TOR-2004(8583)-3470, 15 June 2006.
[41]TOR-2011(8591)-5, Evaluation Guide for Independent Program Assessments.

determining what program assurance tasks should be considered. Table 4-1 is a practice program assurance task example that demonstrates MA activities for the program management functions across the life cycle of the system.

4.7 Summary

In summary, assuring a program's execution is a difficult challenge. A PO needs to manage stakeholder expectations, develop an executable program, anticipate problems, keep mission success in focus, and manage the program without digging a hole too deep to climb out. This chapter alerts the reader to the roadside hazards, provides a conceptual framework to set a safe course, and recommends tools (references) to get out of harm's way.

Table 4-1. Sample Set of Program Assurance MA Tasks (Program Management Tasks)

	Phase				
Task	**0**	**A**	**B**	**C**	**D**
Ensure the Program is Defined					
Ensure clear and valid need is defined	X				
Ensure stakeholder and user buy-in on the program definition and objectives	X				
Ensure complex processes in place to implement new system, interfacing and integration with other legacy system, are identified and addressed in the budget and schedule	X				
Ensure program is achievable in the political environment	X				
Ensure program funding includes adequate management reserve	X				
Ensure a high-level independent cost estimate is conducted	X				
Ensure Program Stand Up Includes Evaluation of Critical Talent					

	Phase				
Task	**0**	**A**	**B**	**C**	**D**
Evaluate and plan government talent required to manage the program	X	X	X	X	
Evaluate quality of the contractor program execution plan, including staffing plan	X	X	X	X	
Ensure effective communication channels are established with customer and user participation	X	X	X	X	X
Ensure the Program Plan is Executable					
Ensure concept development is matured, including future growth options	X	X			
Ensure the major system-level requirements are defined sufficiently to provide a stable basis for development	X	X	X		
Ensure KPPs are defined in clear, comprehensive, concise terms that are understandable to all, including users of the system	X	X	X		
Ensure full life-cycle cost estimate is completed	X	X			
Ensure acquisition program baseline is complete and documented	X	X	X		
Ensure Program is Managed in Accordance with Plan					
Ensure defined contract deliverables are appropriately tailored to reflect contract requirements		X			
Ensure IMP/IMS is developed and current		X	X	X	
Ensure technical, cost, and schedule baselines are current and are aligned		X	X	X	
Ensure the EVMS is synchronized with engineering efforts		X	X	X	

	Phase				
Task	**0**	**A**	**B**	**C**	**D**
Ensure the WBS reflects the program's schedule and budget		X			
Ensure an active and disciplined requirements management process has been established		X	X		
Ensure disciplined configuration and change management processes are implemented		X	X		
Ensure appropriate test planning is in place to include special facilities		X	X		
Ensure inter-program dependencies, interfaces, and commitments are defined and documented to include consideration of all stakeholders		X	X	X	X
Ensure a data-rich "gated review" process is implemented		X	X	X	
Ensure risks are identified and a management plan is in place early in the acquisition life cycle	X	X	X	X	X
Ensure key risk drivers are identified	X	X			
Ensure major cost, requirement, and schedule risk areas are identified	X	X	X	X	
Ensure risks are assessed against the "six seeds of failure"	X	X	X	X	X

4.8 References

Specifications and Standards

—	DOD Technology Readiness Assessment Deskbook, July 2009
AFI 63-101	Acquisition and Sustainment Life Cycle Management, 3 August 2011

DOD 5000	Defense Acquisition Guidebook, 5 May 2010
DODI 5000.02	Operation of the Defense Acquisition System, 8 December 2008
SMCI 63-102	Space Acquisition Board Process, 7 September 2006
TOR-2004(8583)-3470	Executability Metrics for SMC Programs, 15 June 2006
TOR-2005(8583)-3970	Mass Properties Control Standard for Space Vehicles, 20 July 2005
TOR-2008(8583)-7731	Program and Subcontractor Management, G. Schipper, 11 March 2008
TOR-2009(8506)-8955	KDP A Independent Program Assessment (IPA) Evaluation Guide, 12 February 2009
TOR-2009(8583)-8545	Guidelines for Space Systems Critical Gated Events, 9 May 2008

Handbooks

NASA/SP-2007-6105, Rev. 1	NASA Systems Engineering Handbook, December 2007
TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, 20 November 2005

Best Practices

ATR-2009(9369)-20	Independent Review Process – Overview and Best Practices, 20 August 2009

Other

Briefing Papers No. 06-7	“A Beginner’s Guide to Program Metrics,” C. LeeVan and M. Willard, Thomson/West, June 2006
GAO-06-776R	Space System Acquisition, June 2006

GAO-09-705T Space Acquisitions: DOD Faces Substantial Challenges in Developing New Space Systems, 20 May 2009

Critical Factors for Acquisition Success Checklist, Version 3.1, The MITRE Corporation and The Aerospace Corporation, 5 June 2012

Defense Acquisition University ACQuipedia, https://acc.dau.mil/CommunityBrowser.aspx?id=275159

Department of Defense Earned Value Management Implementation Guide, October 2006

Federal Acquisition Regulation, Section 2.101, https://www.acquisition.gov/far/

Guidelines and Metrics for Assessing Space System Cost Estimates, RAND, 2008

Pre-Milestone A and Early-Phase Systems Engineering, A Retrospective Review and Benefits for Future Air Force Systems Acquisition," National Research Council, 2008

Report of the Defense Science Board/Air Force Scientific Advisory Board Joint Task Force on Acquisition of National Security Space Programs, May 2003

Acknowledgements. Valuable direction, advice, review, feedback and content contributions for this chapter were provided by the following Aerospace personnel: Dev Banerjee, Terry Bavaro, Paul Cheng, Gail A. Johnson-Roth, and William F. Tosney.

Chapter 5
Requirements Development, Validation, and Verification Planning

Dan W. Hanifen
GEOINT Development Office
Sergio B. Guarro
Systems Engineering Division
Wade Y. Sakauye
Abraham A. Santiago
Cost, Schedule, and Requirements Department

5.1 Introduction

Requirements development, requirements validation, and requirements verification planning are system engineering (SE) activities that are typically conducted during the front end of a system acquisition life cycle. 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. Mission assurance (MA) incorporates independent technical assessments (ITAs) within these SE activities to arrive at the best systems acquisition approach. As defined in earlier sections, these MA ITAs are commonly conducted by the government program office (PO) consisting of FFRDC and System Engineering Technical Assistance (SETA). The ITAs are performed to ensure the appropriate technical analyses and industry best practices are used and will be applied in a manner that will meet user needs. It is important to ensure the appropriate requirements and processes are established early in the program, as they will be applied throughout the acquisition life cycle.

While the contractor is responsible for mission analysis, requirements and specification development, verification planning, and system validation activities, Aerospace, in partnership with the government PO team, performs associated ITA requirements validation 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 optimized and decomposed into system requirements and flowed to build-to specifications and interfaces. In accomplishing the task of requirements optimization and allocation to lower levels, MA seeks assurance of contractor's models and simulations used to assert the performance represented by the system requirement set. Often this task involves an independent analysis

by The Aerospace Corporation (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. The following discussion treats the term *specifications* as being synonymous with the term *requirements*.

Requirements development, validation, and verification planning activities are most active in the earlier stages of the system development life cycle beginning with system requirements formulation in Phase A and continuing through Mission Assurance Guide (MAG) Phase C activities of development and design. Later in the life cycle and before system deployment, operations readiness assurance (ORA) ensures the existence of a closed-loop process that provides confidence that the built-to system meets the intended needs of the users.

5.2 Definitions

Functional analysis/allocation is the SE activity that defines and integrates a functional architecture to the depth needed to support synthesis of solutions for people, products, processes, and management of risk. Functional analysis and allocation is conducted iteratively to: define successively lower-level functions required to satisfy higher-level functional requirements; identify and define alternative sets of functional requirements; define mission- and environment-driven performance requirements that satisfy higher-level functional requirements; flow down and allocate performance requirements and design constraints; define and refine feasible solution alternatives that meet requirements; and place derived requirements into the functional architecture.

Requirements analysis is the SE activity that analyzes the customer needs, objectives, and requirements in the context of customer missions, utilization environments, and identified system characteristics to determine functional and performance requirements for each primary system function. Requirements analysis produces a complete, optimal, and verifiable set of system-level functional and performance technical requirements and design constraints. An iterative analysis process using the needed operational capabilities, objectives (or goals), measures of effectiveness, missions, and projected utilization environments is used to establish the requirements. DOD policies and practices, acquisition strategies, and public law are also factored into the analysis. A balance between capabilities to be provided and the evolutionary growth potential in addition to cost, schedule, and risk is also considered. The results of requirements analysis are documented in the requirements baseline.[42]

[42]Requirements analyses definition adapted from L. W. Pennell and B. E. Shaw, Aerospace TOR-2005(8583)-3a, *Systems Engineering Requirements and Products*, p. 11, September, 29, 2005. Unlimited distribution.

Requirements development is the SE process of taking all inputs from relevant stakeholders and translating those inputs into technical requirements by conducting requirements analysis, functional analysis and allocation, and requirements synthesis.

Requirements synthesis is the SE activity that defines and designs solutions for each logical set of functional and performance requirements within the functional architecture and integrates them as a physical architecture. Outputs of synthesis are: determination of the completeness of functional and performance requirements for the design; definition of internal and external physical interfaces; identification of critical parameters; defined system and system element solutions to a level of details that enables verification; and translation of the architecture into a work breakdown structure (WBS), specification tree, and configuration baselines.

Requirements validation is the SE activity that provides confidence (through independent analysis or test) that the technical means and processes accomplish their intended purpose,[43] in this case to meet user needs. Requirements validation occurs during the front end of the systems acquisition life cycle. Requirements validation should not be confused with system validation, which occurs during the later stages in the acquisition life cycle. System-level validation occurs before the as-built system is transitioned into mission operations to validate the correct system was built.

Requirements verification planning is the SE activity that develops plans and activities to prove the as-built item complies with the requirements baseline as determined by test, analysis, demonstration, or inspection. The verification activity is performed from the lowest level configuration item (CI) to the system-level. Verification is typically done in a hierarchical fashion from the lowest level requirements up through 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. For purposes of this chapter, requirements verification planning covers the independent assessment of the associated verification methodology, not the verification of specific requirements.

5.3 Objectives

The objective of **requirements development** is to establish a rigorous, iterative process that enables the creation and maintenance of a requirements baseline

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

throughout the acquisition life cycle. Requirements development utilizes the SE activities of requirements analysis, functional analysis and allocation, and requirements synthesis to create the requirements baseline and incorporates elements of system control to maintain the requirements baseline. The requirements development process is shown in Figure 5-1.

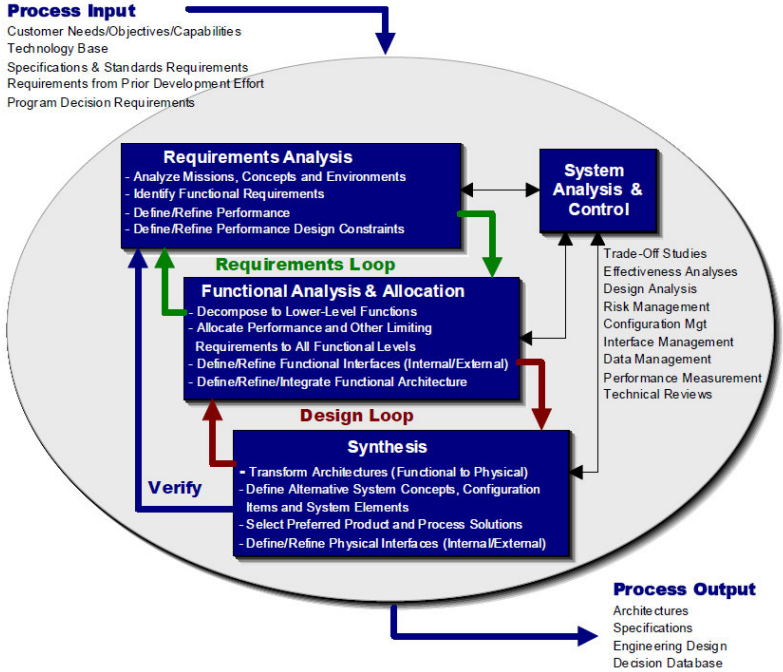


Figure 5-1. System Engineering Process—Requirements Development

As a part of requirements development, requirements analysis produces 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. The requirements analysis process 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 to meet top-level system requirements. Functional analysis and allocation activities, such as decomposing requirements to lower levels, defining internal and external functional interfaces, and refining the functional architecture, are conducted to arrive at a functional design. Synthesis transforms the functional design into a

physical design and also defines the internal and external interfaces. At the completion of synthesis, a system requirements baseline is established that includes external and internal interface requirements. This requirements baseline is 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. Cost is allowed to vary so that the cost of incremental capabilities can be clearly understood. 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 development 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. Requirements validation occurs in the early program phase, concurrently with requirements development. During later phases of the program system validation is performed. Because of 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 (test, analysis, inspection, or demonstration). The objective of **verification planning** is to establish the process, technical criteria, tools, resources (i.e., people, facilities, test equipment, information), and forums required to successfully verify system requirements.

5.4 Practices

5.4.1 Core Activities

5.4.1.1 Requirements Development

In the requirements development process, operational concepts are documented and analyzed (requirements analysis), functional architectures are created, examined, and alternative solutions addressed using a variety of analytical tools

and simulations leading to the decision to proceed with Phase A (functional analysis and allocation). During Phase A (concept development), the preliminary concept is further developed by examining synthesized architectural solutions and requirement sets using more refined tools and simulations (requirements synthesis). 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 decision to proceed to Phase B.

The selected requirement set documented in a systems requirements document (SRD) (per MIL-HDBK-520) or system specification (SS) and associated architecture, decomposes the operator's stated needs and CONOPS by developing a set of operational architecture views and the system specification, as well as 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 preliminary system engineering master plan (SEMP), 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 (design synthesis is covered in more detail in Chapter 6, Design Assurance).

The MA activity associated with requirements development requires government and contractor participation to review and verify the robustness of the processes used to create and maintain the requirements baseline as the system evolves. Requirement development MA activities include ITAs of requirements analysis, functional analysis and allocation, and synthesis (Figure 5-1). The requirements development process is iterative with feedback loops incorporated that establish and accommodate changes to the requirements baseline.

MA tasks supporting requirements development are:

- ITAs of requirements traceability begins with top-level system requirements documents such as CDD, CONOPS, and government or procuring agency directives and policy. Top-to-bottom traces are conducted as well as bottom-to-top to identify orphaned, widowed, or derived requirements. The resulting set of allocated system requirements (functional, performance, interface, environment, and process) are subjected to a final review to ensure they are verifiable with the verification methods selected. Different system and operational views are also developed to ensure self-consistency 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 test cases that are conducted by the developing contractor and then independently validated 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 ensure 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 Aerospace'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 contractor 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 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.

5.4.1.2 Requirements Validation

Requirements validation ensures that the right set of requirements, if used properly to guide a system's development, will result in a system that meets the user's expectations and needs. The primary means to achieve this are through modeling and simulation. Specific requirements validation tasks include:

- Evaluation of user operational scenarios and the establishment of design reference cases
- Evaluation of KPPs
- Evaluation of architecture alternatives against operational scenarios and KPPs

5.4.1.3 Requirements Verification Planning

Verification is a systematic, thorough, rigorous, iterative, and hierarchical process that certifies system requirements (including interfaces, 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 because of 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 (HW) engineering, software (SW) 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 planning process includes active participation, open communications, and timely and comprehensive data exchange among 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,

inspection, and demonstration. Choice of method often requires significant risk tradeoffs because of 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 and documented 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, government-approved verification plan that becomes a cornerstone document for program management and MA.

- Providing the necessary forum(s) to ensure there is a common understanding of the requirements, the requirements are stated in verifiable language, the verification method and approach are clearly established, realistic testing with realistic data is planned, and 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 a comprehensive plan exists to execute all verification methods within the given resources and schedule. A typical overall verification process is shown in Figure 5-2 as it evolves through the planning to the implementation phase. As the design is further defined in detail, the corresponding verification planning becomes more specific.

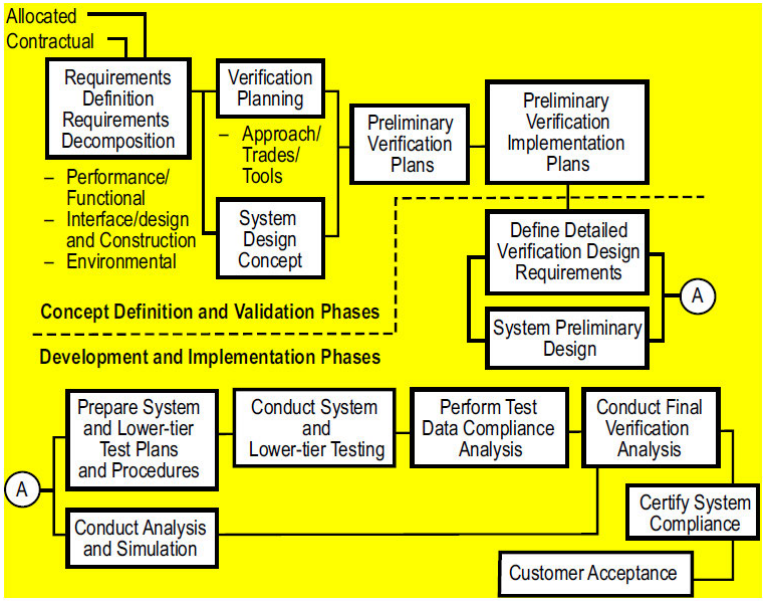


Figure 5-2. Typical Verification Process

Verification planning and implementation are also accomplished in a hierarchical fashion, as depicted in Figure 5-3, which parallels the requirements development process.

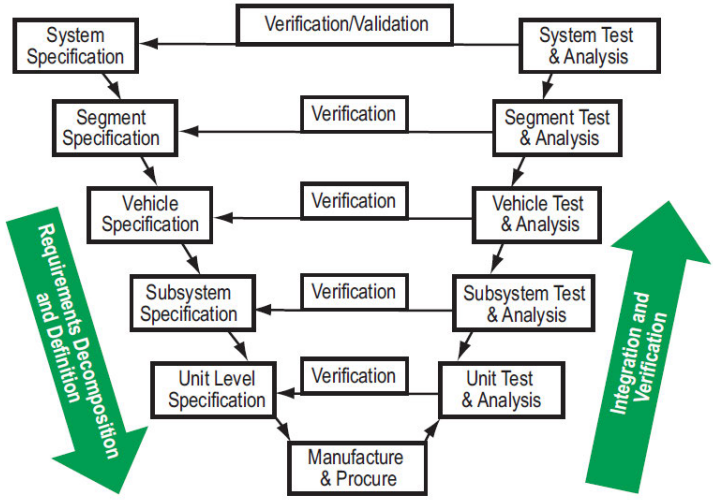


Figure 5-3. Hierarchical Verification Process

5.4.2 Standards/Recommended Practices

The requirements development process, also referred to as the system engineering process, is commonly used in industry and reference can be found in TOR-2005(8583)-3, Rev. B, "Systems Engineering Requirements and Products." Requirements verification planning information can be found in TOR-2006(8506)-4732, Rev. A, Space System Verification Program and Management Process.

Depending on the contract requirements, contractors for most Acquisition Category I and II (ACAT I and II) programs will be required to create a SEMP that is derived from the government systems engineering plan (SEP). Additional elements of the SEMP are based on the contractually binding compliance documents, industry best practices, and contractor best practices. Requirements management plans and a verification program are also common elements in a SEMP.

Commercialized requirements database software such as dynamic object-oriented requirements system (DOORS) is used to trace requirements, verification plans, and interfaces. DOORS can also be linked to architecture development tools such as System Architect, providing visibility into the architecture-level requirements.

5.5 Key Lessons Learned

Key lessons learned in requirements development, validation, and verification planning are described below.

5.5.1 Requirements Development and Validation

- All requirements need to be verifiable.
  - For example, performance requirements without a min/max value or tolerance are not verifiable.
- All requirements must be necessary and traceable to required customer capabilities.
  - Requirements allocation documents (RAD) are often created to show the decomposition and allocation of a requirement. For example, mass and power requirements can be allocated (budgeted) from the system-level into many subsystems. Margin is held at the system level in the event one of the subsystems exceeds its allocation.

- All requirements shall contain bilateral traceability (top-down and bottoms-up).
  - Requirements are decomposed to lower levels, therefore a parent requirement can have many children and a child requirement will have a single parent. There should be no orphaned or widowed requirements.
  - Derived requirements should have rationale justifying creation of the requirement.

5.5.2 Verification Plan

- Verification planning should begin during requirements development.
  - Generate a verification cross-reference matrix (VCRM) with verification details during requirements development. The requirements and VCRM with associated verification details should reside within the same database and be linked to each other.
- Acceptance criteria and verification methods need to be established and agreed on by contractor and government for each requirement within a verification plan. This includes verification at all levels: system, subsystem, and component.
- Requirement verification plans should use the same database that contains the requirements trace and refer to RADs when required.

Other key lessons learned are documented in TOR-2007(8617)-2, "Five Common Mistakes Reviewers Should Look Out For." The document provides guidance for reviewing requirements, interfaces, and test and evaluation (T&E).

5.6 Task Execution by Phase

As identified in Section 5.3, the objective of the requirements development and validation process is to produce a complete and optimal set of requirements based on rigorous analysis of user needs. Requirements development transforms those needs into architectural concepts and views, models/simulations, and functional and system performance requirements through requirements analysis, functional analysis and allocation, and requirements synthesis. The process that generates these products is primarily executed by the prime contractor. However, the associated Aerospace MA process has a distinct role in ensuring the adequacy of these products in achieving mission success. Within this section, the Aerospace detailed tasks, which are implemented in ensuring the requirements development process, are described. These distinct tasks, although distinct from other MA processes, often overlap in several areas of program

activity (e.g., requirements development and validation tasks may overlap with associated MA processes or disciplines.) 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 core MA process (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 development 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 tasks defined in Table 5-1, where there are many more tasks identified in early phases than in the later phases. Table 5-1 more clearly shows the organization of the requirements development and validation MA area. As can be seen, the tasks area is organized by the phases. Starting with 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 the decision to proceed to Phase A. During Phase 0, the program acquisition strategy becomes a key area to ensure adequate resource requirements, i.e., schedule and funding, are being identified in the acquisition strategy plan. If the program does not have sufficient resources at startup, 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, ensuring 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. Additionally, Aerospace will typically conduct mission concept studies, assessing mission feasibility in terms of achievable performance, technology readiness, and risk (requirements analysis). Consistency with the initial concept capability document and preliminary CONOPS will be verified. For technology demonstration programs, Aerospace will ensure 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 Table 5-1.

In Phase A, MA ensures 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 ensuring the Phase A program, as negotiated after contract award, are executable and 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.

After Phase A, requirements development and validation activities shift to ensuring the accuracy and completeness of system requirements and associated requirement allocations to the system segments (functional analysis and allocation, requirements synthesis). A key MA product in this phase is the system requirement set. Verification planning will also be initiated in this phase, with Aerospace ensuring 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 ensuring 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 Phase B decision readiness. The overall outline of Phase A tasks, as well as the outline for all other phases, is shown in Table 5-1. 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 development and validation MA provisions are closely examined in not only the immediate Phase B effort, but in all follow-on contract phases.

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 presents a unique challenge in assessing the adequacy of these elements in meeting the system requirements. This topic is discussed in Chapter 18.

The requirements analysis and validation CMP also ensures 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 ensure the requirement methodology is consistent with the required fidelity and comprehension for that level of integration. Overall, the assessment should ensure a well integrated vertical verification plan where system-level requirements are validated at the highest practical level, but build confidence that validation will be successful based on lower-level verification results.

Phases B and C are similar in content, establishing the preliminary and final designs, respectively. During these phases the requirements development 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 ensure 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 preliminary design review (PDR) with subsequent detailed verification criteria being established by critical design review (CDR). System validation planning completion may be delayed to Phase C. In turn, MA will focus on ensuring 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 contractors.

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 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 integrated verification. In some cases where Phase C activities include pre-production manufacturing, unit or assembly level demonstrations and qualifications will be completed during Phase C. MA will ensure the adequacy of these verifications while determining whether verification can be repeated at a higher level of integration and ultimately validated in an SOS environment. This activity is viewed distinctly from the design assurance process, which often uses the same data to ensure the adequacy of the design.

As in previous phases, during 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 development and validation. During Phase D1, the requirements development 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, Phase D1 will consist of the build and test of the associated HW and SW elements. Formal HW acceptance tests and SW formal qualification test will be the principal vehicles to ensure 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 Phase B and C design phases, this production phase will also generate requirement changes and clarifications as production issues are encountered. MA will ensure any resulting requirement change complies with system-level requirements.

Requirements development and validation (Phase D2) will focus on validating requirements in a pre-launch system environment. For the space segment, this activity will involve ensuring the space vehicle (SV) 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 provide feedback to the system validation effort with noted critical discrepancies being addressed prior to launch.

During Phase D3, Aerospace's requirements development 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 task category (an equivalent of which is actually repeated throughout the various CMPs and SMDs) is not a specific program phase, but a bin to capture nonprogram-specific MA tasks that enable Aerospace to develop and refine organic capabilities to conduct requirements development 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.

Table 5-1. Key Tasks by Phase: Requirements Development, Validation, and Verification Planning

Mission Assurance Phase	Mission Assurance Tasks
Concept Studies (Phase 0)	Validate simulations and modeling tools Validate selection of system concept Assess program acquisition strategy (including resources) Assess analysis of alternatives (AOA) Assess SRD Assess compliance documents Verify initial capabilities description document Assess threats Assess CONOPS Assess architectural views Assess technology demonstration requirements
Concept Development (Phase A)	Assess model and simulation accuracy and plans Assess preliminary mission planning Assess updates to program acquisition strategy (including resources) Develop independent system performance simulation/model Evaluate system concept and requirements Assess and validate system and subsystem requirements Verify system characteristics Assess system trade studies Verify interface requirements Verify and validate requirement allocation flow-down Assess and validate verification plans Ensure integrated verification test plan Verify interface requirements completeness and accuracy Verify traceability to top-level program requirements Identify derived requirements Ensure completeness of requirements Ensure situation awareness has been adequately addressed Ensure completeness of performance evaluation Verify KPPs and technical performance measures (TPMs) Evaluate requirements into implementing documentation (ICD/program requirements document [PRD])

Mission Assurance Phase	Mission Assurance Tasks
Preliminary Design (Phase B)	Assess systems engineering products and processes Assess simulations and models for end-to-end performance accuracy Ensure simulations and models are updated and validated 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 Assess system requirements traceability Assess/Identify derived requirements Assess and validate preliminary verification plan Assess VCRM adequacy Verification tracking system Assess integrated verification strategy Verification compliance
Complete Design (Phase C)	Assess systems engineering processes and products Assess simulations and models for end-to-end performance accuracy Ensure simulations and models are updated and validated Evaluate complete design and requirements Verify and maintain requirement set integrity Verify updated system specifications completeness and accuracy Verify updated interface requirements completeness and accuracy Assess preliminary mission planning Assess requirements verification and tracking system Assess VCRM adequacy Assess final verification planning for completeness and sufficiency Assess verification tracking system Validate updated system requirements allocations Verify requirements compliance for requirements satisfied by design

Mission Assurance Phase	Mission Assurance Tasks
Fabrication/Coding, Test and Integration (Phase D1)	Assess systems engineering processes and products Evaluate product baseline design and requirements Assess system requirements and interfaces Verify updated system specifications completeness and accuracy Verify updated interface requirements completeness and accuracy Ensure interface control process is understood/managed at the system program office (SPO) level Assess system performance Verify KPPs and TPMs Assess requirements verification and tracking system Assess final verification planning for completeness and sufficiency Verify requirements compliance Assess verification tracking system Assure simulations and models are updated and validated Validate updated system requirements allocations
Fielding and Checkout (Phase D2)	Assess systems engineering processes and products Continue assessment of product baseline design and requirements Verify updated system specifications completeness and accuracy Verify updated interface requirements completeness and accuracy Verify system effectiveness Verify KPPs and TPMs Assess demonstrated margins Assess final mission planning Ensure simulations and models are updated and validated Assess end-to-end performance
Operations, Maintenance, Disposal (Phase D3)	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 Ensure simulations and models are updated and validated Assess end-to-end performance

5.7 Government and Contractor Enabling Processes and Products

To successfully execute the identified MA tasks, enabling government and contractor processes and products are required. A basic MA need common to all phases is access to the government's draft and final RFP, the negotiated contract, the system acquisition management plan, cost analysis 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, interface control documents (external interfaces), lower-tier configuration items, SE planning documentation such as the SEMP; verification plan; parts, materials, and process (PMP) management plan; and radiation hardness assurance plan. Examples of contractor MA enabling products at lower levels of assembly include subsystem/unit specifications, interface control documents, design documentation, and test plans and procedures. All of these lower-level enabling products should be documented and traceable (top-down and bottoms-up) to the higher-level enabling products. MA activities are also incorporated at lower levels of assembly in reviewing test plans, test procedures, test data, and the acceptance data packages. Often, it is the accumulation of the acceptance data packages that provides confidence during integration at higher levels of assembly that the HW/SW was adequately designed, built, and tested. The execution of MA activities also requires open access to contractors' IPTs and boards, such as the requirement change control board (CCB), PMP control board, EMC control board, and verification planning IPT, to assess the adequacy of the associated processes. Additionally, for each phase the requirements development and validation MA personnel need to participate in the program initial baseline review and design reviews.

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

5.8 Practice Task Application Example

System engineers and subject matter experts (SMEs) are used by the program office to define robust requirements development processes, validate the program requirements, and define a robust verification planning process. To assist the program office, a standard reference set of tailorable MA tasks is provided in Table 5-2. The products that result from each of the tasks are archived throughout the life of the program.

Table 5-2. Example of Requirements Development, Validation, and Verification Planning Tasks

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Adequacy of SE Processes							
Assess SEMP		X	X	X	X		
Assess preliminary verification plan; ensure an integrated verification test plan is included in the verification plan; ensure the preliminary verification plan complies with best practice		X					
Ensure interface control process is understood and managed at the SPO level; evaluate verification management process: ensure system requirements are verified at the system level			X	X	X		
Prepare mission-specific Aerospace IV&V Plan: • Assess adequacy of contractor requirements verification matrix • Review contractor analysis of interface requirements changes • Review contractor analysis of interface requirements verification			X				
Assess Adequacy of Operations Related Engineering Processes and Products							
Assess the operational system design, concepts, and plans: • Assess the system operational suitability and effectiveness • Ensure operational supportability • Ensure operational requirements and allocation		X	X	X			

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Models, Simulation, and Tools							
Assess M&S for end-to-end performance accuracy	X	X	X	X	X	X	X
Ensure M&S are updated and validated; assess/plan need for simulations, models, and testbeds; develop independent system performance M&S; assess need for independent analysis and simulation		X	X	X			
Assess Specifications and Standards							
Ensure specification and standard are verified applicability for Phase A; evaluate updates to standards; assess system design specifications	X	X					
Review Performance Validation							
Assess system effectiveness; assess demonstrated margins; assess and verify system and interface performance; verify system and interface performance: technical performance parameters (TPPs)						X	X
Assess Other Systems Engineering Activities							
Assess system trade studies; evaluate TPM adequacy; verify system characteristics: ensure completeness of performance evaluation		X					
Assess system requirements allocations and ensure requirements are verified			X				
Assess Adequacy of System Requirements							
Assess system characteristics: • Ensure completeness of performance evaluation		X					

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
• Ensure mission-unique requirements are defined • Ensure requirements are incorporated into implementing documentation ICD/PRD • Assess mission specifications • Assess mission PRD							
Assess system specifications and interface requirements completeness and accuracy; assess traceability to top-level program requirements: • Ensure derived requirements are identified • Ensure completeness of requirements		X					
Ensure that mission objectives are met; ensure that operational needs are met		X					
Ensure system characteristics are verified (i.e., KPP and TPM)		X	X		X	X	X
Ensure traceability to top-level program requirements is verified: assess system requirements traceability; assess system requirements and interfaces: assess system performance margins			X				
Assess requirements verification and tracking system: • Assess preliminary verification plan • Assess integrated verification strategy • Verification compliance			X				
Assess System Requirements and Interfaces							
Assess system requirements allocation			X		X		
Assess SV external interface definition		X	X	X			

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Requirements Verification and Tracking System							
Assess VCRM adequacy			X	X			
Assess verification tracking system		X	X	X			

5.9 References

Policy-Related

AFI 99-101	Developmental Test and Evaluation, 1 November 1996
AFI 99-102	Operational Test and Evaluation, 1 July 1998
DODI 5000.02	Department of Defense Instruction: Operation of the Defense Acquisition System, 8 December 2008
SMCI 63-1201	Assurance of Operational Safety, Suitability, and Effectiveness for Space and Missile Systems, 16 January 2004

Specifications and Standards

ANSI/EIA 632	Processes for Engineering a System, 7 January 1999
IEEE STD	IEEE Standard for Modeling and 1516/2000, Simulation High Level Architecture – Framework and Rules, 1 September 2000
TOR-2005(8583)-3, Rev. B	Systems Engineering Requirements and Products, 15 April 2010. Distribution limited.
TOR-2006(8506)-4732, Rev. A	Space System Verification Program and Management Process 30 June 2008. Distribution limited.

Handbooks

AOA Handbook	A Guide for Performing Analysis Studies: For Analysis of Alternatives or Functional Solution Analyses, July 2004
INCOSE-TP	Systems Engineering Handbook, 2003-016-02, Version 2a, 1 June 2004
IPPD	DOD Integrated Product and Processes Development Handbook, August 1998
MIL-HDBK-520	Systems Requirements Document Guidance, 5 March 2010
MIL-HDBK-881A	Work Breakdown Structure, 2 January 1998
MIL-STD-499B (Draft)	Systems Engineering Handbook, 1999
NAVAIR	Naval Air Systems Command Guide, 1 May 2003 Systems Engineering
TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, 31 January 2006. Distribution limited.
TOR-2006(8546)-4591	Space Vehicle Test and Evaluation Handbook, 30 June 2006. Distribution limited.

Best Practices

CMMI	Combines EIA 731, System Version 1.1 Engineering Capability Model, and the Software Capability Model (previously independently used for process, development, improvement, and assessment)
TOR-2002(3105)-1668	Acquisition Strategy Consideration, 31 March 2002. Distribution limited.
TOR-2004(3909)-3360, Rev 1	Systems Engineer's Major Reviews for National Security Space System Programs, p. 16, 2 February 2005. Distribution limited.

TOR-2007(8617)-2	Five Common Mistakes Reviewers Should Look Out For

Deliverables

DI-CMAN-81248A	Interface Control Document (ICD), 30 September 2000
DI-ILSS-81335	Design Review Data Package, 2 April 1993 (Canceled)
DI-IPSC-81430A	Operational Concept Description (ODC), 10 January 2000
DI-IPSC-81431A	System/Subsystem Specification, 10 January 2000
DI-IPSC-81432A	System/Subsystem Design Description (SSDD), 10 August 1999
DI-IPSC-81434A	Interface Requirements Specification (IRS), 15 December 1999
DI-SESS-81785	System Engineering Management Plan (SEMP), 14 October 2009

Other

Critical Process Assessment Tool (CPAT)

Chapter 6
Design Assurance

William D. Bjorndahl
Mission Assurance Subdivision
Mark M. Simpson
Electronics and Power Systems Department
Linda J. Vandergriff
Exploitation, Phenomenology, and Analysis Department
Howard Wishner
(Retired)

6.1 Introduction

The Aerospace Corporation's (Aerospace's) recent studies suggest that design issues account for 40 percent of on-orbit anomalies[44]. The purpose of design assurance is to reduce these anomalies by discovering, preventing, and correcting errors or potential escapes early in a system's life cycle where issues are more easily and less expensively corrected.

The design assurance process is an iterative set of planning, analysis, test, and inspection activities which are performed from conceptual to preliminary to detailed design stages to improve the probability that space, launch, and ground systems will meet their intended requirements through all operating conditions and throughout the design life. The design assurance activity concerns itself not only with the assessment of the design but also evaluates, through the product qualification, manufacturing, and test phases, whether or not the design intentions are being achieved. Design assurance encompasses: mission design, system design, hardware (HW), and software (SW) design and test. It also encompasses on-orbit anomaly investigations to the extent that lessons learned are captured and communicated so that necessary improvements can be incorporated into future space programs.

Design assurance is not separate from the design function itself, i.e., it is not completely a mission assurance (MA) function. It should consist of internal processes within the design function and an independent check on the existence of these processes and their efficacy by the MA function.

6.2 Definitions

An **audit** is the planned and formal examination and comparison of a process or activity against a requirement or best practice or established procedure.

[44]Aguilar, J. A., et al., "Design Assurance Guide," TOR-2009-(8591)-11, 4 June 2009. Distribution limited.

Design assurance is a formal, systematic process that augments the design effort and increases the probability of product conformance to requirements and mission success (MS). It independently assesses the development of specifications, drawings, models, and analyses which are necessary to physically and functionally describe the intended product as well as all documentation required to procure, manufacture, test, deliver, operate and sustain the product.

Design synthesis[45] is the translation of requirements, standards, concept of operations (CONOPS), and functions (functional architecture) into solutions (physical architecture) through tradeoffs, technology evaluations, and design optimization.

A **mission assurance plan (MAP)** is the program specific MA plan to validate and verify the concept development, design, manufacturing, integration, test, deployment, and operations of a space system.[46]

Mission design analysis is the evaluation as to whether or not the system consisting of launch vehicle (LV) and space vehicle (SV) is capable of meeting the mission requirements with sufficient margin to guarantee MS.

Risk refers to the evaluation of future events that are possible but not yet realized and carry adverse consequences for a program or mission. Risk is measured by the probability of occurrence (i.e., realization) and by the magnitude of the possible impacts measured in some appropriate scale of assessable consequences (i.e., performance, cost, and schedule metrics).

Risk management is an organized and structured process that has five major tasks: risk management planning, risk identification, risk analysis, risk handling (i.e., avoidance or mitigation), and risk monitoring within a given program or mission.

A **risk management plan (RMP)** is a formal plan endorsed by the program manager or director that documents the organized process of risk management. This document defines the flow of risk management activities and assigns basic responsibilities for their execution. General guidance for this document is found in International Organization for Standards (ISO) Standard 17666 (Space Systems—Risk Management Guide) and in the Department of Defense (DOD) Risk Management (RM) Guide. The RMP can be tailored appropriately for each stage of the acquisition.[47]

---

[45]Based on INCOSE Systems Engineering Handbook definition of "synthesis," Appendix E, page 303.
[46]Guarro, S., "The Mission Assurance Guide: System Validation and Verification to Achieve Mission Success," http://www.aero.org/publications/crosslink/fall2007/03.html
[47]Space Vehicle Systems Engineering Handbook, TOR-2006(8506)-4494. Distribution limited.

Software Requirements and Architectures Review (SAR)[48] is a series of multidisciplinary reviews of the SW requirements, architecture, and test planning of technical products, SW development processes, and the current state of the SW development for all SW items. SAR is a review of the finalized software item (SI) requirements and operational concept.

System design[49] 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. The system design is traceable to the requirements and standards identified for the system.

A **system functional review (SFR)**[50] is a multidisciplinary technical review or a series of reviews that shall be conducted to ensure that the system can proceed into preliminary design. This review assesses the system functional requirements as captured in system specifications and ensures that all required system performance is fully decomposed and defined in the functional baseline. The SFR determines whether the system's functional definition is fully decomposed to a low level and whether the integrated product team (IPT) is prepared to start preliminary design.

The **system requirements review (SRR)**[51] is a multifunctional technical review or series of reviews that shall be conducted to ensure that all system and performance requirements are derived from the initial capabilities document (ICD) and are consistent with program budget, schedule, risk and other constraints.

A **technology readiness assessment (TRA)**[52,53] is a systematic, metrics-based process and accompanying report that assesses the maturity of critical HW and SW technology elements. A critical technology element is a technology or the application of a technology that is necessary to accomplish system operational requirements. The TRA is a review conducted by a team of experienced subject matter experts (SMEs).

---

[48]Peresztegy, L. B., and O'Connor, C. E., "Technical Reviews and Audits for Systems, Equipment, and Computer Software," TOR-2007(8583)-6414, 30 January 2009, page 10. Distribution limited.
[49]INCOSE Systems Engineering Handbook, Appendix E, page 288.
[50]Peresztegy, L. B., and O'Connor, C. E., "Technical Reviews and Audits for Systems, Equipment, and Computer Software," TOR-2007(8583)-6414, 30 January 2009. Distribution limited.
[51]Ibid.
[52]Ibid.
[53]"Technology Readiness Assessment (TRA) Deskbook," Department of Defense, July 2009. http://www.dod.mil/ddre/doc/DoD_TRA_July_2009_Read_Version.pdf

6.3 Objectives

6.3.1 Verify 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 verifying that methods and processes are in place to ensure traceability and compliance of proposed solutions to the requirements baseline.

6.3.2 Ensure 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. Methods, models, and tools are examined to ensure their fundamental capabilities for meeting design intentions.

One way to evaluate design accuracy or completeness is to conduct an audit or a review. Audits and reviews are conducted by experts not only at formal reviews but at other times also. Critical design areas are targeted in audits. For example, a critical audit target might be the evaluation of the accommodation in the design for new technology. Independent audits may be performed for critical characteristics or performance parameters.

6.3.3 Validate Documentation, Configuration Management, and Change Control Processes

During the design, development, manufacturing, and test phases of a program, design decisions and changes need to be documented and configuration managed. The change control process should be examined to ensure: changes are reflected in design drawings and related documentation in a timely manner (i.e., not at the end of a program), changes are actively communicated and resolved for work in progress, and the rationale for any design change is well documented so that questions which may come up years later have a reasonable chance of being answered.

6.3.4 Ensure Producibility

It does no good to design something that cannot be built because the fine tolerance requirements of the design exceed anything that modern manufacturing processes are capable of, or that uses materials or parts for which production processes have not been developed. Ensuring that manufacturing and materials and parts (M&P) engineers are included in the design process is

critical. Early interaction with manufacturing engineering can identify long lead-time items, material source limitations, availability of manufacturing resources, and special production processes.

Also, design drawings can sometimes be unclear or misinterpreted as manufacturing processes and drawing aids are developed. Design assurance examines the design to manufacturing process to ensure that what will be produced is a valid interpretation of the design.

6.3.5 Ensure Designs are Testable and Tests are Valid Demonstrations of Design Intent

Design assurance supports “design-to-test” by ensuring that appropriate design integration and verification is planned and performed. Test equipment and processes should be shown adequate in providing results that validate design requirements. Not only must the physical aspects of test processes be examined (e.g., harness connection into the proper socket), but also how the results of tests are processed and how they are related to and validate design requirements. A test result is no good if the design analysis is flawed or based on wrong assumptions. There have been notable examples of systems that have failed during test because the test design and procedures were based on misunderstandings or ignorance of design features and requirements.

6.3.6 Ensure Designs are Supportable

Design assurance supports the maintenance and logistics support functions by ensuring that the design, once produced, can be maintained. This is especially true of SW where long-term maintenance costs can far exceed the cost of the initial design phase. An example from the HW side might be the consideration of whether or not component parts are likely to become obsolescent before committing to a particular design.

Trades against different solutions should consider how handling and support equipment, test and checkout equipment, logistics support, sparing, facilities, and the maintenance operations concept will be accommodated. This also includes verifying that support equipment meets reliability and mean-time-to-repair (MTTR) requirements.

6.3.7 Ensure Lessons Learned are Captured and Communicated

Lessons learned from anomaly and failure investigations should be captured through adequate documentation and communicated so that corrections to other production or in-development systems can be made.

6.4 Practices

6.4.1 Core Activities

Core activities (i.e., key processes and strategies) necessary for accomplishing design assurance objectives are described in this section. It is important to keep in mind that the accomplishment of these activities requires the efforts of knowledgeable and experienced individuals. The most key practice in design assurance is to ensure that proper expertise, across a wide range of disciplines is enlisted in design assurance efforts. Appendix A3, *Space System Development Analyses*, provides a good indication of the specific and wide range of disciplines and activities required.

6.4.1.1 Develop a Design Assurance Management Plan

Design assurance management begins early during the concept study phase. As concepts are examined, certain basic design decisions should be made. These decisions and the analysis results that they are based on should be thought of as products that require design assurance. It is an important part of design assurance to evaluate, examine, and validate processes for how these design decisions are made. As the program proceeds through concept development into preliminary design phases, design assurance becomes even more critical.

The government program office (PO) team should develop a design assurance management plan that includes the requirements for design assurance and a description of the objective data products required to demonstrate design assurance. The plan should define roles, responsibilities, practices, and tasks to validate and verify that the contractor's design assurance plan is adequate and being carried out.

The contractor needs to develop a design assurance management plan that defines the processes and procedures it will employ to translate the requirements and constraints into a conforming architecture.

Both the government PO and the contractor(s) should ensure that appropriate practices described within the design assurance management plans are flowed down to subcontractors and suppliers. For example, the management plan should specify a process that is used to document and control design changes. This requirement should also be levied on subcontractors (and suppliers if necessary).

6.4.1.2 Conduct Mission Design Analysis

Fundamentally, the purpose of this task is to determine that the mission system is capable of delivering the specific SV to its planned orbit, and that the SV should operate as intended with sufficient margin to guarantee MS.

This analysis is performed to verify adequate mission planning for all operational conditions. It includes examining system level and integration requirements; mission-specific payload integration requirements; ensuring that baseline reliability is preserved and requirements have been met; ensuring that all prior and related flight and test anomalies have been adequately resolved; and that lessons learned have been evaluated and incorporated.

Mission analyses include establishing that the flight trajectory environments and mission design are optimized and satisfy flight safety constraints. It also evaluates whether or not the system has adequate weight, power[54], radio frequency (RF) link, propellant, and consumable margins. Dynamic loads are analyzed to verify booster HW capability and ICD compliance. Guidance, navigation, and control (GN&C) performance is analyzed for acceptable injection accuracy and control stability. Particular emphasis is placed on HW, SW, or unique applications. Evaluations of separation clearance, aerodynamic, thermodynamic, vibroacoustic, electromagnetic interference/electromagnetic compatibility (EMI/EMC), and contamination requirements are performed to verify operation within vehicle capabilities and ICD requirements.

6.4.1.3 Audit the Management of Specifications, Their Communication, and Design Incorporation

The contractor should provide a clear and auditable process of accurately translating requirements into a design. A common source of development issues is 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 great cost.

The process of checking and using heritage designs should be transparent and have clear safeguards to prevent improper reuse. Peer review by experts not associated with the program should be a part of the contractor's processes.

6.4.1.4 Examine Design Methodologies

Design methodologies should be examined to ensure that designs are properly evaluated, reviewed, and documented. Also, an evaluation should be made to ensure that there is a closed loop system for incorporating lessons learned**.**

[54]See for example, Saunders, M., Richie, W., Rogers, J., and Moore, A., "Predicting mission success in small satellite missions," Acta Astronautica, vol. 52, (2003), pp. 361-370. The authors provide useful guidelines for weight and power margins at various stages of system development. The guidelines are provided for a range of programs (albeit medium and small satellites) from new to production line builds.

Audits of analysis procedures and tools along with any incorporated assumptions should be conducted to ensure that these procedures and tools do lead to a design that will meet requirements. A simple example would be to see that units of measurement are consistently defined. Input data such as physical constants should be examined as well as any material physical data that the model may rely on.

It is important to pay attention to design assurance metrics that can discern problems. Drawing metrics are one example of a useful assurance tool. For example, many changes early on during conceptual or preliminary development might be expected whereas many changes in a later phase might not be expected. An examination of drawing change metrics would provide an indicator of how the program is performing. Drawings can also be examined to ensure sign-off by all appropriate engineering disciplines.

6.4.1.5 Control Documents

Configuration management (CM) of program documentation should be demonstrated. Not only must a library system of management be demonstrated, but the communication and use of documents across the program should be examined. If manufacturing is working from old design documents when newer and changed versions exist, problems will occur.

It is necessary to ensure that any approved changes to designs and requirements are documented (along with the decision process itself) in a timely and formal manner. For example, drawing changes, when approved, should be made and new configuration controlled drawings generated and made accessible to all.

6.4.1.6 Perform Change Control

Change control is often associated with document control. However, it also includes the mechanisms whereby changes to documents are carried out. For example, change control boards (CCBs) consisting of a cross-section of program disciplines, should be set up at appropriate times during the program life cycle. Broad participation is necessary to ensure that potential impacts of changes across the system are examined. For example, the replacement of a part on a circuit board may affect a manufacturing process requiring manufacturing engineering to participate in the CCB. In addition, the timing of a signal may change based on the replacement and SW engineering and SE may need to become involved and make changes in embedded SW to account for the timing difference. Examination of the change control process is an important core activity of design assurance.

6.4.1.7 Conduct Independent Design Audits

Targeted independent audits at different levels of design maturity should be performed. Independent assessments should start early during the concept studies and concept development phases. Deficiencies should be documented and communicated to the program. The program should then generate resolution plans and the progress of these resolutions should be briefed to the design audit team periodically until accomplished. One thing to keep in mind is that only half the work of an audit is accomplished during the discovery phase. The other half is accomplished in the communication and ensuring resolution phases. In addition to targeted audits, design assurance includes the independent assessment of the maturity level of various designs, issues, and resolution plans at formal design reviews such as the systems design review (SDR).

6.4.1.8 Perform Test

Continuing design assurance through test is of critical importance. In Section 6.6.1, a key lesson learned is described from a problem that occurred on the Hubble Space Telescope, which was partly because design engineering was not involved in the verification of the design through test. Sometimes, and perhaps often, design engineers who participate in the up-front design of a system, move on to other programs by the time that the initial system is manufactured and gets into test.

During test, the verification of the implementation of design against the requirements occurs and it is important that design engineering is checking to ensure design intent is truly being demonstrated. This should require a number of design assurance efforts. One is the determination that the test procedure and equipment will meet the intent of the test. Second, that the results of the test are significant in terms of information generated and that the results are adequately analyzed and processed to provide a result that verifies a requirement. This is not a trivial process. There have been cases where the parameters of an environmental test have been determined by a physical property measurement that has been either wrong or misapplied. When the environmental test was conducted, the system was damaged (or in some cases undertested).

A specific category of testing, qualification testing, is particularly important and needs close attention by those who seek to ensure design assurance. Qualification testing subjects the design to stressing environments such as thermal cycling, vibration, shock, electromagnetic, and perhaps thermal vacuum. One purpose of qualification testing is to demonstrate the robustness of the design to limits, which include margin to the use and acceptance

environments[55]. Design flaws which need to be corrected may be caught during this testing. Examples of design flaws include inadequate structural support or mismatch of thermal expansion that leads to failure.

6.4.1.9 Perform Lessons Learned

One of the major contributions to the National Space Enterprises' body of knowledge is Aerospace's well maintained explicit and tacit space systems knowledge repository. Through a continual process of program evaluation to capture innovative solutions, analyze failures, past system performance, current technology trends, and indications and warnings for future programs, Aerospace is able to anticipate and recommend best practices for future space system acquisition. 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.

6.4.2 Standards/Recommended Practices

Associated standards and recommended practices for design assurance can be found in many of the references given in Section 6.9. A good overall guide is the Design Assurance Guide[56]. This guide to recommended practices defines key design assurance enterprise attributes and program elements. A key design assurance enterprise attribute for example might be the presence of a SME in a particular area of the system design. A key program element might be a comprehensive verification matrix. The Design Assurance Guide describes a risk management based approach for assessing a program's design maturity.

Another key reference is TOR-2007(8583)-6414 *Technical Reviews and Audits for Systems, Equipments, and Computer Software*. This document defines the major design review milestones: the SDR, the preliminary design review (PDR), and the critical design review (CDR). It also provides a list of the items to be evaluated during these reviews. These lists can be used (as checklists) by independent audit or review teams either during the milestone reviews or at intermediate times in the program's life cycle as appropriate.

6.5 Key Lessons Learned

Sections 6.6.1 through 6.6.4 are brief descriptions of design failures that may have been avoided had design assurance processes been in place and followed. At the end of each description are notes made to illustrate specific design assurance principles or practices that, if followed, would have helped avoid the

[55]Perl, E., "Test Requirements for Launch, Upper Stage, and Space Vehicles," TR-2004(8583)-1 Rev. A, SMC-TR-06-11, 6 September 2006. Distribution limited.
[56]Aguilar, J. A., et al, "Design Assurance Guide," TOR-2009(8591)-11, 4 June 2009. Distribution limited.

problems that occurred. References are given for those who would like to dig deeper. There are also many more reports and commentaries available on the web.

6.5.1 Hubble Space Telescope

The Hubble Space Telescope was launched and expected to provide clear pictures of the universe. The first pictures were fuzzy because of a spherical aberration in the primary lens. The spherical aberration was traced to a test and measurement error associated with special (ground) test equipment and procedures. A NASA report[57] highlights numerous deficiencies and lessons learned from this event.

Page 10 of the NASA report notes the following. “In fact, the designer of the original Reflective Null Corrector and Inverse Null Corrector stated to the Board that he never had been in the tower to see the device in actual operation.”

Another statement from the same page of that report is “Baseline design criteria used in the final design phase (PDR through CDR) served as the basis for special inspections (critical source, receiving, in-process, and final). These requirements should have encompassed all STE such as the Null Correctors used to define critical performance parameters.”

The lesson from this example is that knowledgeable individuals (i.e., the designer) should have been involved in the downstream test processes to ensure that design requirements were accounted for in test equipment design and test process development.

6.5.2 Wide-Field Infrared Explorer Mission Failure[58,59]

The WIRE mission was designed to perform an infrared survey of the sky and provide information to support studies of the evolution of galaxies. To perform the survey measurements, it was necessary to keep the telescopic assembly (which utilized silicon arsenide detectors) cold using solid hydrogen.

During power-on of the pyro electronics box, field-programmable gate arrays (FPGAs) inside the box were placed in a state that allowed energy to be prematurely applied to the pyro devices that were to disengage a cover for the detector assembly. When this premature disengagement occurred, the hydrogen vented at a rate which was rapid enough to cause the vehicle to spin. The

[57] Rodney, G. A., “Hubble Space Telescope: SRM&QA Observations and Lessons Learned,” NASA-TM-105505.
[58] ftp://ftp hq.nasa.gov/pub/pao/reports/1999/wire_summary.pdf
[59] http://klabs.org/richcontent/Reports/nasa_wire_lesson.pdf

premature loss of the cryogen caused the failure of the primary mission of the instrument.

Design failure occurred in two areas. First, the initial design did not account for the FPGA start-up transient, and this design was not peer reviewed by an outside expert or team of experts. Secondly, "The design of the test box focused more on verifying that pyros received proper current when they were supposed to fire, with little consideration given to verifying that the pryos did not receive current when they were not supposed to fire."[60]

The lessons learned on this system were that transient states must be evaluated for effect on the overall system; timely independent expert peer review with a focus on what is missed is essential; and tests should be designed to test both the proper positive and negative functions.

6.5.3 Genesis Mission Mishap[61]

The purpose of the Genesis mission was to collect samples of the solar wind. It flew about a million miles to an orbit between the earth and the sun where it remained for about 23 months. Upon its return to earth, a parachute was to be deployed to allow the safe landing of the payload. The parachute did not deploy and the vehicle hit the ground at about 190 miles per hour.

The gravity switch which was to detect the entry into the Earth's atmosphere was inverted in the design. The force on the sensor in response to the deceleration was in the opposite direction to what it should have been. Electrical contact was not made and the parachute was not deployed.

The peer design review process appears weak for lack of the right technical expertise and no end-to-end SE responsibility. Although verification by inspection was conducted, it was conducted by an electrical engineer not familiar with the mechanical operating characteristics of the switch. In addition, reviewers may have been relying on the upcoming centrifuge verification test.

The initially planned centrifuge verification test was deleted because of schedule pressure. It was assumed that a "quick lift" test would uncover any electrical problems with the box and demonstrate switch contact through momentary continuity (forgetting the need for a specific electromechanical switch orientation).

The Red Team Review was inadequate for a number of reasons: not enough time for review; the lack of specific expertise (electrical power rather than a

[60] Ibid.
[61] http://www.nasa.gov/pdf/149414main_Genesis_MIB.pdf

combination of electrical and electromechanical or mechanical) for review of the switch operation; and, a belief that the design was “heritage” although substantial design modifications had been made.

The lessons learned on this system were that timely independent expert peer review is necessary and that “faster, better, cheaper” by reducing testing saved nothing.

6.5.4 Mars Climate Orbiter

This is an example that illustrates the need of design assurance for SW. Following are words directly from the Phase 1 report of the Mishap Investigation Board.[62]

> “The MCO Mission objective was to orbit Mars as the first interplanetary weather satellite and provide a communications relay for the MPL which is due to reach Mars in December 1999. The MCO was launched on December 11, 1998, and was lost sometime following the spacecraft's entry into Mars occultation during the Mars Orbit Insertion (MOI) maneuver. The spacecraft’s carrier signal was last seen at approximately 09:04:52 UTC on Thursday, September 23, 1999.
>
> The MCO MIB has determined that the root cause for the loss of the MCO spacecraft was the failure to use metric units in the coding of a ground software file, “Small Forces,” used in trajectory models. Specifically, thruster performance data in English units instead of metric units was used in the software application code titled SM_FORCES (small forces). A file called Angular Momentum Desaturation (AMD) contained the output data from the SM_FORCES software. The data in the AMD file was required to be in metric units per existing software interface documentation, and the trajectory modelers assumed the data was provided in metric units per the requirements.
>
> During the 9-month journey from Earth to Mars, propulsion maneuvers were periodically performed to remove angular momentum buildup in the on-board reaction wheels (flywheels). These Angular Momentum Desaturation (AMD) events occurred 10-14 times more often than was expected by the operations navigation team. This was because the MCO solar array was asymmetrical relative to the spacecraft body as compared to Mars Global Surveyor (MGS) which had symmetrical solar arrays. This asymmetric effect significantly increased the Sun-

[62] ftp://ftp.hq.nasa.gov/pub/pao/reports/1999/MCO_report.pdf, “Mars Climate Orbiter Mishap Investigation Board, Phase 1 Report,” November 10, 1999.

> induced (solar pressure-induced) momentum buildup on the spacecraft. The increased AMD events coupled with the fact that the angular momentum (impulse) data was in English, rather than metric, units, resulted in small errors being introduced in the trajectory estimate over the course of the 9-month journey. At the time of Mars insertion, the spacecraft trajectory was approximately 170 kilometers lower than planned. As a result, MCO either was destroyed in the atmosphere or re-entered heliocentric space after leaving Mars' atmosphere."

It is not hard to see that design assurance could have played a key role in preventing this mishap. A review of the requirements and interfaces between programs and verification of the SW should have identified the need for a translation to metric units by the ground SW. Following are words directly from the Mishap Investigation Board report:

> "The Software Interface Specification (SIS), used to define the format of the AMD file, specifies the units associated with the impulse bit to be Newton-seconds (N-s). Newton-seconds are the proper units for impulse (Force x Time) for metric units. The AMD software installed on the spacecraft used metric units for the computation and was correct. In the case of the ground software, the impulse bit reported to the AMD file was in English units of pounds (force)-seconds (lbf-s) rather than the metric units specified. Subsequent processing of the impulse bit values from the AMD file by the navigation software underestimated the effect of the thruster firings on the spacecraft trajectory by a factor of 4.45 (1 pound force=4.45 Newtons)."

The lesson learned on this system was that a comprehensive review for SW and interface compatibility was required to catch this error.

6.6 Task Execution by Phase

Figure 6-1 shows design assurance activities associated with the defense acquisition process.[63] Appendix A3 lists mission assurance verification tasks to be accomplished during each phase of a program. This list which is quite long and comprehensive contains a number of verification tasks associated with design assurance. Sections 6.7.1 through 6.7.5 provide a synopsis of some of the key design assurance tasks by program phase.

[63] DODI 5000.02 Guidance

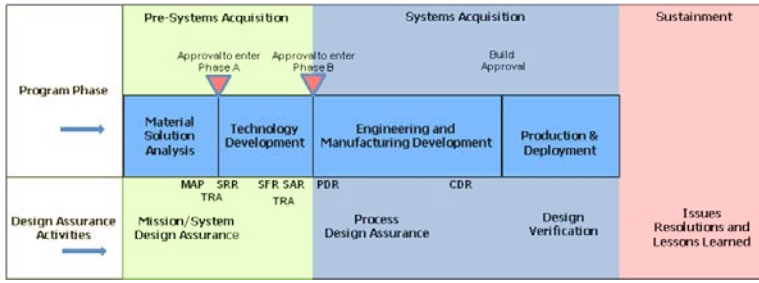


Figure 6-1. Design Assurance and the Defense Acquisition Management System

6.6.1 Phase 0 – Concept Studies

About three-quarters of the total system life cycle costs are based on decisions made before Milestone A[64]. This means the decisions made in the pre-Milestone A phase (Phase 0) are critical to help avoid or minimize cost and schedule overruns later in the program. Design assurance performed in pre-systems acquisition has a critical impact on the total system life cycle cost.

Phase 0 activities include those necessary to initiate the request for proposal (RFP). Specific activities include specification of system design standards, design processes, and design products required by the RFP. It is necessary to assess the adequacy of available simulation and modeling tools. It is also necessary to determine industry capabilities for the proposed system and the maturity of design and manufacturing processes needed to meet system requirements and to incorporate new technologies as required. A TRA should be conducted. To provide these assessments it may be necessary for Aerospace and other federally funded research and development centers (FFRDCs) or systems engineering and technical assistance (SETAs) to have access to contractor design capabilities and to contractor information that provides evidence of the maturity of product designs.

During Phase 0 the extent of tailoring of requirements should be determined and included in an initial MA plan. Many, if not all of the standards on which requirements are based, will contain some measure of design assurance activities, and setting up the tailoring baseline at the outset mitigates issues downstream as designs and tests are being generated and finalized.

Aerospace may be asked to develop alternate system designs, conduct trade studies, and provide detailed “sizing” of selected concepts. Design assurance

[64]National Research Council, *Pre-Milestone A and Early-Phase Systems Engineering A Retrospective Review and Benefits for Future Air Force Acquisition*, http://www.nap.edu/catalog.php?record_id=12065, 2008.

would consist of an assessment and verification of the accuracy and completeness of these studies. It would also provide an input to an assessment of program risks associated with technical feasibility and performance to baseline schedule and funding. These risks should be identified and along with their proposed mitigations documented in an RMP.

6.6.2 Phase A – Concept Development

During the concept development phase (Phase A), design assurance focuses on program plans to ensure incorporation of the design standards, design processes, and design products as specified in the contract. Much of design synthesis begins in Phase A and so the design management system should be evaluated.

It is necessary to examine program execution plans in terms of the allocated resources during the integrated baseline review (IBR). It is important to gain insight into allocated resources for prime and major subcontractors' as early as possible to identify potential risks in downstream design activities.

Four important reviews or series of reviews occur during this phase of the program: the SRR, SFR, TRA, and SAR[65].

Design assurance activities that support the completion of a successful SRR include conduction of trade studies to optimize system and subsystem designs, initial allocation of system requirements to HW and SW, and evaluation of capability to process the proposed design given available program resources. During this time, appropriate weight and power margins should be specified and tracked as more detail about the HW design and power requirements become known.

The TRA is also a critical milestone for design assurance during Phase A. Often new technology insertions require new design approaches and these approaches can affect multiple systems or subsystems. For example, a new electronic technology might impact not only the electrical design of a box, but also because of necessary heat dissipation, the thermal design of the spacecraft. Design assurance should confirm that concept studies accurately identify the risks and that initial baseline plans adequately set aside time and funding for the tasks required to incorporate new technologies into the conceptual designs.

The SFR is one of the last reviews prior to entering preliminary design and it is important that traceability of the selected design to system key performance parameters (KPPs) is clearly shown and that interface requirements are

[65]Peresztegy, L. B., and O'Connor, C. E., "Technical Reviews and Audits for Systems, Equipment, and Computer Software," TOR-2007(8583)-6414, 30 January 2009.

comprehensively identified. Much time can be wasted during subsequent detailed design if these requirements are not specified.

The SAR is held after the SFR and is a multidisciplinary review of the SW requirements and development process, architecture, and test planning products. Because operational functionality depends on complex interactions of SW and HW, one of the important concerns for design assurance is that a viable path with respect to program budget and schedule exists to develop HW and SW concurrently. This may entail sharing of development resources or the production of duplicate resources such as test beds to accomplish this objective. In addition, SW/HW interface requirements should be clearly defined in detail to preclude wasted money and time in later detailed design.

6.6.3 Phase B – Preliminary Design

Preliminary Design (Phase B) is the beginning of a more detailed design at the configured item (CI) level and culminates with a PDR. As the design matures, assurance processes expand their focus to encompass design for manufacturing (including an evaluation of manufacturing process qualification) and design for testability (ensuring that design not only facilitates test processes but that the tests themselves will validate the design requirements).

Both design for manufacturing and design for testability objectives can be supported by incremental design model verification. As breadboards, brass-boards, and flight-like prototypes are built, design assurance assesses the associated demonstrations and test results to verify that they not only meet requirements, but are consistent with design analyses. Higher-level mockups may also be used to develop detailed design criteria and help support design analyses and required models, such as a SV dynamics and thermal math model. SW prototypes may be used to provide early assurance that the proposed design will meet performance criteria.

Design assurance includes ensuring that appropriate specialty engineering peer reviews occur. It also verifies the existence and compatibility of the physical, functional, and SW interfaces among CIs and other supporting test and integration equipment (including the facilities in which tests are conducted). Ground and launch systems are also included.

6.6.4 Phase C – Complete Design

Complete Design (Phase C) is the continuation of design activities and the completion of CI design prior to the manufacturing readiness review and the start of production. Phase C culminates with a formal, multidisciplinary CDR of each CI followed by a system level CDR.

During this phase it is important to ensure that the findings from design peer reviews have been captured and implemented. Producibility analysis should be completed, and the state of design drawings should be such that clear manufacturing and production paperwork (special instructions and manufacturing aids) can be generated.

Detailed design compatibility should be completed during this phase. Compatibility between CIs, support equipment (ground and test), and SW should be examined. It is often at this stage that problems originate that show up later. This is because once the CDR has been completed, teams for different pieces of HW focus on their specific responsibilities as the HW moves into production. It is only later when interfaces are made that it is discovered that specific details of the interfaces have been missed or misinterpreted. When communication between two electronic boxes is involved, SW is also affected, and, SW engineering is often asked to determine if a SW fix can be generated.

In addition to assessing the design products, MA as part of the design assurance activities will also continue to independently audit design processes and examine related design metrics to 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 design margins; check the design for compliance to industry standards (Aerospace's best practices), and check applicable lessons learned databases for similar developments.

During this phase, detailed qualification plans should be complete and updated with evidence of on-going qualification activities. Associated results should be examined to ensure consistency with design analyses and predictions. Where commercial off-the-shelf (COTS) and heritage HW and SW items are being used, MA will conduct a detailed evaluation of the item's ability to satisfy the unique program performance, quality, and environmental requirements.

6.6.5 Phase D – Build and Operations

Build and Operations (Phase D) is typically divided into three sub-phases: Phase D1, Fabrication and Integration; Phase D2, System Fielding, Test, and Check-out; and Phase D3, Operations and Disposal (or Sustainment). Design assurance activities during these sub-phases are discussed separately in Sections 6.6.5.1 through 6.6.5.3.

6.6.5.1 Phase D1 – Fabrication and Integration

During Phase D1, the build and operations phase, it is important that design engineering and assurance ensure that what is being built and tested is consistent

with what was intended. This was a key lesson learned from the Hubble Space Telescope program (described in Section 6.5.1).

During this phase, demonstration and test results are used to verify the design meets requirements as well as ensure consistency with design analyses and predictions. Tested and qualified items are ensured 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 ensure that design errors encountered in this phase are fully resolved and that the corrective action (CA) 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, ensuring that all constraints are met over the mission envelope. Mission-specific performance metrics 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 are also addressed by design assurance. Finally, operations and maintenance (O&M) design assurance tasks will focus on the flight SW and ground system SW and HW upgrades and bug fixes.

6.6.5.2 Phase D2 – System Fielding, Test, and Check-Out

During Phase D2, design assurance will verify that the system performance meets specification. Any updates to models and simulations based on observed performance should be made and documented during this phase.

Anomalous conditions will be investigated for root cause and CA during this phase. It is important that design personnel assigned to these investigations include personnel who are experienced and participated in the system design. They will then be able to adequately capture lessons learned and pass them on to on-going programs and functional organizations.

6.6.5.3 Phase D3 – Operations and Disposal (or Sustainment)

During Phase D3, anomalies may continue to occur and the remarks made in Section 6.6.5.2 apply here also. As the operational system ages, performance characteristics may change and design engineers should evaluate how these changes might be used as data to modify design life simulations. Lessons learned from this benchmarking activity should be documented and passed on to other programs along with recommendations to the functional organizations that maintain the simulations and models.

6.7 Government and Contractor Enabling Processes and Products

As discussed earlier, the basic objectives of design assurance are to ensure 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 MS and are considered among the most important MA processes. 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. Sufficiency is viewed as the ability of a design element to perform its intended function overall operating conditions and throughout its mission life.

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 review of the prime contractor's design management plan to ensure that these compliance documents are being invoked should be done. 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.

6.7.1 Phase 0 – Concept Studies

Independent Aerospace-led design analyses and simulations are conducted to ensure that the system architecture, design, and interfaces will meet the program requirements. A valuable capability of 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 also ensure that enabling technologies have been identified. This aids in determining the feasibility of attaining the required technology readiness levels given the program's roadmaps for technology demonstration. This independent Aerospace assessment is needed to ensure that the program is not based on unwarranted assumptions both in terms of the identification (or lack thereof) of critical technologies and planned demonstrations of technology readiness.

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 ensure that industry standard tools are used to ensure compatibility with Aerospace resources.

6.7.2 Phase A – Concept Development

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 ensure the equipment/SW obsolescence and planned upgrades have been adequately considered. As outlined in the task database, emphasis is placed on ensuring that non-development item (NDI), reuse code, and COTS/government off-the-shelf (GOTS) products are fully supportable.

6.7.3 Phase B – Preliminary Design

As the system design is promoted to the detailed design phase, a key task early in Phase B is to ensure 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 ensure 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.

6.7.4 Phase C – Complete Design

During the detailed design effort, design documentation should be assessed against a drawing checklist and should exhibit the appropriate signoff from the supporting specialty engineering areas. If possible, design error metrics should be collected and trended. An audit of manufacturing paperwork should be conducted to ensure that the design has been properly and clearly captured in the work instructions. Since this phase culminates in the CDR, and the various product teams will soon begin manufacturing, a thorough examination of interface requirements should be conducted to prevent missed or crossed “wires.”

6.7.5 Phase D – Build and Operations

During Phase D, the first production “as-built” items are reviewed to ensure they reflect the “as-designed” baseline, and that the manufacturing results are consistent with design analyses. As the first flight articles are integrated and sent to the field in Phase D2, a key task would then be to ensure that higher-level

integration and system demonstration results are consistent with previous design analyses. Additionally, Aerospace would ensure 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 ensuring that adequate propellant margins exist and that the ground system and flight SW designs are compatible with the changes to the SV.

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

6.8 Practice Task Application Example

Following is an example of how design assurance might be implemented. It is a simple example but illustrates some of the key design assurance activities as they occur during the life of a program. The genesis of the example is this: A university consortium has developed new solid-state technology which can potentially increase the capability of a system to handle communications traffic. Now, a program is initiated to investigate the feasibility of building a system around this technology.

For purposes of illustration, only some high-level design assurance activities are highlighted to give the reader an idea of what the tasks are at various stages within the program life (the acquisition cycle). More complete lists of activities can be derived from information in the following references: the Design Assurance Guide[66]; Guidelines for Space Systems Critical Gated Events[67]; Technical Reviews and Audits for Systems, Equipment, and Computer Software[68]; and in Appendix A3. It should be emphasized again at this point that the intent of design assurance is to independently ensure that the processes exist to accomplish the described activities, and that they are being carried out by the appropriate disciplines. It should not be the intent to redo the tasks described. Also, and again, the independent assessment activities should be carried out by knowledgeable and experienced individuals.

Table 6-1 is a general checklist showing the tasks as a function of program phase, and in Table 6-2 specific phases are broken out with respect to example design assurance activities that would be carried out during that phase.

[66]Aguilar, J. A., "Design Assurance Guide," TOR-2009(8591)-11, 4 June 2009.
[67]Tosney, W. F., Cheng, P. G., and Juranek, J. B., "Guidelines for Space Systems Critical Gated Events," TOR-2009(8583)-8545, 9 May 2008. Distribution limited.
[68]Peresztegy, L. B., and O'Connor, C. E., "Technical Reviews and Audits for Systems, Equipment, and Computer Software," TOR-2007(8583)-6414, 30 January 2009. Distribution limited.

Table 6-1. Example Set of Design Assurance Tasks and Phase Checklist

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Perform analysis of alternatives (AOAs) and associated tasks	X						
Assess system architecture	X						
Assess system trade studies		X					
Evaluate similar concepts and technologies	X	X	X	X			
Assess interface risk and impacts on other systems and architectures		X					
Conduct system architecture development efforts and produce the system view (SV) architecture products, if required		X					
Assess technology maturity and selection	X	X	X	X			
Manufacturing assurance, manufacturing phase	X	X	X	X			
Assess and evaluate design studies	X	X	X	X	X		
Validate and support space segment design						X	
Verify space segment on-orbit mission design							X
Verify space segment system design		X	X	X			
Verify the detailed preliminary design			X				

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify the preliminary space vehicle, subsystem, and unit designs			X				
Ensure/verify/validate the adequacy of the segment designs		X	X	X		X	

In Phase 0, Concept Studies, various design concepts which utilize the new technology are developed. An assessment of the adequacy of existing design tools and initial contractor capabilities is made. Careful consideration is given to program descriptions and implied requirements for RFPs.

In Phase A, Concept Development, the design and its requirements become clearer. It is important to ensure that designs and design decisions are managed.

In Phase B, Preliminary Design, CI level design begins and designs for manufacturing and testability are taken into account. Requirements are being tied to verification methods. The feasibility of verification methods both from a test and analysis standpoint needs to be examined.

In Phase C, Complete Design, it is important to ensure that design is complete and that all interface requirements have been properly taken into account.

In Phase D1, Fabrication and Integration, as the design gets into manufacturing, changes will most likely be required and lessons learned associated with these changes will be generated.

In Phase D2, System Fielding, Test, and Checkout, verifying that design intent is met is key at this stage of the program.

In Phase D3, Operations and Disposal (or Sustainment), as operational anomalies arise, it is important that the investigation teams are staffed with program experienced design personnel so that the best chance exists for determining probable root cause and CA and that lessons learned are properly captured and documented.

Table 6-2. Practice Task Application

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Specify standards for design and design products	X						
Assess and document design tool adequacy	X						
Provide an assessment of industry design capability	X						
Assess design and manufacturing capability for insertion of new technology	X						
Provide inputs to MA/RM plans	X						
In light of above assessments, provide input to RFP, or determine adequacy of RFP	X						
Ensure system-level requirements are known and understood and allocated to the next level down (e.g., communications subsystem)		X					
Assess adequacy of allocated design resources		X					
Assess design management process		X					
Ensure appropriate margins on power/weight allocations		X					
Document technology insertion risks from design/manufacturing perspectives and ensure resources are allocated for successful insertion		X					
Ensure that interface requirements are comprehensively identified		X					

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess the program's approach for SW development and identify shared (with HW) development resources and viability/risks associated with plan		X					
Ensure adequacy of follow-on RFP		X					
Verify execution of design management plan			X				
Assess requirements flow-down			X				
Assess interface requirements tracking			X				
Assess verification linkage to requirements			X				
Ensure technology insertion plans are developed with appropriate demonstrations to meet design requirements			X				
Ensure specialty design engineering functions and peer reviews are being carried out			X				
Ensure design testability			X				
Ensure design producibility			X				
Ensure state of completeness of drawings to enable clear manufacturing and production paperwork				X			
Ensure design compatibility across HW and HW/SW interfaces				X			

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure qualification plans are complete and qualification results generated to date are consistent with design analysis and predictions				X			
Ensure consistency in design intent across space, ground, and launch systems				X			
Ensure weight and power margins are appropriately updated				X			
Ensure consistency across design intent (requirements), modeling and simulation (M&S), and test verification planning				X			
Participate to ensure that the non-conformance and anomaly resolution processes are identifying and capturing design issues					X		
Verify that design changes are reviewed at a CCB level and that design and associated assembly paperwork is updated and communicated					X		
Capture and communicate lessons learned					X		
Verify as-built HW configurations and interfaces					X		
Verify ground and system HW/SW tests demonstrate design intent (requirements)					X		
Verify performance meets design intent (requirements)						X	
Ensure anomaly investigations are supported by design engineers and design specialty engineers who are knowledgeable about the design						X	

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure CAs associated with design are captured and communicated to other ongoing programs						X	
Update M&S						X	
Capture and communicate lessons learned						X	
Ensure anomaly investigations during the operational phase are supported by design engineers and design specialty engineers who are knowledgeable about the design							X
Ensure CAs associated with design are captured and communicated to other ongoing programs							X
Ensure aging impacts are evaluated and that models and simulations are updated							X
Capture and communicate lessons learned							X

6.9 References

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 Institute of Electrical and Electronic Engineers (IEEE), American Institute of Aeronautics and Astronauts (AIAA), and American Society for Testing and Materials (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.

Policy-related

AFI 99-101	Developmental Test and Evaluation, 1 November 1996
AFI 99-102	Operational Test and Evaluation, 1 July 1998
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

Specifications and Standards

AFSPCMAN 91-710	Range Safety User Requirements Manual, Volumes 1–7, (Replaces EWRR 127-1), 1 July 2004
AIAA S-080-1998	Space Systems, Metallic Pressure Vessels, Pressurized Structures, and Pressure Components, 1 September 1998

AIAA S-081-2000	Space Systems – Composite Overwrapped Pressure Vessels (COPVs), 1 December 2000
AIAA S-111 2005	Qualification and Quality Requirements for Space Qualified Solar Cells, 1 May 2005
AIAA S-112 2005	Qualification and Quality Requirements for Space Qualified Solar Panels (draft), 1 May 2005
AIAA S-113-2005	Criteria for Explosive Subsystems and Devices Used on Space and Launch Vehicles, 30 June 2005
AIAA S-114-2005	Moving Mechanical Assemblies Standard for Space and Launch Vehicles (replaces MIL-A-83577C), 30 June 2005
ANSI/EIA 632	Processes for Engineering a System, 7 January 1999
ASTM E1548-04	Standard Practices for Preparation of Aerospace Contamination Control Plans, Tailoring and Background, 12 September 2004
COE UIS	Common Operating Environment (COE) User Interface Specification (UIS), Version 4.3, (CM Reference: 59314), December 2003
EIA/IEEE J-STD-016 3.2	Software Development Specification, Program-Unique Documents, 1995
IEEE 1471	IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, 21 September 2000
IEEE STD 1516/2000	IEEE Standard for Modeling and Simulation High Level Architecture – Framework and Rules, 1 September 2000
ISO/IEC STD 15939	Software Engineering – Software Measurement Process, 11 July 2002

MIL-STD-1367A	Packaging, Handling, Storage, and Transportability Program Requirements for Systems and Equipments, 2 October 1989
MIL-STD-1540E, Rev. A	Test Requirements for Launch, Upper-Stage, and Space Vehicles, 31 January 2004 (replaces MIL-STD-1540C). See also TOR-2004(8583)-1, Moving Mechanical Assemblies Standard for Space and Launch Vehicles (Draft 1). Distribution limited.
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-STD-1833	Test Requirements for Ground Equipment and Associated Computer Software Supporting Space Vehicles, 13 November 1989
MIL-STD-461E	Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment, 20 August 1999
MIL-STD-470B	Maintainability Program for Systems and Equipment, 30 May 1989
MIL-STD-810F, Notice 3	Environmental Engineering Considerations and Laboratory Tests, 5 May 2003
NASA-TM-105505	Hubble Space Telescope: SRM&QA Observations and Lessons Learned, 12 May 2008
TOR-2003(8583)-2894	Space Systems – Structures Design and Test Requirements, 2 August 2004. Distribution limited.
TOR-2003(8583)-2895, Rev. 1	Solid Rocket Motor Case Design and Test Requirements, 22 December 2004. Distribution limited.

TOR-2003(8583)-2896	Space Systems – Flight Pressurized Systems (replaces MIL-STD-1522A), 31 August 2003. Distribution limited.
TOR-2004(3909)-3315, Rev. A	Parts, Materials, and Process Control Program for Space Vehicles, 12 August 2004 (replaces MIL-STD-1546). Distribution limited.
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). Distribution limited.
TOR-2004(3909)-3405	Metrics-Based Software Acquisition Management, 5 May 2004. Distribution limited.
TOR-2004(3909)-3537, Rev. B	Software Development Standard for Space Systems, 11 March 2005. Distribution limited.
TOR-2004(8583)-3275	Survivability Program Management for Space Systems, 31 March 2005. Distribution limited.
TOR-2004(8583)-5, Rev. 1	Space Battery Standard, 11 May 2005. Distribution limited.
TOR-2005(8583)-1, Rev. A	Electromagnetic Compatibility Requirements for Space Equipment Systems, M. Dunbar, 8 August 2005. Distribution limited.
TOR-2005(8583)-2	Electrical Power Systems, Direct Current, Space Vehicle Design Requirements, 11 May 2005. Distribution limited.
TOR-2005(8583)-3, Rev. A	Systems Engineering Requirements and Products, 29 September 2005. Distribution limited.
TOR-2005(8583)-3970	Mass Properties Control Standard for Space Vehicles, 20 July 2005. Distribution limited.
TOR-2006 (8506)-4732	Program and Management Process, Space System Verification 30 June 2006. Distribution limited.

TOR-2007(8583)-6414	Technical Reviews and Audits for Systems, Equipment, and Computer Software, 30 January 2009
TOR-2008(8583)-8492	Technical Requirements for Wiring Harness Space Vehicle, Design and Testing, General Specification for, 28 April 2008. Distribution limited.
TOR-98(1412)-1, Rev. A	Parts, Materials, and Process Control Program for Expendable Launch Vehicles-Revision A, 1 January 2004. Distribution limited.
TR-2004(8583)-1, Rev. A (also published as SMC-TR-06-11)	Test Requirements for Launch, Upper Stage, and Space Vehicles, 6 September 2006

Handbooks

—	INCOSE System Engineering Handbook, A Guide for System Life Cycle Processes and Activities, Version 3.2.2, 25 January 2010
ISBN 1-88-4989	Spacecraft Thermal Control Handbook, Volume 2, Cryogenics 14-4 (v.2), AIAA, 2002
ISBN 1-884989-11X	Spacecraft Thermal Control Handbook, Volume 1, AIAA, 2002
ISBN 1-884989-15-2	Space Modeling and Simulation Roles and Applications Throughout the System Life Cycle, AIAA, 2004
MIL-HDBK-17-2F	Composite Materials Handbook, 17 June 2002
MIL-HDBK-5J	Metallic Materials and Elements for Aerospace Vehicle Structures, 31 January 2003
MIL-HDBK-217F	Reliability for Electronic Equipment, 2 December 1991

MIL-HDBK-83575	General Handbook for Space Vehicle Wiring Harness Design and Testing
TOR-2005(8583)-4474	Requirements for End-of-Life Disposal of Satellites Operating at Geosynchronous Altitude. Distribution limited.
TOR-2006(3904)-1	Digital ASIC/PLD Development Handbook for Space Systems, 30 November 2005. Distribution limited.
TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, 31 January 2006. Distribution limited.
TOR-2006(8546)-4591	Space Vehicle Test and Evaluation Handbook, 30 June 2006. Distribution limited.

Best Practices

SMC-TR-98-35	Tribology in the Space Environment, 15 October 1997
TOR-2009(8583)-8545	Guidelines for Space Systems Critical Gated Events, 9 May 2008. Distribution limited.
TOR-2009(8591)-11	Design Assurance Guide, 4 June 2009. Distribution limited.

Deliverables

DI-CMAN-81248A	Interface Control Document (ICD), 30 September 2000
DI-EMCS-80199B	Electromagnetic Interference Control, 20 August 1999
DI-EMCS-80201B	Electromagnetic Interference Test Procedures, 20 August 1999
DI-ILSS-81335	Design Review Data Package, 2 April 1993
DI-IPSC-81430A	Operational Concept Description (OCD), 10 January 2000

DI-IPSC-81431A	System/Segment Interface Control Specification, 25 January 1993
DI-IPSC-81432A	System/Subsystem Design Description (SSDD), 10 August 2002
DI-IPSC-81434A	Interface Requirements Specification (IRS), 15 December 1999
DODI 5000.02	Operation of the Defense Acquisition System 8 December 2008

Other

Crosslink	Mission Assurance, "The Mission Assurance Guide: System Validation and Verification to Achieve Mission Success," Vol. 8, No. 2, Fall 2007
GAO-02-701	Capturing Design and Manufacturing Knowledge, Early Improves Acquisition Outcomes, July 2002

"Predicting mission success in small satellite missions," Acta Astronautica

Critical Process Assessment Tool (CPAT)

ftp://ftp.hq nasa.gov/pub/pao/reports/1999/MCO_report.pdf, "Mars Climate Orbiter Mishap Investigation Board, Phase 1 Report," 10 November 1999.

ftp://ftp.hq nasa.gov/pub/pao/reports/1999/wire_summary.pdf

http://klabs.org/richcontent/Reports/nasa_wire_lesson.pdf

http://www.nasa.gov/pdf/149414main_Genesis_MIB.pdf

Pre-Milestone A and Early-Phase Systems Engineering: A Retrospective Review and Benefits for Future Air Force Acquisition, National Research Council, http://www.nap.edu/catalog.php?record_id=12065, 2008

Technology Readiness Assessment (TRA) Deskbook, Department of Defense, July 2009

Chapter 7
Manufacturing Assurance

Steven R. Robertson
Parts, Materials and Processes Department
Arthur L. McClellan
Product and Process Assurance Department
Dan W. Hanifen
GEOINT Development Office
May M. Kwan
Product and Process Assurance Department

7.1 Introduction

Manufacturing engineering encompasses the use of available and certified materials, parts, and manufacturing processes to create products that fulfill documented design requirements. The manufacturing process is often complex and susceptible to errors from many sources such as incorrect design information, material defects, tolerance errors, processing errors, operator errors, and calibration errors. Prudent and successful manufacturing processes use a system of checks and validations (i.e., in-process tests, inspections, and analysis) to verify that, at each stage of the manufacturing sequence, the end product of a particular process meets the quality standards for that stage of the manufacturing sequence.

To produce high-quality and repeatable products that meet the as-designed requirements, manufacturing engineers work closely with systems engineering, design engineering, parts, materials, and processes (PMP) engineering, test engineering, reliability engineering, safety engineering, quality assurance, and configuration management. This interaction occurs throughout the program life cycle, from preliminary design, through detailed design, product development, production, integration and test, and in some cases through delivery and operation.

7.2 Definitions

Manufacturing[69] is composed of all the processes used in converting raw materials into products or components. The major manufacturing functions require engagement with supplier management, operations, quality assurance, testing, and shipping/receiving. As such, manufacturing supports the generation of work instructions, tool design, scheduling, material procurement, fabrication,

[69]MIL-STD-1528A, Manufacturing Management Program, para 3.4, 09 September 1986 (canceled MIL-STD).

assembly, test, packaging, installation and checkout, product assurance, and the planning of labor and equipment resources.

Manufacturing engineering[70] is the specialty of professional engineering that requires such education and experience as is necessary to convert designs into manufactured products and to understand and apply engineering procedures in manufacturing processes and methods of production of industrial commodities and products. Manufacturing disciplines include component engineering, advance manufacturing engineering, quality assurance engineering, industry engineering, and materials and process (M&P) engineering. Manufacturing engineering requires the ability to plan the manufacturing process; to research and develop tools, processes, machines, and equipment; and to integrate the facilities and systems for producing quality products within defined cost and schedule constraints.

Producibility is a design accomplishment that enables manufacturing to fabricate hardware (HW) in a repeatable and consistent manner 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 HW designs that optimize the ease and economy of fabrication, assembly, inspection, test, and acceptance of HW without sacrificing desired function, performance, or quality. Additionally, for space and launch vehicles where emphasis is placed on low-volume production and quality workmanship, the risk to the mission dominates producibility considerations.

7.3 Objectives

The objectives of manufacturing assurance are (1) to ensure the manufacturing processes are able to produce HW that meets the design requirements and (2) to translate the design into a reliable, durable manufactured item using manufacturing processes that are highly repeatable and error free. Consistent, reliable, and repeatable manufacturing processes improve HW quality and reduce the potential for escapes, thereby improving mission success.

During conceptual design and preliminary design phases, the objective of manufacturing assurance is to influence the design process from the perspective of HW producibility. Based on an understanding of proven manufacturing processes, technologies, and practices, the objective is to design HW that satisfies the functional and design intent while optimizing ease and economy of fabrication. At the end of the preliminary design phase, manufacturing assurance further ensures that there is a qualified supply chain and further verifies that

[70] Ibid., para. 3.5.

acceptance criteria for workmanship, data collects, receiving inspection, and build acceptance are well defined.

In the critical design phase, manufacturing assurance confirms the producibility of the final design, verifies that there is adequate data collection and inspection control, and assesses the readiness of production resources, including facility, procurement, planning, tooling, personnel, training etc., to support HW production. Manufacturing assurance also assesses the validity of the contractors' production schedule and manpower loading. The program is responsible for ensuring manufacturing assurance activities are implemented at subcontractors, suppliers, and vendors.

7.4 Practices

7.4.1 Core Activities

The following are core manufacturing assurance tasks:

1. **Ensure that a manufacturing management plan (MMP)** is started early in the concept development phase of the program. The MMP can be contractually mandated as a contract deliverable for the development contractors. At a minimum, the MMP should include:

    - Manufacturing organization chart
    - Planning for make or buy decisions
    - Planning for tooling
    - Planning for special test equipment
    - Receiving inspections
    - Production yield thresholds
    - Producibility studies
    - Inspection requirements
    - Plans for data collection of process parameters and inspection results
    - Fabrication flow diagrams including inspection points
    - Fabrication plans
    - Identification and planning for long-lead items
    - Plans for mitigating material obsolescence and diminishing supplier-base issues
    - Production facility loading
    - Plans for capacity investment
    - Subcontractor or vendor delivery schedules and training
    - Early planning for 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[71]
- As part of manufacturing source selection, vendor evaluation for capabilities should be included, and alternate suppliers should be developed or identified or developed
- Process development and qualification planning
- Prohibited materials planning and management
- Traceability management to the piece part and materials

2. **Conduct producibility assessments** early in the conceptual design process. A producibility analysis compares alternative materials, processes, and manufacturing methods to determine the most cost-effective methods to achieve the design intent with selections that accommodate 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 of resources with other programs with respect to floor space, test equipment, and personnel. This process helps to identify possible risk areas by assessing whether standard manufacturing processes and materials can be employed or whether new materials and processes need to be qualified. Conventional producibility considerations focused on high-volume production are not applicable to national security space (NSS) systems that are likely to involve low-volume production and quality craftsmanship.

3. **Ensure the contractor engages the relevant disciplines (e.g., design, manufacturing, quality assurance, PMP engineering) during the early design process** so that all drawings, specifications, etc., are reviewed and coordinated. This helps prevent designers from selecting parts, materials, or designs that are difficult to manufacture and/or difficult to qualify or integrate in the next level of assembly.

4. **Ensure qualification of new materials and processes.** Evaluation of new manufacturing processes and/or facilities is particularly critical because NSS systems typically push state-of-the-art technologies that, in turn, impose changes to manufacturing processes and supporting infrastructure. New processes and facilities must be qualified prior to manufacturing production HW. Producibility and manufacturing considerations include material selection, tooling, test equipment, processes, facilities, skills, and in-process and receiving inspections, human factors, subcontractor or vendor control, standardization requirements, safety requirements, corrosion and contamination, biomedical concerns, interface units, commercially available equipment,

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

support equipment requirements, manufacturing and test software (SW), considerations of process yield, process stability, and the impact of process variability on product quality.

5. **Ensure manufacturing process mapping** is accomplished before production begins. Process mapping provides an understanding of the manufacturing work flow from basic flight component, to assembly, to subassembly, and finally, to the 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. Process mapping also provides insight into the length of time required to complete each manufacturing task and sequence of tasks, thus, providing input to program schedules.

6. **Ensure development and fabrication of engineering models** to provide confidence that new designs introduced to a contractor, subcontractor, or vendor manufacturing process(es) can be accommodated without causing adverse manufacturing impacts, including increasing defect levels and rework, which result in unpredictable schedule impacts or increased cost. 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. HW and other resources (e.g., mockups) are allocated as “proof of design” and as “proof of manufacturing” to validate production tooling, troubleshoot equipment, and verify manufacturing logistics.

7. **Ensure manufacturing process monitoring/control** is effective in validating that the resulting launch or space vehicle HW is representative of the qualified unit. The criticality of space missions requires that manufacturers impose strict controls on each item in addition to detailed traceability for each item. Process monitoring should include statistical process control and other metrics which are appropriate to the process to reduce variability and defects and ensure quality. Data collection points and accept/reject criteria should be clearly established.

   The contractor’s process for executing engineering changes should be carefully assessed so as to control the quality and pace of change and its impact on the manufacturing processes and the end products. Even insignificant items, such as a threaded fastener, must be verified to meet design requirements, including material properties, composition, dimensions, and installation requirements (e.g., lubrication, torque). This encompasses the use of incoming receiving inspection, stocking and kitting processes, in-process reviews, audits and assessments of manufacturing processes, and associated quality processes to detect and

correct defects introduced during fabrication. The goal is to prevent any defects from escaping undetected to the next process. At each inspection point, manufacturing records and in-process test data are examined and compared to well-defined acceptance criteria to ensure 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 assess design conformance. Data collection should include detailed characterization of the item performance, documentation of any discrepancies, and a failure analysis report.

8. **Ensure that tools and methods** are selected and used to monitor or control the manufacturing processes. Statistical process control of key process attributes should be used. Periodic calibration of all automated processes and measurement and sensor tools is performed to maintain the fidelity and accuracy of the inspection tools and equipment.

9. **Verify that production schedule and control system are established** for all production activities. At a minimum, the system should identify key production milestones, track production schedules of components and assemblies, track engineering changes for insertion into production, and analyze lead times required for government- and contractor-furnished properties. The control system should encompass detailed traceability and configuration management of all manufacturing documentation.

10. **Conduct periodic review of critical items, certifications, and risks** identified via the risk management process to ensure all items that require a supplemental evaluation, such as a pedigree review, are included, and to recommend changes if warranted.

11. **Ensure rigorous subcontractor and supplier management** to ensure adequate flowdown of system requirements. Technical interchange meetings and formal program reviews are used to monitor the subcontractors' development and production efforts. In addition, planned audits are conducted at the subcontractors' facilities to ensure compliance with program quality requirements. The contractor's quality organization should develop metrics and use audits to develop a list of approved suppliers for critical subcontracted items. Rigorous subcontract management is essential to ensuring that lessons learned are flowed down to suppliers and the suppliers' processes are free of risk-laden practices or prohibited materials.

12. **Verify that tolerances** are correct and verify that mockups are used to fit-check critical interfaces.

13. **Establish a system to ensure detailed traceability is captured** to track each item's pedigree. At a minimum, the system must be able to establish an as-built vs. as-designed configuration, and provide a means to find installed items in the event of a recall caused by 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 HW. Work with the contractor's quality organization to verify that a record exists of all processes performed (e.g., traveler), including tooling used, inspections and measurements, and a discrepancy reporting/closure system. The as-built documentation should also include process-unique data, such as cure times and temperatures. Verify that a record exists of all out-of-sequence operations to ensure the integrity of the product has not been compromised. Review such records to ensure processes have been performed and deviations and discrepancies have been adequately dispositioned and resolved.

14. **Provide oversight of material review board (MRB) activities** to review acceptability of all dispositions, but with an emphasis on "use as is" decisions. 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 HW.

7.5 Key Lessons Learned

7.5.1 Manufacturing is Unable to Catch Design Errors

The goal of manufacturing assurance is to produce high-quality and repeatable products that meet design requirements; however, accurate translation of the design requirements does not guarantee that the final product will meet user expectation or mission requirements. As such, the success of manufacturing assurance depends on the quality and accuracy of the design. It is imperative that maximum coordination exists between the manufacturing and design organizations early in the design process to address producibility concerns with respect to the performance and reliability requirements of the intended product.

In addition, all participants in the design process, including design engineering, quality engineering, and PMP engineering, should be engaged early in the design process. This approach minimizes potential errors in the PMP selections and helps to avoid designs that may be difficult to manufacture, qualify, or integrate into the assembly.

7.5.2 Design Maturity

Before the start of production, it is important that the design is mature and stable so that design errors, deficiencies, and modifications are not over-burdensome on manufacturing. To avoid potentially risky processes and reliability issues, it is essential to minimize fixing design problems during manufacturing. For example, in electronic HW, immature designs necessitated “fixes” to be implemented after circuit card manufacturing/assembly, resulting in excessive jumper wiring, which in turn, leads to excessive stresses on electronic components and circuit shorting failure risks that may compromise mission assurance. Furthermore, correcting design issues during the manufacturing phase may incur added cost for configuration and process requalification.

7.5.3 Focus on Mission Assurance Risk

Producibility for the space industry differs significantly from high-rate production industries, such as the automotive or aircraft industries, in that considerations for mission assurance (MA) risk play a dominant role in producibility decisions. For example, jumper wire applications in the automotive industry are cost driven; whereas in the space application, the use of jumper wires on electronic boards poses workmanship risks.

7.5.4 Apply Manufacturing Assurance Scope to all Levels

As stated earlier, rigorous subcontract management is essential to ensure lessons learned in manufacturing are flowed down to suppliers, and supplier processes are free from risk-laden practices and prohibited materials. Correction of these issues late in the program phase can be very costly and many issues can be prevented by detailed producibility and manufacturing reviews prior to the start of subcontractor production.

7.5.5 Seamlessly Integrate Manufacturing and Quality Systems

Data required for quality assurance is generated and collected during manufacturing. This data should provide a record of all processes performed, including details of the fixtures/tooling used, process control test data, inspections and measurements, and discrepancy reports. Statistical process control metrics can provide invaluable insight into improving quality by reducing process variability and defects.

7.5.6 Specifically Address Challenging Processes That May Require Exceptional Skills or Experience

Sufficient time must be planned in the schedule for operator training and certification. The detailed procedures should be carefully documented with the

aid of photographs or videos, where applicable, and made easily accessible to operators on the factory floor. Special attention should also be given to the training of alternate and backup operators to avoid single-point failure scenarios that could potentially compromise product quality and cause schedule delays.

7.6 Task Execution by Phase

Within the Mission Assurance Baseline (MAB), manufacturing assurance tasks are defined for each of the following seven Mission Assurance Guide (MAG) phases.

1. Phase 0: Pre-Phase 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 for manufacturing is primarily related to the destruction of manufacturing capability, e.g., disposal of custom tooling and equipment)

Table 7-1 summarizes the key manufacturing engineering tasks to ensure HW quality meets the design documentation, program schedule, and cost. Manufacturing assurance task products are emails, briefings, and reports documenting the results of both manufacturing and quality control-derived plans, reviews, analyses, audits, formal review boards (e.g., MRB), process development and qualification data, and other data or information that provides insight into the robustness of the manufacturing phase of the program.

Table 7-1. Key Tasks by Phase

	Phase					
Task	**0**	**A**	**B**	**C**	**D1**	**D2**
Provide content for acquisition documents as needed.	X					
Assess contract items, including statement of work (SOW), contract deliverable requirements list (CDRL)/data item descriptions (DIDs), request for proposal (RFP), and work breakdown structure (WBS) to ensure all	X					

	Phase					
Task	**0**	**A**	**B**	**C**	**D1**	**D2**
contractor tasks and deliverables are included.						
Assess contractual implementation of manufacturing in the contract to ensure all contractor tasks and deliverables are included.		X				
Review manufacturing plan and contractor's manufacturing infrastructure.		X				
As appropriate, review systems requirements review (SRR) and system design review (SDR) topics to ensure manufacturing-related, risk-reduction efforts are planned and implementable.		X				
Assess the content and accuracy during the preliminary design audits (PDA).			X			
Develop customized preliminary design review (PDR) criteria, if warranted.			X			
Assess all PDR criteria for manufacturing.			X			
Assess production readiness and test readiness documentation and ensure all criteria are satisfied during critical design audits (CDAs).				X		
Ensure material and process qualifications are complete and accurate.				X		
Develop customized critical design review (CDR) criteria.				X		
Assess CDR content.				X		
Assess manufacturing readiness review (MRR) entrance/exit criteria and whether the criteria have been fulfilled.				X		

	Phase					
Task	**0**	**A**	**B**	**C**	**D1**	**D2**
Assess completeness and accuracy in technical reviews, including test readiness review (TRR), formal qualification reviews (FQRs), production readiness review (PRR), etc.					X	
Review end item data packages (EIDPs): Completion of Phase D1 technical audits (e.g., physical configuration audit [PCA], functional configuration audit [FCA]).					X	
Conduct independent readiness review team (IRRT) assessments, pre-ship reviews (PSR), hardware acceptance review (HAR), pedigree reviews, etc.					X	
Provide oversight and technical content on manufacturing-derived or impacted review boards, e.g. MRB.					X	
Assess content and accuracy in technical reviews, including system verification review (SVR), mission readiness review (MRR), launch readiness review (LRR), flight readiness review (FRR).						X
Conduct IRRT assessments.						X
Provide oversight and technical content on manufacturing derived or impacted review boards, e.g., MRB.						X

7.6.1 Phase 0 – Concept Design

In Phase 0, manufacturing assurance performed at the pre-systems acquisition phase ensures that the RFP adequately accounts for the industry's capabilities for manufacturing processes via the SOW; CDRL; DIDs; and manufacturing specifications and standards. A technology readiness assessment (TRA) should be conducted to assess the maturity of product designs. A manufacturing control plan may be tailored to meet specific program requirements.

Subject matter experts (SMEs) with manufacturing domain knowledge should be engaged with designers to develop alternate system designs, conduct trade studies, and provide detailed "sizing" of selected concept designs.

7.6.2 Phase A – Concept Development

Manufacturing assurance activities during concept development are aimed at gaining insight into the prime's or major subcontractors' allocated resources for the purpose of identifying potential risks during subsequent production. A manufacturing assessment is made based on the contractor's integrated management plan (IMP), CDRLs, make or buy process, adequacy of resources, feasibility studies, process development plans, qualification test plan for manufacturing processes, test criteria, and cost and schedule impacts. Manufacturing assurance should also confirm that initial baseline plans include adequate schedule and funding to develop new manufacturing technologies.

7.6.3 Phase B – Preliminary Design

Phase B, the beginning of a more detailed design phase, culminates with a PDR. As the design becomes more mature, manufacturing assurance ensures design for manufacturing and assembly (DFMA) and completeness of producibility analyses. Manufacturing tasks will also include an assessment of the strategies for technology obsolescence and diminishing manufacturing resources, make or buy decisions, and the use of special test equipment, tooling, and support equipment. Manufacturing assurance may also review and assess the design and fabrication of breadboards, brassboards, and flight-like prototypes.

7.6.4 Phase C – Complete Design

Phase C shares the same objectives as in Phase B, but at a more detailed level to 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 completeness of the processes for packaging, handling, storage, and transportation (PHS&T) of parts, units, and the final product. Phase C concludes with a formal, multidisciplinary CDR, followed by a CDR at the system level, and finally, an MRR.

At the conclusion of Phase C, the design is stable, with all changes captured and implemented, and producibility analysis completed. The quality of the engineering drawings should be such that clear manufacturing/production work instructions can be generated.

At MRR, manufacturing assurance ensures systems have been put in place to collect in-process quality control data, address scrap minimization, implement

lessons learned, and reduce rework and repair. Manufacturing assurance also ensures that requirements for facilities, materials, tooling and fixtures, test equipment, processing equipment, personnel, operator training, government-furnished property, and SW (required to support the manufacturing process) are defined, and all appropriate resources are ready and available to commence production.

7.6.5 Phase D – Build and Operations

7.6.5.1 Phase D1 – Fabrication and Integration

In Phase D1, manufacturing assurance ensures that the contractor has an effective data retrieval system for determining the as-built configuration, a variability reduction program, manufacturing process flow charts, manufacturing process qualification approaches, and inspection/process control methods.

During the production phase, manufacturing assurance provides oversight to manufacturing-derived or impacted review boards, e.g., MRBs, failure review boards (FRBs), and corrective action boards (CABs). Manufacturing assurance tasks include participation in technical reviews, such as TRRs and FQRs.

At the end of Phase D1, manufacturing also supports technical audits, including PCA, FCA, PSRs, HARs, and pedigree reviews.

7.6.5.2 Phase D2 – System Fielding, Test, and Check-out

Manufacturing assurance ensures all open manufacturing-related technical and anomalous issues are closed and the space vehicle is ready for launch. Manufacturing tasks may include providing support to SVRs, MRRs, LRRs, and FRRs.

7.6.6 Core Mission Assurance Processes Supported by Manufacturing Assurance

During requirement analysis and validation, manufacturing assurance assists in developing manufacturing requirements for inclusion in the RFP, including assessment of the IMP, CDRLs, make or buy decisions, adequacy of resources, qualification plans, and plans for certification of critical processes. Manufacturing assurance also evaluates the baseline design requirements presented by the prime contractor and assesses the flowdown of manufacturing requirements to the subcontracts.

In design assurance, manufacturing provides oversight to the HW design process, ensures completeness of producibility studies, and assesses the make or buy decisions, DFMA, manufacturing methods, and strategies for mitigating technology obsolescence and diminishing supply base. Manufacturing also assesses the planning for other resources, including special test equipment, tooling, and support equipment.

In manufacturing assurance, manufacturing tasks ensure completeness of the entrance/exit criteria and MRRs; ensure the accuracy and completeness of configuration control of manufacturing process documentation; ensure the stability of the production process and completeness of inspection/process control methods; ensure the accuracy and validity of the manufacturing schedule; and evaluate the adequacy for PHS&T of parts, units, and the final product.

During integration and test evaluation, manufacturing tasks ensure the completeness of the TRRs and provide oversight in integration and test (I&T) processes and procedures. Manufacturing also participates in the review of test anomalies and supports FRB meetings.

7.7 Government and Contractor Enabling Processes and Products

The manufacturing assurance team requires access to the government's draft and final RFP, the negotiated contract, and the contractor's engineering team at all levels of the program from the design period to the testing phase. Contractor CDRLs for SDR, PDR, CDR, MRR, and EIDP are also needed. A list of key government and contractor enabling manufacturing products is given in Table 7-2.

Table 7-2. Enabling Products

Phase	Government Enabling Products	Contractor Enabling Products
Phase 0	• RFP, SOW, CDRL, DIDs, WBS	
Phase A	• Final contract • Criteria for system requirements • SRR • SDR	• Completion of integrated baseline review (IBR) • SRR • SDR • Risk reduction plans

Phase	Government Enabling Products	Contractor Enabling Products
Phase B	• Entrance/exit criteria for PDR • PDAs • TRA	• Completion of CDRLs for PDR • Completion of CDAs • Completion of internal TRA • Risk assessment
Phase C	• Entrance/exit criteria for CDR and MRR • CDAs • TRA	• Completion of CDRLs for CDR and MRR • Completion of CDAs
Phase D1	• Phase D1 technical reviews, including TRR, FQR, PRR • Phase D1 technical audits, including PCA, FCA • IRRT assessments	• Completion of CDRLs for Phase D1 technical reviews • EIDPs • Completion of HAR
Phase D2	• Phase D2 technical reviews, including SVR, MRR, LRR, FRR • IRRT assessments	• Completion of CDRLs for technical reviews

7.8 Practice Manufacturing Task Application Example

The following is an example of how manufacturing assurance might be implemented during the program life cycle. This example illustrates the high-level manufacturing assurance activities associated with various phases. Using this guide as a roadmap, the appropriate manufacturing SME assists the program office in determining the manufacturing and producibility tasks.

Table 7-3. Practice Task Application

	Phase					
Task	**0**	**A**	**B**	**C**	**D1**	**D2**
Review Contractual Implementation of the MMP						
Assess management section for completeness in the RFP, SOW, CDRLs,	X	X				

	Phase					
Task	**0**	**A**	**B**	**C**	**D1**	**D2**
DID, WBS, etc.						
Assess PDR Criteria for Manufacturing						
Assess manufacturing infrastructure	X	X	X			
Assess any manufacturing related risk reduction efforts	X	X	X			
Assess early manufacturing development		X	X			
Conduct Independent Assessment of Pre-Phase B TRA			X	X		
Assess Manufacturing Plan and Production Readiness						
Assess quality and completeness of engineering drawings			X	X		
Assess quality and accuracy of manufacturing processes and assembly work instructions			X	X		
Assess Accuracy and Completeness of Material and Process Qualifications			X	X		
Review and Approve Program-Specific PMP			X	X		
Conduct Independent Assessment of Pre-Phase C TRA			X	X		
Assess Production Readiness at MRR						
Verify availability of materials			X	X	X	

	Phase					
Task	**0**	**A**	**B**	**C**	**D1**	**D2**
Verify personnel readiness (training/certification)			X	X	X	
Verify availability of equipment, fixtures, and tooling			X	X	X	
Verify facility readiness			X	X	X	
Assess credibility of production schedule				X	X	
Provide Oversight to Manufacturing-Derived Review Boards, Including MRB, FRB, and CAB				X	X	
Review TRRs and FQRs				X	X	
Assess Content and Accuracy of Test Procedures and Exit Criteria						
Assess Quality and Acceptability of HW				X	X	X
Conduct PSR, HAR, and pedigree review				X	X	
Review EIDPs, including PCA and FCA				X	X	X

7.9 References

Policy-Related

AFI 99-1	Test and Evaluation Process, 1 August 2000
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

Specification and Standards

MIL-STD-1528A	Manufacturing Management Program, 9 September 1986

Handbooks

MIL-HDBK-727	Design Guidance for Producibility Provides Guidance for Producibility Assessments, 5 April 1984
TOR-(8583)-5235	Parts, Materials, and Processes Control Program for Space and Launch Vehicles, 8 November 2006
TOR-(8583)-5236	Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles, 13 November 2006
TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, 30 November 2005
TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, (Chapter 20), 30 November 2005

Best Practices

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

Other

Critical Process Assessment Tool (CPAT), Manufacturing

Chapter 8
Integration, Test, and Evaluation

Dan W. Hanifen
GEOINT Development Office/Payload
William F. Tosney
Julia D. White
Corporate Chief Engineering Office
Thomas C. Hecht
System Integration and Test Office

8.1 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 discernible evidence of compliance. The final step for a national security space (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. This chapter will focus on test. Analysis also plays a key role in mission success (MS). The various analyses that contribute to space system development are listed in Appendix A3.

8.2 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 (SV) hardware (HW) testing uses rigorous test planning and flight-like test articles to contractually verify requirements and validate unit,

subsystem, and system performance. Informal SV HW 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.

Tests can also be parsed into acceptance tests, qualification tests, and protoqualification tests. Acceptance tests are used to show workmanship is adequate. Acceptance tests assume a proven design and include functional and environmental tests. The stress level of acceptance tests slightly exceeds that of the flight environment. Qualification tests are intended to prove design. Qualification tests also include functional and environmental tests but the stress levels are far in excess of the flight environment. Qualification testing may include tests that are not deemed necessary for acceptance testing, such as survivability tests. The stress levels of qualification tests are so high that the test is deemed destructive. Because of the high cost of flight HW there is a hybrid of qualification and acceptance testing, called protoqualification. Protoqualification testing deemed to be destructive protoqualification is a hybrid of qualification and acceptance testing. The stress levels of protoqualification testing exceed those of acceptance testing, but are not so high as to be destructive. Protoqualification testing may also include extra tests that are not needed for acceptance testing. The advantage of protoqualification testing is that HW tested can be flown.

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.

8.3 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.

- Contribute to an effective and efficient test.

- Ensure that test anomalies are resolved satisfactorily.

- Ensure that requirements are indeed met. Ideally this is accomplished by close cooperation between the customer and the contractor when the plans for meeting requirements are devised and when the final report describing how the requirement has been met is reviewed. See Chapter 5 for an in-depth discussion of the role of MA in requirements verification.

8.4 Practices and Tasks

Most activities associated with the development, integration, validation, and verification of a space system composed of components, units, subsystems, and systems[72], are formally planned and performed by contractor personnel. Typical program office (PO) MA activities include ensuring the appropriate testing, especially development, qualification, and acceptance testing, is appropriately planned, performed, witnessed, and documented. Test results are independently evaluated to establish development, qualification, and acceptance status. Government PO 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 (IRTs), which can include personnel from The Aerospace Corporation (Aerospace), 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 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 tests are usually done to demonstrate proof of concept, answer specific questions about certain technologies, or assist with failure analysis.

“Test as you fly/fly as you test” is a key test philosophy for any NSS SV or launch vehicle (LV) test program. LVs or SVs are exercised as they would be during flight or on-orbit mission, controlling the flight equipment and SW (test what you fly) by ground equipment and SW 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., LVs or SVs controlled by test equipment, subsystems

[72]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 (SW), services, and personnel required for its operation. A government PO 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 (LV) 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.

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.

A lesson learned from many mission-ending in-flight failures is that it is necessary both to attempt to TLYF and to acknowledge the inability to completely do so. TLYF may not be accomplished because of 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.

8.4.1 Integration

Successful SV or LV HW 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 SW 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 MS. LV 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 to validate that design concepts, processes, or techniques will achieve the desired results; reduce risk prior to the fabrication of qualification and flight HW; validate test support equipment and that test procedures are correct; acquire data to verify system models and simulations (M&S); and investigate problems found during testing in later stages of qualification and acceptance. SW test is addressed in Chapter 18.

- **Life testing** is a ground test program for satellites and LVs 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 HW units with insufficient history relative to the flight units, system application, or environment being addressed to demonstrate that the contractor's design, manufacturing process, and acceptance program produce HW that meets the expected environmental requirements (transportation, launch, on-orbit operations, and repeated acceptance testing) as well as mission life requirements with margin. Be aware that a significant number of flight failures are caused by false assumption of heritage. Review claims of flight heritage with suspicion.

- **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 HW, SW, 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 LV and the SV after arrival from their respective factories, and then conducted again after the spacecraft is integrated to the LV. These tests not only demonstrate system interface compatibility between the space and LVs, 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, SW, 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, and 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 (CAs)/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 SV subsystem performance, to verify requirements (if required), to characterize operating limits, and to discover any problems affecting MS 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 SV's performance according to specification (e.g., precision, accuracy, throughput, and timeliness). The frequency and extent of calibration testing is dependent on SV 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 an SOS-level test using operational SVs, 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 SV, 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 HW 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 ensures 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 (MIL-SPECs) 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 ensure 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.

8.4.2 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 decisionmaking
- 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 to allow a judgment of requirements satisfaction. Typical activities include:

- **Pre-test reviews** are conducted to ensure the test article, test equipment, facilities, procedures, HW, and SW 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 MS 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 of 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 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 MS 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 because of program constraints. Second, test risk assessment examines the risk to the flight HW 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 SW/HW for nominal and off-nominal operating states, modes, potential redundancies, and failures in both nominal and off-nominal (worst-case) operational environments.[73]

- **Failure Reporting and Corrective Action System (FRACAS)** is an orderly method to capture and report test failures, associate failures with root cause(s), track the implementation of corrective actions (CAs) to remediate failures, and track required retests to verify that the causes of the failures are corrected. A failure review board (FRB) is an established forum composed of contractors, subcontractors or suppliers, the government PO, and consultants to coordinate the review of all significant failure reports, review failure trends, track and review the timely implementation of CAs, to provide closeout approval for reported failures (see also Chapter 11).

8.5 Lessons Learned

8.5.1 Consider Test Like You Fly Early in Development

TLYF is a philosophy that should be considered early in development. The point of it in this section is that in many cases, if you think about TLYF when you get to test—it's too late. One can't fire thrusters in a high bay. You can't fire your flight pyros to see if they work. The 1-g environment may preclude moving antennas, solar arrays, and deployable devices. To improve the flight-like characteristics of testing, limitations like these have to be considered early. Then one can add test points to verify pyro circuit continuity or to show when thrusters are receiving drive signals. One may be able to add other test points to moving equipment or build off-loaders so it can actually be controlled. By thinking about this early, one can improve the quality of testing rather than being boxed into accepting TLYF exceptions later in the program.

8.5.2 Take Precautions so Test Doesn't Damage Flight Equipment

Section 8.5.1 advises the use of test points. Test points in general are a good thing, but an unprotected test point may allow flight HW to be damaged. Test points should be buffered. That way if an unintended voltage or short is applied to the test point, the HW isn't damaged or the pyro doesn't fire.

[73] 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 TR-2004(8583)-1 (a.k.a. SMC TR-06-11) (replaces MIL-STD 1540D), "Test Requirements for Launch, Upper Stage, and Space Vehicles."

Be aware that environmental stresses on HW accumulate. As anomalies are investigated a piece of equipment may be vibrated or thermal cycled many times more than planned in a perfectly successful test flow. In one example, a unit had relays that unexpectedly and temporarily transferred during vibration. Diagnosing the associated symptoms required the unit be vibrated and then functionally tested many times. The multiple vibrations, even at acceptance levels, were causing the unit to reach its allowable quota for vibration exposure. Fortunately it was found that failure symptoms would appear at vibration levels lower than acceptance levels. The vibration levels were reduced and troubleshooting continued until the root cause was found. By reducing the vibration levels, the total exposure of the unit was kept within specification. Another example of accumulated environmental exposure occurred during an acoustic vibration shaping run for an entire satellite. During the shaping run, the payload fairing tip dislodged and fell through the volume that would normally contain the satellite. This occurred after the fairing had been used to test multiple satellites. The payload fairing had been worn out by exposure to environments in excess of design limits.

A high bay can be a perilous place in a satellite; nonstandard work is particularly a hazard at that location. An example is a case where an identified satellite anomaly was being assessed with the use of a written test aid. The test aid was a generic break-out box connected to the satellite via a custom cable. A plastic overlay was placed on top of the breakout box to indicate what pin on the box corresponded to the appropriate cable pin. The wrong voltage was inadvertently connected to the wrong pin and destroyed $35,000 worth of flight HW. The labeling on the test aid was ambiguous, which contributed to the mistake. Test aids should be clear and as a best practice dry runs should be conducted on critical activities with appropriate supervisor oversight prior to committing the flight hardware to the same test.

Some additional anecdotes from incidents in the high bay are offered as lessons learned. The first involves contractor technicians damaging connector pins every two to three weeks. Eventually the contractor created a short class to educate the technicians how to properly mate the connectors. After the technicians completed the class, the connector damage immediately stopped. The lesson learned is that technicians should be properly trained on procedures. The second story involves satellite heaters that were inadvertently turned off during the cold cycle of the thermal vacuum test. The only person authorized to send commands to turn the heaters back on was the test director, who was not available, and the equipment was overstressed. The lesson here is that key personnel must be available during critical testing. A final anecdote is a satellite that experienced battery shorts to ground. Technicians shorted cable pins that connected the solar array to the satellite and significant current traveled from the battery to ground, causing damage to the array. The potential for damage was not recognized or flagged by the procedure. Power sources are typically issued with female

connectors and power users are issued with male connectors. The solar array designed as a power source was built with female connectors. The connector that mated to the solar array was connected to the battery, through the field effect transistor. The connector on the battery side had male pins to mate with the solar array pins and the battery-side connector, with a vast potential for damage, had male pins. The two shorting incidents could have been prevented if the battery-side connectors had been designed with female pins.

One additional lesson for avoiding test damage comes from a discovery at a vendor. The vendor manufactured a product that operated at 28 volts and a product that operated at 60 volts. The vendor used a single test console to test both products. A toggle switch on the test console selected whether 28 volts or 60 volts would be applied to the unit under test. Fortunately, no damage occurred, but a slight lapse in configuration control would apply 60 volts to a unit designed to operate at 28 volts—with resulting damage. Test equipment should not have potential to damage flight hardware.

8.5.3 Activate Flight Batteries Conservatively

Flight batteries have a limited ground life. Activated too soon in the integration and technology (I&T) program, the battery will exceed its ground life and become unsuitable for flight. Programs tend to be optimistic regarding the time remaining to get through the test regimen. In most cases, this optimism does not impact the chances for MS. However, when a program is certain they are going to launch in a year, they may activate their flight batteries. A major HW anomaly or a need to rewrite the flight SW delays launch for another year, and with this delay, the ground life of the batteries expires. As flight batteries are very expensive, this is wasteful. On the bright side, TLYF fidelity is improved, as flight batteries are relegated to being test batteries.

8.5.4 Testing Should Not Mask Faults

Special test equipment and test instruments are typically grounded. In one instance a satellite was assembled without a ground connection between two major subassemblies. During the satellite testing, the test equipment provided the needed ground connection. With this connection the satellite successfully passed the test and launched, and failure ensued as the satellite was not tested in flight, ungrounded, configuration. The best way to detect the presence of needed ground connections is to perform a special “plugs-out test.” The plugs-out test involves physically disconnecting the satellite from its special test equipment (STE). Communication with the satellite is achieved via radio frequency (RF) couplers. The only hard-wired connection is a kill switch for use in an emergency. In this flight-like configuration the satellite is given enough commands to demonstrate satisfactory operation.

Another instance of test equipment being the problem rather than part of the solution occurred when the same equipment was used to produce and then test the flight product. As it turned out, the equipment used to produce and test the flight product was flawed; thus, the flight product was flawed, and, thus, the test equipment did not detect the flaw. The flaw was detected only after launch. The lesson learned is to maintain more independence between the production and the testing.

8.5.5 Lessons to Improve Efficiency of Integration and Test

Identification of assemblies with specific required orientation can prevent deployment the wrong way or solar arrays turned the wrong direction.

Design for anomalies in test is an important lesson learned. If a power box has fuses, expect them to blow during I&T. Place them where they can be replaced by removing a side panel. Do not bury the fuses deep in the box where you need an entire acceptance test if you replace a fuse. Put hinged panels on your satellite, with the cables going across the hinge line. If a box fails in test, the panel can be opened for access without disconnecting vast numbers of cables. Do not use an adhesive thermal bonding compound underneath boxes as it is virtually impossible to remove a failed unit for rework and penalty test.

Balance the time on the A and B sides of a satellite during vehicle test. There is a tendency for programs to spend almost all their vehicle test time on the A-side. Brief forays are made to the B-side or combinations of A- and B-side, primarily to show that such things are possible. The problem arises if a program wants to make an argument of flightworthiness based on hours of trouble-free operation. One program encountered a minor anomaly late in its test flow. At the time the satellite had experienced thousands of hours of A-side test time, but only hundreds of hours of operation on the B-side. Based on the trouble-free operation on the A-side, a valid argument for use-as-is of the A-side HW was constructed. No such argument for the B-side HW was possible. The program spent extra, originally unscheduled time on the B-side HW just to accumulate test hours. Had the program anticipated the situation, more time could have been spent on the B-side HW throughout the vehicle test, with no impact. Had this been done, both A- and B-sides would have had a few thousand hours of trouble-free operation by the time of the anomaly. No test extension would have been needed to just accumulate B-side hours.

Beware of multiple intelligences executing the same tasks. Multiple intelligences can be on the satellite or split between satellite and test equipment. As an example, a satellite did battery charge control by a computer, backed up by an analog circuit. Most of the power anomalies through vehicle test occurred when both the computer and analog circuit tried to control charging or

alternately when both the computer and analog circuit assumed the other was executing.

Flight-like (engineering) units are highly advised to prove unit design. The test impact comes after the design is proven. Then the engineering units should be assembled into a semblance of the complete satellite. The resulting test bed, called herein an engineering unit test assembly (EUTA), has multiple important uses. First as a SW test bed; with new satellites using more and more SW, SW testing has become a huge program challenge. SW will typically be initially tested by a SW tool. Then the SW should graduate to being tested on the EUTA. The alternative is to test somewhat immature SW on the actual satellite, which may create a situation that damages the flight hardware and ties up a scarce resource. In addition to testing SW, the EUTA aids in design integration and anomaly investigation. Another use of the EUTA is to support launch rehearsals. SW simulations of the satellite lack fidelity (rehearse like you fly) and the satellite itself is too valuable to tie up for a week-long rehearsal. The EUTA is the optimum compromise. One program is currently using three EUTAs for the above purposes. The three EUTAs are 100 percent subscribed and the program longs for more.

Early mention was made of a vehicle troubleshooting test aid and how its misuse led to the damage of flight HW. Despite that unfortunate example, test aids are necessary to allow troubleshooting. Each program must decide for itself if it wants to build test aids prior to specific anomalies. Building test aids early can lead to wasting money on test aids that are never used. Waiting for the anomaly risks sitting dormant while test aids are constructed to allow troubleshooting to proceed.

Unverified failures (UVFs) can be minimized by taking two independent measurements of commands leaving and responses entering test equipment. If this approach is used, some UVF anomalies would be isolated to the test equipment. Another hint for minimizing UVFs is, when practical, to stop automatic tests when a failure occurs. The idea is to conduct a careful anomaly investigation rather than having the automatic test continue and erase intermittent symptoms.

Tests should be pyramided so that the most demanding tests are conducted at the lowest possible assembly. The idea is to have anomalies appear when the equipment is most accessible. This allows more perceptive troubleshooting. Also, it is cheaper to tie up a box during troubleshooting instead of an entire vehicle.

Finally, test results should be archived and accessible. During I&T, past test data should be available to aid in troubleshooting test problems. After launch, the test results should be available for on-orbit anomaly investigation.

8.5.6 Mission Assurance Role in Integration, Test, and Evaluation

Attend Test Readiness Reviews (TRRs) and Test Exit Reviews (TERs). To pursue MA from a stronger bargaining position, it is helpful if the customer has contractual approval/disapproval authority at TRRs and TERs. At TRRs, in addition to the obvious task of ensuring the upcoming test will accomplish its objectives, ensure that test equipment will not go out of calibration midway through. At TERs the obvious task is to ensure that the test accomplished the intended objectives. The pitfall is that configuration is often changed on completion of a test. One must ensure that any anomaly investigation that is in progress has reached a point where configuration can be changed without affecting the troubleshooting. If an anomaly only occurs at cold temperature, sufficient data is critical before allowing the satellite to leave the thermal vacuum chamber.

Test anomalies will often result in FRBs. Attend and take an active role in FRBs. In addition, review the closure of lower-level anomaly reports. One may discover a significant anomaly that should have been elevated to FRB. One may discover that uncontrolled configuration changes are occurring. As an example of the latter, consider a connector pin that is bent during assembly. Low-level anomaly paper may relocate the signal to unused pins. That might be the only record that a signal goes through Pin 38, when all the other formal documentation shows it going through Pin 36.

Review the closure of all satellite anomalies. To enforce best MA practices, it is ideal to have contractual approval/disapproval rights.

Similarly, review the reports describing how requirements are satisfied. Again, to enforce best MA practices, it is ideal to have contractual approval/disapproval rights.

8.6 Integration, Test, and Evaluation Strategies and Execution

The majority of IT&E effort occurs during Phases B, C, D1, and D2. As HW and SW mature through the design and development process, incremental testing at varying levels of assembly occurs. During Phases B and C, the emphasis is on design validation. During Phase D1, the emphasis is on validating test support equipment, establishing system performance baselines, and conducting unit/system qualification or acceptance. During Phase D2, the emphasis is SOS functional testing in the operational environment, resulting in operational turnover of the new space system into mission operations.

Those involved in test should work closely with those in other disciplines throughout the program life cycle. Test points to allow testing of pyro signal paths and deployables should be incorporated during the design phase. It will be

too late to add this capability after a satellite has been assembled. Further, a great many apparent failures are actually caused by test equipment. Test engineers should proactively work to prevent such false alarms. When anomalies do occur, test engineers should work closely with the anomaly investigators. Also, test equipment often can be improved based on the test experience, with long-term program benefit.

8.6.1 Integration, Test, and Evaluation Activities by Phase

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

Phase 0: Consideration for perceptive and sufficient IT&E begins during 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 STE for high-fidelity calibration and evaluation.

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 I&T strategies and philosophy become clearer, and the needed ground test infrastructure, GSE, and STE 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 brassboard/breadboard/prototype units. Brassboard/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 Phases B and C.

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 completed 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 CAs. 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 Phase B, IT&E begins to also focus on test risks to the flight HW over the course of the entire test sequence to avoid overstressing flight HW. 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.

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 ongoing developmental testing. 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 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 Phase D1 (fabrication and integration). During 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 HW over the course of the entire planned test sequence to avoid overstressing flight HW. 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 D1: During 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 SV, 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 SV to the launch site.

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.

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 SW, HW, and data configuration changes, and all spacecraft and ground system anomaly recovery activities, including diagnosis of root cause and the validation of CAs (including SW/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.

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 ensures 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 SW, data, and HW configuration management process that will support test configuration definitions throughout the system life cycle.

8.6.2 Integration, Test, and Evaluation Activities by Discipline

The Mission Assurance Baseline (MAB) for the IT&E process is organized in a hierarchy by life cycle phase, as discussed in Section 8.6.1. For each life cycle phase, the process is further organized into the following categories:

- **Program planning** includes an evaluation of the contract mechanisms defining the scope and tasks for the work performed by the contractor to ensure 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 (SE)** includes a series of tasks to ensure that the requirements allocation process traces to the test process both ways and that adequate schedule and resources exist for both system integration activities and a system test program. Assessment of testing schedules, test risks, and verification process, and allocation of test as a method are addressed in SE.

- **Space systems** integration tasks are required to evaluate whether the contractor's process, sequencing, and schedules successfully build up the SV 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 SE functions.

8.6.3 Key Integration, Test, and Evaluation Tasks and Objectives

Sufficient testing is a key to increased MS. This section is intended to highlight those key tasks that are deemed more important to the goal of achieving MS.

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 startup, 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 with historical test programs, costs, and MS trends will provide valuable insight 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.). The integration and test environment (e.g., humidity, contamination, debris, temperature, etc.) can also impact the T&E MA activities. Additionally, IT&E evaluates existing technology or delivered flight HW 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 prior test history to optimize the test program and avoid over-testing potential flight HW, thereby decreasing predicted mission life and reducing MS.

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 contractor processes are in place to rationally approach test milestones with key pretest reviews, clear entrance criteria and procedures, and also ensure all test failures are documented and chased to root cause, and 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 M&S that will be used during system-level verification to provide the basis of predicted performance for on-orbit testing from beginning-of-life (BOL) initialization to end-of-life (EOL) disposal. Where needed, MA can also provide capabilities for independent testing to assess test failure root causes and recommend mitigation steps prior to retesting.

IT&E MA must also evaluate the test program to ensure that test risks are considered. These risks fall into five 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 caused by 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 HW 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 HW with limited mission life once on orbit. Fourth, precautions must be taken to ensure I&T does not damage flight HW. Fifth, care must be taken to ensure test does not mask faults.

Throughout all the phases, IT&E MA also provides an independent assessment of the concept of operations (CONOPS), the integration and test program, test plans, test procedures (TPs), 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 SW logic paths, all HW states (e.g., on, standby, off), HW modes (e.g., 100 percent, 50 percent, 25 percent capacity/capability), all HW redundant capabilities, all HW and SW fault detection and housekeeping functions, and all external interfaces.

Finally, while this chapter promotes testing as the preferred verification method, test does have limitations. A test regimen will usually reveal anomalies. In the course of correcting those anomalies, both the flight product and the test equipment are strengthened. However, test is not a cure for a product that is developed to less than rigorous standards. Many anomalies will occur in test, only if you are lucky. If you are unlucky, the anomaly will appear after launch. Hence, test must be supplemented by perceptive analysis to maximize the chances of discovering and mitigating mission-ending faults. Also, as discussed here and elsewhere in this chapter, extra effort must be directed toward MS throughout the entire enterprise.

8.7 Government and Contractor Processes and Products

8.7.1 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 SE reviews, telecommunications, development, and test-related milestones (e.g., System Requirement Review [SRR], Preliminary Design Review [PDR], Critical Design Review [CDR], TRR) and integrated product teams (IPTs) or working groups (WGs). To facilitate IT&E, the government PO 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.

8.7.2 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, SE, and test engineering processes; I&T planning and execution processes; verification planning and execution processes; CONOPS WGs; and configuration management (CM), risk management (RM), and test failure review/CA 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 STE. This includes preliminary and final unit, subsystem, and system design presentations and data, I&T requirements, plans and procedures; detailed integrated master schedules (IMPs) (prime and subcontractor); verification plans; verification ledgers (map requirements to verification methods to verification evidence); test reports; and test/engineering memos documenting verification evidence.

8.8 Integration, Test, and Evaluation Checklist Discussion

Two useful checklists of activities contributing to space system development are Aerospace's Integrated Mission Assurance Tool (iMAT) and TOR-2010(3900)-2, Aerospace Mission Assurance Technical Baseline Draft—National Systems Group Input. These documents include extensive checklists of activities necessary for product development. Searching for the words "test" or "evaluation" within these documents reveals dozens of referenced tasks. Some of these tasks refer to the assembly and test of the satellite. There are also some tasks listed that deal with ground segment and system tests. However, if one returns to the theme of this chapter, the intent is to apply MA best practices at all levels of IT&E. That means going beyond the satellite-centric space I&T tasks. I&T activities are conducted at the subsystem level, which is usually covered by high-level checklists. Integration and test activities are also conducted at the unit level and lower.

There is also the evaluation part of IT&E to consider. Requirements verification is spread among the subsystem activities. If one extends evaluation to include consideration of anomalies, the reliability tasks are fodder for examination.

Finally, proactive efforts are advised herein to get maximum benefit from IT&E. To get contractual authority over IT&E activity one needs involvement in defining the contract, the statement of work, the CDRLs, and compliance documents. Incorporating test points into flight products is often a way of improving the perceptiveness of IT&E. Getting test points implies involvement with unit, subsystem, and vehicle design.

Table 8-1 includes a partial listing of T&E tasks contributing to a satellite program. Listed tasks go from the unit level, through subsystem, payload and bus, to the SV. Tasks also include some ground segment and system level testing tasks to the all up system level. Note that HW and SW testing is included. Tasks include both electrical and mechanical effort. Functional and environmental testing must be considered. The checklist in Table 8-1 omits the tasks related to contract definition. However, as mentioned above, thought needs to be given to T&E, even at that program phase, to ensure contractual tools are in place to accomplish effective T&E at later phases. The message is, IT&E pervades a program. Hence it pervades checklists describing space system development tasks.

Table 8-1. Representative Test and Evaluation Tasks

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Program Roles and Responsibilities							
Ensure appropriate expertise in program office exists to perform evaluation of test and integration planning.		X	X	X	X		
Assess the effectiveness of test and evaluation integrated product team.		X	X	X	X		
Ensure systems engineering has responsibility for implementation of system-to-unit-level requirement verification.		X	X	X	X		
Assess contractor test capability.		X	X	X			
Assess Concept Testability							
Assess testability of candidate system concepts and technologies, space vehicle system, ground support, and special test equipment strategy.	X	X	X				
Assess needed test infrastructure and the testability and test requirements of technology demonstrations.	X	X	X				
Assess Test Risks							
Ensure test risk assessment examines the potential risks to the flight hardware from the proposed test program.		X	X	X	X	X	
Ensure evaluation of space vehicle and subsystem test risks.		X	X	X	X		

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure risks associated with deviations from environmental testing standards are evaluated.		X	X	X			
Ensure evaluation of the impacts of repetitive testing on flight hardware at each level of assembly to include retesting.		X	X	X	X	X	
Assess Verification Management Process							
Ensure the contractor's proposed method of verification is sufficient and perceptive for each contractor-proposed verification method at each level of assembly.		X	X	X	X	X	
Ensure issues with the proposed test, integration, and verification plans and procedures are identified.		X	X	X			
Ensure TLYF principles are identified in the contractor's test program.		X	X	X	X	X	
Assess Verification Requirements and Planning							
Evaluate TEMP and system verification test plan and ensure proper measures of effectiveness are identified and element interfaces are tested.		X	X	X	X		
Ensure appropriateness and risk of verification by any method other than testing is evaluated.		X	X	X			
Ensure assessment of the degree to which the requirements are objectively verifiable and correct unverifiable requirements.		X	X	X			
Assess LV/SV integrated test plans.		X	X	X	X		

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Review assembly, test, and checkout procedures.		X	X	X	X		
Ensure operational concepts and requirement margin suitability.		X	X	X	X		
Assess need for simulations, models, and testbeds.		X	X	X	X		
Assess accelerated life test program.		X	X	X	X		
Ensure evaluation of COTS and Heritage HW and SW test requirements.		X	X	X	X		
Ensure interface control plan is integrated with IT&E plan and integration planning is complete.		X	X	X	X		
Ensure technical performance metric (TPM) can be sufficiently verified or validated.		X	X	X	X		
Ensure test planning adequately covers all operating modes and mission phases.			X	X	X	X	
Ensure test plans and procedures are complete, objectives are clear, and test success criteria are defined.		X	X	X	X		
Ensure special test facilities and equipment for integration and test verification are identified, reserved, and/or acquired.		X	X	X	X		
Assess Integration, Test and Evaluation as a Gated Process							
Ensure entrance and exit criteria are defined for assessment points in the test campaign.			X	X			
Ensure the I&T schedule is evaluated as a “gated” process.			X	X	X		

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure test campaign provides timely and credible results to support milestone decisionmaking.			X	X	X	X	
Conduct Software-Related Independent Analyses							
Ensure independent software modeling and analysis is performed.		X	X	X	X	X	X
Ensure independent software verification and validation (IV&V) is performed.			X	X	X	X	
Ensure onboard software mission constants are validated.			X	X	X	X	
Ensure onboard software qualification testing is validated.			X	X	X	X	
Ensure resources required for onboard software integration and qualification testing are validated.			X	X	X	X	
Assess Contractor Software-Related Plans and Processes							
Assess contractor's software unit test planning.			X	X	X	X	X
Assess contractor's software integration test planning.			X	X	X	X	X
Assess contractor's software qualification test planning.			X	X	X	X	X
Assess contractor's software test environments.			X	X	X	X	X
Assess contractor's installation and transition to operations planning.			X	X	X	X	
Assess IV&V contractor's plans.			X	X	X		

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess contractor's software implementation and test processes.		X	X	X	X		
Assess contractor's test process performance.			X	X	X		
Assess contractor's software test procedures.		X	X	X	X	X	X
Assess contractor's software test reports.		X	X	X	X	X	X
Assess contractor's software test activities.			X	X	X	X	X
Assess contractor's software installation activities.			X	X	X	X	X
Assess IV&V contractor's implementation and progress.			X	X	X	X	
Assess Ground Control and On-Orbit Test Perceptiveness							
Ensure evaluation of the contractor's allocation of ground control tests and on-orbit testing to verify and/or validate functional, performance, and/or interface requirements.			X	X	X		
Verify ground elements certified operational (including aerospace ground equipment [AGE] and range systems).					X	X	
Ensure the ground testing is complete and perceptive.					X	X	
Ensure the ground test program includes space vehicle ground control elements to accomplish space-ground compatibility checks and final ground control acceptance testing.				X	X	X	

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Adequacy of Assembly and Integration Strategy							
Ensure long-lead planning and procurement issues are evaluated.		X	X				
Ensure special test equipment integration is evaluated and incorporated in verification planning.			X	X			
Ensure preliminary segment integration planning adequately addresses buildup process and maintains equipment integrity.		X	X	X	X		
Ensure space vehicle system integration planning adequately address buildup process of the system operational (flight and ground control), test support, handling, calibration, transport, and protection equipment.		X	X	X	X		
Ensure overall systems integration completed and verified.				X	X	X	
Ensure GSE integration planning for the test support, handling, calibration, transportation, and protection of equipment is adequate and complete.		X	X	X	X		
Ensure planning conducted for all major system corrective actions is completed			X	X	X		
Ensure integration and test plan, from unit to system level, is of acceptable risk and credible schedule with reasonable margins.		X	X	X			

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Verification Test Results							
Ensure product satisfies system performance requirements.				X	X		
Ensure all non-conformance dispositions are completed.				X	X		
Ensure contractors utilized a consistent test methodology.				X	X		
Ensure contractor records, investigates, and corrects all failures/test anomalies.				X	X		
Ensure hardware and software testing is complete and requirements are verified and certified for use.				X	X		
Ensure system/subsystem testing is complete and requirements are verified.				X	X		
Ensure acceptance testing is complete and requirements are verified.				X	X		
Ensure system is integrated with other major components and performance is verified.				X	X	X	
Ensure requirements verification and sell-off packages contain accurate test data that supports contractor conclusions.		X	X	X	X	X	
Ensure analysis, simulation, inspection, and test results are evaluated to determine readiness to proceed to subsequent test or program activities.				X	X	X	

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess System Verification Processes and Ensure Tests Complete							
Ensure system verifications/test procedures are reviewed/approved for release.					X	X	
Assess system verifications/tests are performed in accordance with approved procedures.					X	X	
Ensure all anomalies/non-conformances are evaluated, closed, and/or acceptable to fly as-is.					X	X	
Assess D&OTE certification requirements, as they pertain to IT&E.			X	X	X	X	
Assess Intersegment Test Perceptivity							
Assess intersegment test perceptivity		X	X	X	X	X	
Deployment Test and Checkout (Vehicle Segment and Inter-Segment and Op Test and Evaluation Phase)							
Assess deployment test and checkout (vehicle segment and intersegment and Op T&E phase).						X	
Evaluate the conduct of the test.					X	X	
Evaluate post-test data.					X	X	
Evaluate buy-off/sell-off packages.					X	X	
Evaluate informal testing conduct and results.					X	X	

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Conduct informal testing for diagnostics.					X	X	
Evaluate test packages.					X	X	

8.9 References

Policy-Related

AFI 99-101	Developmental Test and Evaluation, 1 November 1996
AFI 99-102	Operational Test and Evaluation, 1 July 1998
AFI 99-106	Joint Test and Evaluation, 13 March 1994
AFI 99-109	Test Resource Planning, 21 July 1994
AFPD 99-1	Test and Evaluation Process, 3 April 2009
NSS-03-01	National Security Space Acquisition Policy, Guidance for DOD Space System Acquisition Process, 27 December 2004
SMCI 63-1201	Assurance of Operational Safety, Suitability, and Effectiveness for Space and Missile Systems, 16 January 2004

Specifications and Standards

ANSI/NCSL Z540.1	Calibration Laboratories and Measuring and Test Equipment—General Requirements, 2002
DOD-W-83755, Rev. A, Notice 1	General Handbook for Space Vehicle Wiring Harness Design and Testing, 4 September 1992

IEEE12207	Information Technology—Software Life Cycle Processes Software Verification, 2008
ISO/IEC 17025:1911	General Requirements for the Competency of Testing and Calibration Laboratories, 2005
MIL-STD-1543B	Reliability Program Requirements for Space and Launch Vehicles, 25 October 1988
MIL-STD-1833	Test Requirements for Ground Equipment and Associated Computer Software Supporting Space Vehicles, 13 November 1989
MIL-STD-45662	Calibration Systems Requirements, 1 August 1988
MIL-STD-785B, Notice 2	Reliability Program for Systems and Equipment Development and Production, 5 August 1988
MIL-STD-810F, Notice 3	Environmental Engineering Considerations and Laboratory Tests, 5 May 2003
TOR-2003(8583)-2895	Solid Rocket Motor Case Design and Test Requirements, 22 December 2004
TOR-2004 (8583)-3291	Criteria for Explosive System and Devices Used on Space Systems Vehicles, 9 August 2004, (replaces MIL-A-83578A and MIL-STD-1576)
TOR-2004(3901)-3242	General Guideline for Space Vehicle (SV) Verification Plan Development and Execution, 15 March 2004
TOR-2005(8583)-1 [also published as SMC-S-008(2008)]	Electromagnetic Compatibility Requirements for Space Equipment and Systems, August 2005 (replaces MIL-STD-1540D)

TOR-2010(3900)-2	Aerospace Mission Assurance Technical Baseline – Draft – National Systems Group Input, 30 April 2009
TR-2004(8583)-1, Rev. A [also published as SMC-S-016(2008)]	Test Requirements for Launch, Upper-Stage, and Space Vehicles (a k.a SMC TR-06-11), 6 September 2006

Handbooks

IBSN 1-884989-13-6	Nickel-Hydrogen Life Cycle Testing Reviews and Analysis, 2003
IBSN 1-884989-15-2	Space Modeling and Simulation Roles and Applications Throughout the System Life Cycle, 2004
ISBN 1-884989-14-4(V.2)	Spacecraft Thermal Control Handbook, Volume 2, Cryogenics 14-4 (v.2), 2004
ISBN 1-884989-11-X(V.1)	Spacecraft Thermal Control Handbook, Volume 1, Fundamental Technologies, 2002
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-334A	Environmental Stress Screening (ESS) of Electronic Equipment, 16 August 1993
MIL-HDBK-340A, Vol. II	Test Requirements for Launch, Upper-Stage, and Space Vehicles: Application Guidelines, 1 April 1999
MIL-HDBK-781A	Handbook for Reliability Test Methods, Plans, and Environments for Engineering, Development Qualification, and Production, 1 April 1996
MIL-HDBK-83575	General Handbook for Space Vehicle Wiring Harness Design and Testing, 4 June 2005

NASA Technical Memorandum 110172	Pyrotechnic Design, Development and Qualification, June 1995
TOR-2001(1465)-0934	Software Independent Verification and Validation (IV&V), 28 February 2001
TOR-2006 (8506)-4494	Space Vehicle Systems Engineering Handbook, 31 January 2006
TOR-2006 (8546)-4591	Space Vehicle Test and Evaluation Handbook, 6 November 2006
TOR-2006(3904)-1	Digital ASIC/PLD Development Handbook for Space Systems, 30 November 2005

Best Practices

AIAA-91-1302	Thermal Testing Explained, AIAA 26th Thermophysics Conference, AIAA Paper 91-1302, 26 June 1991
ATM 2002(3130-12)-1	Design and Verification of Launch and Space Vehicle Structure Briefing, 1 May 2002
ATM 2003(3907-62)-1	Recommended Sequence for Thermal Vacuum and Dynamics System Testing, 10 September 2003
TOR-2009(8586)-1	Unverified Failures (UVFs): What Are They, How Often Do They Occur, Why Do They Happen, and What Should Be Done About Them, March 2009

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 NDTI-80566	Test Plan, 13 April 1988
DI NDTI-80809B	Test/Inspection Report, 24 January 1997
DI NDTI-81284	Test and Evaluation Program Plan, 11 September 1992
DI QCIC-80553	Acceptance Test Plan, 25 March 1998

Other

Critical Process Assessment Tool (CPAT), 14 August 1998

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

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

Chapter 9
Operational Readiness

Rex Childers
Satcom Operations Support
Dan W. Hanifen
GEOINT Development Office
James B. Gin
AWTR Systems Engineering

9.1 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 operation. ORA begins early in development and continues through the system operational life. ORA is normally implemented via a combination of process/procedure planning, training, control, and verification activities.

9.2 Definitions

The term **'operations readiness'** refers to all the activities required to transport, receive, accept, store, handle, test, deploy, and/or control space vehicle (SV), launch vehicle (LV), supporting ground systems, auxiliary and ancillary facilities such that associated operations can be conducted safely and successfully. Basically, operations readiness includes those people, products, and processes that must be in place before the LV and SV can leave the launch pad.

Operations Readiness Planning is the set of activities required to develop and verify all of the products required to conduct the readiness activities mentioned above. These products include:

- Operations concepts
- Handling and testing equipment
- Handling, testing, and command control procedures
- Training and assessment of crew proficiency
- Ground system tailoring/modifications, if required
- Custom applications, where appropriate

Operations Activation is a set of activities whereby newly acquired capabilities and/or systems are evaluated by a government program office (PO), engineering development team, or joint contractor/government operations unit before they are validated and approved for mission operations. For the purposes of this

guide, activation includes SV activation on orbit, LV activation after successful completion of launch base processing when judged ready to perform flight operations, and ground system activation after deployment.

Mission operations is the program stage after LV processing and satellite and/or ground system activation where operators and users control the intended mission for the LV or satellite until completion end-of-life (EOL).

9.3 Objectives

The objectives of ORA as carried out by the government PO, development contractor, launch base team, and end users are as follows:

- Readiness Planning Assurance
  - Guarantees that the material handling of the elements of a segment and the interaction of personnel and external equipment with the segment itself can be, and are, executed safely and without causing damage to the system or to the handling equipment.
  - Ensures long-lead system issues are addressed, managed, and resolved by all program entities.
- Activation Assurance
  - Ensures that the SV and LV are configured and ready to perform mission and flight operations, respectively.
  - Ensures that the ground segment is fully functional, with software (SW) and databases compatible with the space segment.
  - Ensures that the end user and operational facilities have sufficient processes, products, and personnel to successfully maintain both ground and space segments.
  - Ensures rehearsal content and conduct covers all nominal operational activities, as well as sufficient non-nominal events, to mitigate assessed risks.
- Mission Operation Assurance
  - Ensures mission and SV performance are maximized.
  - Ensures risk management analysis (RMA) data are gathered and analyzed.

- Ensures the PO and end user community perform, with Aerospace support, studies and analyses focused on improvements to follow-on spacecraft and payload requirements and design.
- Ensures total space segment management, including life-extension analyses and disposal planning.

For LVs the objectives of ORA are successfully demonstrated when an LV reliably completes flight operations and places its payload in its intended orbit.

For SVs the objectives of ORA are successfully demonstrated 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 development and verification of all products and processes required to conduct operations to ensure they are consistent with overall system integrity and safety goals, and, on the other hand, the validation that the operational use of these products and processes meets their intent and preserves actual system integrity and safety.

9.4 Practices

9.4.1 Core Activities

9.4.1.1 Readiness Planning

Table 9-1. Readiness Planning Tasks

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Summary of Operations Readiness Tasks	X	X	X	X	X	X	X
Assess impacts of operations concepts and implementation	X	X	X	X			
Assess requirements implementation		X	X	X	X		
Assess security requirements and implementation		X	X	X	X	X	

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess simulation effectiveness and certification				X	X	X	
Assess flight/ground SW I&T				X	X	X	
Assess site activation and transition plans				X	X	X	X
Assess schedule integration and executability					X	X	
Assess communications readiness					X	X	
Assess factory support and preparedness					X	X	X
Assess facility/hardware (HW)/SW maintenance processes					X	X	X
Assess configuration control					X	X	
Assess system functionality					X	X	
Assess rehearsal preparation and execution						X	
Assess staffing and training preparedness						X	
Assess operations products						X	
Assess facilities’ readiness						X	
Assess system/launch readiness						X	
Assess system operability						X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess system RMA						X	X
Ensure mission performance						X	X
Ensure and evaluate on-orbit operations						X	X
Generic Operations Readiness Task	X	X	X	X	X	X	X

Identification of Operations Requirements. Readiness planning is a continuous activity over the life cycle of the system and contains critical mission assurance (MA) 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. LV system, ground transportation, and launch base infrastructure requirements and operations concepts are developed for the resources needed to successfully process and launch the SV. Physical, functional, environmental, operations, performance, and safety requirements are identified and testability, safety, launch base processing, and SV pathfinder activities also are considered and documented.

Human factors engineering considers the functions that have been allocated to system operators and users, how much time is allocated for these tasks, what information is required and level of proficiency is needed, and how the system operators, maintainers, and users will interact with and use 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 SV readiness planning process. Fault conditions as indicated by the contractor’s failure mode

and effects analyses (FMEAs) are addressed with associated contingency operations developed to ensure the SV 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.

Development and Delivery of Operations Products. The responsible government PO works with the launch base/deployment site and range operations personnel to ensure all operations planning is completed and in place for receiving the HW, utilizing needed facilities, security, safety, launch processing, environmental impacts, administrative communications, and telemetry receipt and processing, and ensuring radar and optical tracking 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 handling and storage of the system and its components are adequate.

Ground site(s) infrastructure requirements and operations concepts are developed for the resources needed to successfully command and control the SV from separation from the LV through mission life. Physical, functional, environmental, operations, performance, and safety requirements are documented. Testability and training activities also are considered.

The responsible government PO works with the operations base/command and control site personnel to ensure all operations planning is completed and in place for utilizing needed facilities, security, safety, environmental impacts, communications for administration, and telemetry receipt/processing to support activation 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 they are adequate to support on-orbit operations.

The operations team, with support from the development team, develops operational concepts, team processes, and handling and control procedures such that launch base, launch, initialization, mission, and contingency operations can be conducted safely and successfully. Verification occurs through a combination of inspection, exercise, simulation, test, and review.

Contingency planning is a necessary element in the overall SV readiness planning process. Fault conditions as indicated by the contractor’s FMEAs are addressed with associated contingency operations developed to ensure the SV 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.

In many instances, it is impractical to utilize pathfinder or flight vehicles to support contingency and training activity, thus requiring the development of simulators. 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. Planning should address the development of simulator requirements, including human-machine interaction requirements, possible reuse of contractor's SW test tools, and approach in certifying the resultant simulator's use.

Monitor and Review Development and Test Operations. A program must have a thorough and timely understanding of development and test activities for the HW and SW to begin operations planning, identify changes required in that planning, and ensure such changes are implemented expeditiously. To this effect, operations personnel monitor ongoing system development to fully understand capabilities and limitations of the HW, SW, 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.

Ideally, factory acceptance testing (FAT) would use the procedures, simulators, and test equipment developed for the launch and operations phase. The program operations personnel review the detailed FAT 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 conduct of the actual test. Test report results are reviewed and accepted prior to shipment to an operational deployment site. This review includes HW buildup and acceptance test pedigree data for both flight HW and ground support equipment, including reports on any test anomalies.

Training Development and Execution. The operators of the SV, LV, and ground system require training on the space or launch vehicle they will be operating as well as on the ground system(s) they will be using to accomplish operations. The developer, with input from the operator, develops the required training and in some cases provides the initial training to the operators. For launch and early orbit operations actual team rehearsals and exercises are conducted.

Pre-Ship Reviews. The program conducts HW pre-ship reviews (PSRs) to ensure flight HW and components, SW, ground support equipment, and procedural documentation are ready for transport 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 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, or other receiving site, to ensure the site is ready to receive program HW, receiving support has been appropriately scheduled, and receiving facilities are prepared to support HW arrival and post-shipping inspection activities.

9.4.1.2 Activation

Launch/Deployment Base Operation Activation. On arrival of the SV or LV at the launch base, PO personnel participate in all ground support operations required to configure and validate the SV or LV system(s) readiness for launch. In many instances, The Aerospace Corporation (Aerospace) is required to certify that the operations were satisfactorily executed as part of the launch certification process.

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 PO 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 any deficiencies in crew setup are documented and assessed as not mission critical, with workarounds established.

Pre-Flight Review of Flight Operations. A flight operations review (FOR) is conducted before each launch. The system contractor joins the government PO 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 all flight and ground HW, SW, personnel, and procedures are ready and all interface and cross-compatibility issues have been identified and resolved

In the case of the deployment of an SV 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 SV or ground system.

9.4.1.3 Launch Vehicle Mission Operations

Flight Operations. The program conducts flight operations with the LV contractor and the range/launch site operator, and performs operational readiness testing. From an MA perspective, the launch operations review of launch processes and procedures has the primary objective of assessing system performance, identifying lessons learned, and developing implementation plans to incorporate those lessons learned in the procedures of the next launch cycle. Prior to mission operations a review is held to assess readiness for the ground systems to support mission operations. Specifically the purpose of the review is to:

- Examine demonstrations, tests, analyses, and audits to determine system readiness for a safe and successful mission operations

- Ensure all ground HW, SW, personnel, and procedures are ready and all critical interfaces and cross-compatibility issues have been identified and resolved prior to commencement of mission operations

- Ensure all non-critical interfaces and cross-compatibility issues have been identified and there is a suitable plan for mission operations

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 an 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 in the procedures of the next launch cycle. A "post deployment review" can be similarly conducted for SV systems once on orbit and/or for supporting ground control stations or systems.

9.4.13 On-Orbit Satellite Activation Operations

- After the SV has separated from the LV, PO personnel participate in all operations required to initialize and validate the SV's readiness to perform mission operations.

- Prior to transitioning from activation to mission operations a review is held to assess readiness for mission operations. Specifically the purpose of the review is to:

- Examine demonstrations, tests, analyses, and audits to determine system readiness for a safe and successful mission operations

- Ensure all SV and ground HW, SW, personnel, and procedures are ready and all critical interface and cross-compatibility issues have been identified and resolved

- Ensure all non-critical interface and cross-compatibility issues have been identified and there is a suitable plan for resolution post transition to mission operations

9.4.1.4 Ground System Activation Activities

After the installation of a new ground system at the operational deployment site, PO personnel participate in all ground support operations required to activate and validate the system(s) readiness to support operations.

- Prior to transitioning from activation to mission operations a review is held to assess readiness for the new ground system to support mission operations. Specifically the purpose of the review is to:

- Examine demonstrations, tests, analyses, and audits to determine system readiness for safe and successful mission operations

- Ensure all ground HW, SW, personnel, and procedures are ready and that all critical interface and cross-compatibility issues have been identified and resolved

- Ensure all non-critical interface and cross-compatibility issues have been identified and there is a suitable plan for resolution post transition to mission operations

9.4.2 Standards/Recommended Practices

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 (a k.a. 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 document for 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).

9.5 Key Lessons Learned

At each review lessons learned in the process of arriving at the major milestone or transition point in the development and deployment of the vehicle or system are identified and documented. A lesson may consist of preventable errors uncovered, a HW or SW flaw corrected, or a beneficial method identified. Lessons learned can also cover procedural steps and improvements in HW, SW, and procedures. Lessons learned for a particular SV or LV or ground system may have applicability to other vehicles and systems. The applicability of each lesson to this SV or LV and ground system must be appraised by the Mission Assurance Guide (MAG) team. Those determined to have applicability for this event must be used to guide procedure development or modification.

9.6 Task 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.

Phase 0. In Phase 0, the proposed system operational suitability is assessed along with ensuring consistency of the operation concepts that are captured in pre-Milestone A program summaries, including capabilities development document, initial concept of operations (CONOPS), 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. Ensuring that the appropriate human engineering standards (such as Standards for Human Computer Interface found in the ISO) 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 (TRD) or following system specifications developed in Phase A for feasibility and consistency with the program documentation.

In addition, Phase 0 should include assessment and oversight of:

- Military construction (MILCON) or equivalent funding and approval processes understood for new and/or modified operations structures

- Security concerns addressed and approved, regarding all locations requiring government physical security (commercial buildings, city/state codes affecting physical defense, Secretary of the Air Force (SAF) and Department of Defense (DOD) security approvals, etc.)

- Operational command funding, staffing, training, and re-call for backup locations

Phase A. During Phase A, operational personnel should be represented at the system design review (SDR) 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 HW and SW elements are assessed.

The operational readiness process will also examine the related operational infrastructure. If the required infrastructure is not available, the MA process should ensure those infrastructure requirements are identified and a determination made as to whether they can be acquired with programmed resources in time to support the program. During Phase A, MA will also ensure 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.

Phases B and C. As the design progresses through Phases B and C, the operational readiness MA process examines the detailed design to ensure 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 ensure 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.

Phase D1. 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 Phase D1. During the Phase D1 fabrication and integration, launch site personnel and ground segment operators and support personnel participate in factory acceptance and qualification testing activities to ensure 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 (GUIs) and often requests refinements during this phase.

Phase D2. At the end of Phase D1, launch base planning and procedural development are completed. MA planning would address the Phase D2 verification tasks required to support launch preparation and government's launch certification process. Launch "commit" and abort criteria are developed and refined in Phase D2 and verified under the operational readiness MA process. Launch site procedures are also verified during Phase D2 and placed under configuration management (CM) along with associated scripts and test

SW. Prior to the actual delivery of the flight equipment to the field, MA would ensure 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. Command plans and other operations procedures are verified during Phase D2 and placed under CM. As the launch site processing continues, incremental operational reviews are conducted at both the launch and ground sites to verify readiness to proceed with the next activity. In support of the test and evaluation master plan (TEMP), 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 Phase D2, launch preparation operations are conducted. Specific targeted mission parameters are verified along with day-of-launch placards.

Phase D3. During Phase D3, the actual launch, activation, 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.

9.7 Government and Contractor Enabling Processes and Products

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 phases is access to the government's draft and final RFP, the negotiated contract, the capabilities description document, CONOPS, and TEMP. Operational personnel should participate in all the stages in requirement and design development as well as during the vehicle qualification and acceptance testing. Access to PSRs is critical in that the operational community should ensure 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 should 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 (ORAs) 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.

9.8 Practice Task Application Example

The readiness tasks encompass all the activities required to plan, transport, receive, accept, store, handle, test, deploy, and configure launch and space vehicles and supporting ground systems in preparation for launch, activation, and mission operations. 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 operational safety, suitability, and effectiveness process.

The objective 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 the integrated system (including HW and SW 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 to ensure 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 ensure 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 should become familiar with not only the flight equipment, but also the ground support equipment and associated SW 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

should be verified with regard to maintaining vehicle integrity while performing their intended function.

See Table 9-2 for an example of SV operational readiness MA tasks. (These tasks do not include the ground system ORA.)

Table 9-2. Example of SV Operational Readiness MA Tasks

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Impacts of Operational Concepts and Implementation							
Ensure operations impact on and inputs to system CONOPS	X	X	X	X			
Ensure operations implementation of system CONOPS			X	X	X	X	X
Assess Requirements Implementation							
Ensure requirements are implemented with operational provisions		X	X	X	X	X	X
Assess Rehearsal Preparation and Execution							
Ensure rehearsal execution, fidelity, and improvement						X	X
Ensure launch commit criteria						X	
Ensure application of rehearsal lessons learned						X	
Assess Staffing and Training Preparedness							
Ensure operational crew training content and conduct						X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Operations Products							
Ensure command procedure adequacy						X	X
Evaluation On-Orbit Operations							
Evaluate and support anomaly recovery process						X	X
Evaluate non-nominal operations activities						X	X

9.9 References

Policy-Related

AFI 10-1201	Space Operations, 25 July 1994
AFI 10-1211	Space Launch Operations, 17 July 2006
AFI 16-1001	Verification, Validation, and Accreditation, 1 June 1996
AFI 99-102	Operational Test and Evaluation, 1 July 1998
AFSPCI 10-1208	Spacelift Operations, 1 November 2005

Specifications and Standards

MIL-STD-1472F	Design Criteria, Human Engineering Standard, 5 December 2003
MIL-STD-1833	Test Requirements for Ground Equipment and Associated Computer Software Supporting Space Vehicles, 13 November 1989

SMCI 63-1201	Suitability & Effectiveness for Space & Missiles Systems, 1 April 2004
SMCI 63-1202	Space Flight Worthiness, 1 April 2004
SMCI 63-1205	The SMC System Safety Program, 28 June 2011
TR-2004(8583)-1, Rev. A [also published as SMC-S-016(2008)]	Test Requirements for Launch, Upper-Stage, and Space Vehicles, 6 September 2006

Chapter 10
Operations & Sustainment

Mark M. Oleksak
DMSP Spacecraft and Operations

10.1 Introduction

The purpose of this chapter is to describe the various mission assurance (MA) tasks required to perform engineering assessments, detail changes and impacts, and address subsequent changes to the system. Internal changes (i.e., anomalies, aging system, and usage degradation) and external changes (i.e., changing threats) during the operations phase of the program life cycle require MA activities that are largely one and same as in earlier life cycle phases. The life cycle of any system should include a scheduled development sustainment program.

10.2 Definitions

An **acquisition** is the conceptualization, initiation, design, development, testing, contracting, production, deployment, and disposal of a directed and funded effort that provides a new, improved, or continued materiel, weapon, information system, logistics support, or service capability in response to an approved need.

Development is part of a broader term, Research, Development, Test and Evaluation (RDT&E). The term “research and development” (R&D) broadly covers the work performed by a government agency or the private sector. Research is the systematic study directed toward gaining scientific knowledge or understanding of a subject area. Development is the systematic use of the knowledge and understanding gained from research for the production of useful materials, devices, systems, or methods. RDT&E includes all supporting test and evaluation activities.

Maintenance keeps a system or system components in proper condition and repair.

Operations is the use of the system, subsystem, or major end item in its intended application.

Sustainment is continuous materiel support which consists of the planning, programming, and execution of a logistics support strategy for a system, subsystem, or major end item to maintain operational capabilities from system fielding through disposal.

Initial Operations Capability (IOC) is the first attainment of the capability to effectively employ a weapon, item of equipment, or system of approved specific characteristics with the appropriate number, type, and mix of trained and equipped personnel necessary to operate, maintain, and support the system. IOC should be event-driven and not tied to a specific future date.

Interim Contract Support (ICS) is temporary support method for an initial period of operation for a system, subsystem, training system, equipment, or end item.

Satellite Control Authority (SCA) is authority to command and control the spacecraft.

10.3 Objectives

The key objective in this phase of the program life cycle is to operate and sustain the system from fielding to disposal. Sub-objectives may be defined, such as:

- Field the system(s)
- Operate the system such that the mission (communication, navigation, surveillance, etc.) is fulfilled
- Sustain/maintain the system to maximize uptime and minimize downtime
- Characterize and trend system performance on an ongoing basis
- Be positioned to diagnose issues and repair the system as quickly as possible
- Replace and safely dispose of the system as it wears out, becomes too expensive to sustain, or is replaced by a new system with improved capability.

The goal is to maintain performance through continued monitoring, predictive assessment, periodic maintenance, and asset replenishment (to include database updates). If performance, realtime or predicted, is determined to be less than the minimum acceptable performance then recovery activities are based on the system performance projections. Degradation is at times realized as an artifact of component age, usage-related degradation, or component failure. The life cycle of any system should include a schedule development sustainment and modernization program.

10.4 Practices

System requirements can be thought of as belonging to or being sourced from one of three major stakeholders: acquirers, operators, and maintainers. Ultimately all requirements come from the operator or user of the system as the acquirers and maintainers exist to support the operator. The acquisition stakeholder, the program office (PO), is responsible for the sustainment of the system and is concerned with the formal allocation and verification and validation of top-level operational requirements as they are decomposed to the various system end items. The maintenance stakeholder is concerned with keeping the system operational. The objective of the maintenance is to preserve the functions and sustain the inherent level of reliability with the operation context over the life of the program. To accomplish this maintenance, data documentation records and tracks various maintenance activities. This applies most aptly to the ground segment when replacement purchases are made and are subject to the original acquisition. Maintenance may perform trending analysis in the case of ground segment for predictive replacement cycles. However, the space segment reliability and assessment engineering is usually executed by the acquiring stakeholder to ensure the readiness of the system to perform the assigned mission until the end of the designed or projected life cycle. Inputs to these processes include data generated by the operators and the maintainers. Changes to the technical baseline are an artifact of both external (i.e., changing threats) and internal (i.e., anomalies, aging system, usage degradation) factors.

10.4.1 Core Activities

The core MA activities in this phase should support the ongoing sustainment of the system elements and mission operations. These include the following activities.

10.4.1.1 Software Sustainment

Software sustainment applies to the space segment (satellite constellations) and to the ground segment (used for command and control of on-orbit assets) for the D3 phase of a program. These deployed systems are software intensive. Chapter 18 describes SW assurance and will be a key touchstone for a D3 program. Sustainment releases of SW can occur on a regular schedule or as required. All releases must meet the operational requirements of the system. Some general categories driving SW updates are: corrections to noted anomalies or discrepancies; insertion of diagnostics for troubleshooting/insight; workarounds in SW for hardware (HW) problems; changes in mission requirements; and updates to reflect commercial off-the-shelf (COTS) product releases.

The software life cycle model complexity and the SW life cycle as described in Chapter 18 illustrate increments, spirals, or builds occurring early in the development, roughly occurring in the preliminary design review (PDR) to critical design review (CDR) of the program life cycle. The specific MA tasks and reviews for a sustainment phase SW increment, spiral, or build however will likely be tailored and could be a somewhat different set than those from earlier in a program's life cycle. In principle the same processes and MA tasks should be followed for any SW development with tailoring as appropriate in consideration of the application and phase of the program.

A sustainment build will by definition occur after fielding the system. One direct consequence of this situation is the near certain unavoidability of temporarily taking the asset in question out of mission to load and/or activate the new build or increment. The recommended approach for sustainment SW builds is to divide the MA activities into two major activities. The first activity is "factory"-centric and consists of the tasks needed to ensure the SW product is adequately built and tested and is low risk/ready for the intended use.

The second major activity is "site"-centric and is focused on readiness to load and activate the SW product in question. This can actually be considered a form of operations readiness assurance (ORA), (see Chapter 9). This activity is also considered a form of Readiness Review (see Chapter 11). This overall approach overlaps with readiness reviews conducted by the system operators at the operational sites. The dual approach of the PO and the Operating Wing or Squadron both conducting overlapping reviews has been found to be highly effective and synergistic. Also note that one additional consideration is operational security. The dates or times that the asset in question will be taken out of service to perform a load will likely be considered classified.

A final consideration for D3 software MA is assessing the need and the value of retaining Federally Funded Research and Development (FFRDC) or systems engineering and technical assistance (SETA) flight (or ground) flight or mission software simulation labs and environments. If the PO has been receiving flight software releases from the contractor during the development phase, retention of that simulation environment in light of a likely decreased engineering budget needs to be considered and appropriately resourced. Continuation of such environments allows for continued MA support as flight software sustainment releases occur. Existence of a realtime simulation laboratory allows the PO sustainment team to bring more to the table in terms of technical contributions and timely response when anomaly investigations are required.

10.4.1.2 Hardware Sustainment

HW sustainment is obviously a different consideration for the ground segment in having the possibility of addition/subtraction/replacement of HW. The goal of

maintenance to the ground element is to maintain performance through continued monitoring, predictive assessment, periodic maintenance, and asset replenishment. If performance, realtime or predicted, is determined to be less than the minimum acceptable performance recovery planning then planning lead time before system impact is based on the component/system performance projections. Recovery and modernization includes component updates and modification, improvements as opportunities, and component redevelopment as necessary to ensure performance is maintained at levels above the acceptable performance parameters. Replan efforts imply new spiral(s) of development (HW and SW) and MA tasks for early acquisition life cycle, sometimes back to preliminary design. Under this scenario, the core MA processes (CMPs) for early life cycle phases should be re-examined and replanned for the new or modified ground segment. The User segment may similarly require a replan effort reaching back to processes and MA oversight considered early in a typical development life cycle. Each program and each situation will be unique and the MA approach will depend on the specific circumstances encountered.

Engineering budgets for programs that have achieved IOC and are funded on operations and maintenance (O&M)/3400 color of money will likely be reduced compared to earlier development phases. Limited budgets constrain the amount of long-term/ongoing performance characterizations and HW trending. An initial and comprehensive set of on-orbit performance tests and characterizations will have been performed at the beginning of life (BOL) during on-orbit developmental and operational tests. The continuation performance and HW health trending (and engineering analysis of the collected data) once normal mission ops and sustainment has commenced will be limited. In all likelihood, operational elements, strings, and components that are exhibiting nominal performance and smoothly varying telemetry trends will receive only minimal engineering review and analysis. One exception to this rule may be for key mission-enabling components. For example, both the Navigation and Protected Satcom mission areas depend on high-precision atomic clocks on board the respective satellite constellations. The Aerospace Corporation (Aerospace) is funded by both mission areas to keep a close watch on the performance of these key components.

A related question that should be addressed is the value of taking custodianship of any available or surplus development-phase government-owned/contractor-built and operated assets. These could be high-fidelity engineering model (EM) boxes, life-test units, downgraded flight units, or full-up flight spares. If the development contractor continues to support the program in the operations and sustainment phase, then EM, life-test, and/or residual flight units would likely continue to be used by the contractor in their continuing support. If, however, the contractor’s scope in sustainment is such that these assets will not be used, the PO should consider requesting custodianship of the assets. Examples include the PO acquisition of life-test traveling wave tube (TWT) amplifiers and flight

spare rubidium master oscillator atomic clocks. These assets were successfully leveraged to support Aerospace independent R&D activities and long-term device characterizations as well as providing insight into performance and trending of the analogous HW flying in the operational satellites and future operational satellites.

10.4.1.3 Operations Mission Assurance

Of vital importance for the overall MA effort is the existence of an embedded PO presence at the operational site. The embedded or site PO presence provides a front-line perspective. The ideal working relationship between the two PO components (i.e., at the Material Wing and at the operational site) should be close and continuous, with free two-way communications. Both parties will have a unique perspective on the program and mission. PO planning for MA in the D3 phase needs to consider how that support will cover both the normal ops scenario as well as the scenario of anomaly ops and recovery. A few typical support examples during normal ops include independent verification of new or changed commands, independent readiness assessment for SW uploads, passplan review for satellite repositioning, and select independent trending of HW unit performance. The PO presence at the operating site will serve as the "first responders" to any anomaly encountered. It is incumbent on the PO to define the process for dealing with anomaly notification and recall of personnel. This process will need to comply with appropriate security classification issues arising out the anomaly and resulting loss (either temporary or permanent) of mission capability. The same applies for any vulnerability that may be revealed either as a result of an anomaly or just through the insights gained by close observation of the system in operational use. While there is no doubt that support to development phase programs is important and at times can be very stressful, programs in the mission operations phase raise the *Responsiveness* bar. By definition, these systems are supporting DOD missions and operations of critical importance to our country. Support to a D3 phase program will require a dedicated team that is structured and willing to respond to anomaly recalls and operational issues on a "24/7" basis. Of course, funding/budget limitations and available engineering resources will serve as constraints to that support. Access to classified communications (video teleconferences [VTCs], Secret Internet Protocol Router Network [SIPRNet], etc.) is an additional consideration.

The attrition represents a challenge to those given the responsibility to manage the sustainment support post-IOC with careful consideration of the types of skills and resources that will need to be retained. Migration of staff to a follow-on effort within the same mission area is a preferred outcome from a reach-back perspective. For example, a key engineer for a spacecraft subsystem can almost always be more easily borrowed back from the follow-on program in the same organization than from another unrelated mission area/organization. Sustainment

resourcing requires a thoughtful strategy that considers limited resources with planned activities as well as unplanned contingencies (i.e, anomalies).

10.5 Key Lessons Learned

Applicability of any particular lesson learned will vary program to program. The following are some general lessons learned to consider in the operations/sustainment phase of a program.

- Plan for an abrupt funding level change at sustainment. While there is a clear ramp-up and later ramp-down of funding and manpower during development, the onset of sustainment can result in a sharp drop in funding. Staffing plans will need to reflect the reduced funding. In addition, the types of skills required, and even the location of the staff, may change for sustainment. Programs should plan and appropriately resource a scheduled sustainment program.

- Create a data and knowledge retention process/system during development that may be accessed later during the sustainment phase of the program. Resolution or workaround of anomalies often requires access to low-level design and/or build documentation to work problems to their root cause.

- Assess compatibility of the current system in the sustainment phase (and impacts of changes to that system) to the follow-on system proposed or in development. Requirements for compatibility between a system in sustainment and a successor or follow-on system may lead to tension between the sustaining and developing organizations. Changes implemented during sustainment (typically to address deficiencies or discrepancies encountered during operations) can be viewed as new or changed requirements to the developing contractor(s) of the successor or follow-on system. That will almost certainly lead to negative cost impacts in the development program. If analogous changes are not implemented in the follow-on system, however, compatibility may be jeopardized.

10.6 Task Execution

10.6.1 Requirements Satisfaction

The operational baseline is documented through technical command media (i.e., technical orders). For the most part, the day-to-day operations and maintenance are executed through prescriptive processes. Outputs of these activities include reports that document the repair, maintenance, material improvement, incidents,

and deficiencies. This data is used to provide proactive predictive trend analysis of the readiness of the systems, however the data can also be accessed in the case of a mishap or major incident to provide a reactive assessment specific to the incident or deficiency. The data and analysis are subject to additional analysis to verify the system operational requirements are not less than the minimum acceptable performance. Based on a requirements assessment a risk may be identified that may be validated for product development (i.e., HW fix/buy, SW update). These modifications are subject to a change control process that includes revalidation of the system requirements. The change control process includes updates to the system baseline to reflect new operational and/or maintenance requirements associated with the modification. The major modifications, or "replans," are considered separate acquisitions and are required to follow the standard system engineering processes (and appropriate MA) to include qualification, acceptance testing with full functional and physical audits of the modification prior to deployment. The system PO is responsible for the modifications to ensure continued successful operations. Figure 10-1 provides a graphic representation of the change control process that is executed by the sustainment PO.

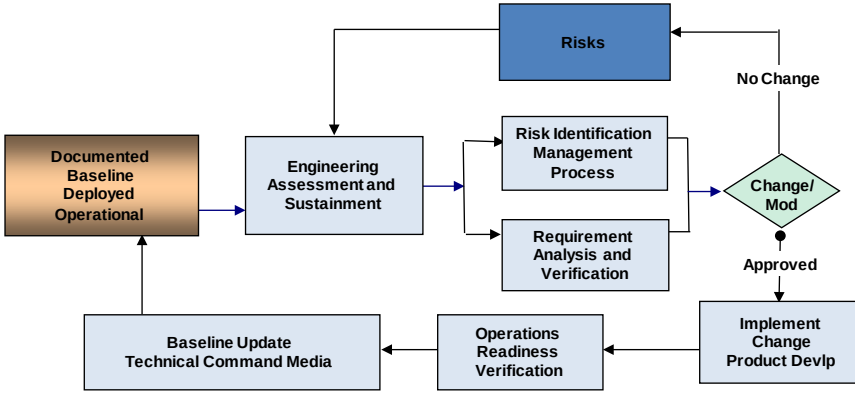


Figure 10-1. Requirements Satisfaction in the Sustainment Phase of the System

Programs in Phase D3 must continue to ensure that system requirements remain satisfied to the extent possible as assets age and eventually degrade or fail and/or disposal is executed. Note that much of the effort during the Operations and Sustainment phase will focus on SW (Space and Ground segments). The system engineering model shown in Figure 10-1 is fully applicable to that effort. Alternative SW systems engineering (SE) models, such as the ones developed by the Software Engineering Institute, are also available.

10.6.2 Program Documentation and Knowledge Retention

A proactive and preplanned effort should be made for any key program technical and programmatic documentation. A knowledge retention program should be established earlier in the program life cycle, with important documents archived in a government repository such as Livelink or similar database. If this was not done in earlier phases, a round-up of key program documents and data should be considered. This activity is essential to support and maintain the SE processes shown in Figure 10-1. The contractors of the program should have their own data retention/knowledge retention as contractually required by the government customer.

10.6.3 Risk Management

Risk identification and management/mitigation at this stage of the life cycle is vital. The PO analysis and depth of effort for any particular MA task will be constrained by available engineering resources and available budgets. Most, if not all, identifiable risks at this stage of the program life cycle take the form of … if risk X is realized, mission operations will be impacted. In fact, one view of the Operations and Sustainment phase is that it is all risk management for the government PO. That is, all activities undertaken by the PO in support of an operational system are actually risk management tasks. This view is especially cogent given the almost certain reduction in available funding compared to the development phase. In this type of environment, a prioritization scheme will be necessary to "buy down" the risk to the extent the budgets allow.

The mechanics of the risk identification and management process in the Operations and Sustainment phase are much the same as in the earlier development phase. Risks should be identified in terms of likelihood of occurrence and impact if the articulated risk materializes. Mitigations should be identified and developed; however, those mitigations will be constrained by resource budgets. Periodic refresh of the program's top risks should continue to be conducted. Analysis of system operational and trend data, as well as discrepancy or outage reports, etc., will serve as one source of risks in this phase.

One generic risk for any program utilizing a space segment is that of aging on-orbit satellites. Short of a NASA Hubble Space Telescope –like refurbishment mission, deployed satellites (especially those in above low Earth orbits [LEOs]) will not receive any hands-on maintenance. Many satellites do however continue to function long past their design life requirements, in large part because of the presence of redundant components. As redundant components are "consumed," the risk to additional mission life increases. Aging, of course, also occurs in Ground segment equipment. The risk here, however, can be greater mitigated as

the equipment in question is generally accessible and can be repaired or replaced.

10.6.4 Simulations and Tools

Continued use of independent simulations or tools post-IOC requires consideration. Allocation of sufficient budget for engineering staff *and* their tools and simulations will be required. Any “crown jewel” simulation used by the PO during development will almost certainly remain very useful for the post-IOC operations phase. If use of development phase simulations and tools is not planned in the operations phase, the development simulations and tools should be well documented and provisions made to the extent feasible to archive those for possible re-activation. As an example, at the time of writing this chapter, the reactivation of an Aerospace program satellite controls simulation originated more than 20 years ago was successfully undertaken. This simulation was used to great success in modeling the stability of a contractor-proposed life extension technique. Creating or recreating such a simulation from scratch during the operations phase of this program would have not been feasible from a manpower budget or timeliness perspective.

10.6.4.1 Reliability Modeling

One key modeling area carried on from the development phase is that associated with reliability. Satellite reliability models require periodic update to reflect the accumulation of on-orbit in mission life as well as incorporation of any on-orbit component failures; extrapolations of depletion of fuel or other expendables; and inclusion of any satellite or mission life-limiting wear-out mechanism extrapolations. These factors serve as the basis for possible truncations of the satellite reliability curves, which in turn are the basic input into the Aerospace General Availability Program (GAP) model. The various mission area functional availability reports produced by Air Force Space Command Headquarters (AFSPC HQ)/A3 staff are underpinned by the Aerospace GAP results. AFSPCI 10-140, Satellite Functional Availability Planning, serves as the government command media for this task. One aspect of Aerospace independent MA in this area is to review and either concur with or adjust as necessary contractor-provided reliability model updates and life-limiting extrapolations. In AFSPCI 10-140, these items are referred to generically as “parameter lists.” GAP results and associated functional availability reports are important inputs for the 14th Air Force/A3 chaired Constellation Sustainment Assessment Team (CSAT) reviews. The CSAT in turn, form an important input to the joint Consolidated Space Launch Review Board process for determining national launch priorities for constellation build-up or replenishment. The same reports also support government acquisition planning for follow-on or replacement systems.

10.6.4.2 Collision Avoidance

Another important modeling and simulation task in this phase is collision avoidance (COLA). This is not the one-time launch COLA task that will have occurred during satellite fielding. Rather, this is the ongoing effort to ensure adequate spacing between a program's space assets and all other active or inactive objects. The importance of this task was certainly emphasized recently in the satellite-to-satellite collision of an inactive Russian satellite (COSMOS 2251) with the then-operational Iridium satellite 33.[74] AFI 91-217, Space Safety and Mishap Prevention Program, is the relevant government command media for COLA. The COLA task is also called out in AFSPCI 10-1204, Satellite Operations. The PO and Aerospace MA depth of effort in the area of COLA can vary from none to significant and is dependent on the specific needs of the program and available resources to fund support. Aerospace specialists should be consulted as to a program specific support plan for performing probability assessments when a near approach is predicted. One challenging situation, for example, can arise at geosynchronous orbit, when a space asset ends up co-located with another satellite in the same orbital slot or box. COLA in this case can then become a repetitive "production"-like process. Satellite repositions ("repos") also represent a potential MA task. Repos can involve both a general readiness to execute the operation as well as more specialized subtasks such as COLA. Operational security concerns may require that the timing of the reposition be held as classified.

10.6.4.3 End of Life/Satellite Disposal/Fuel Remaining

The D3 phase of the life cycle concludes with satellite disposal. The policy of the United States (U.S.) is to dispose of satellite assets so as to not leave space junk in orbits used by active missions. Disposal strategies must take into account the laws of physics and orbital mechanics. Satellites in geosynchronous orbits should be super-synched into the graveyard orbital belt, which is located approximately 300 km above. AFSPCI 10-1204, Satellite Operations, paragraph 3.6 provides general guidance for disposal. Detailed direction is found in AFI 91-217.

Low Earth orbiting assets may be driven into the atmosphere, wherein all but the most robust pieces should burn completely on entry into the atmosphere. This strategy can be controversial, as was the case in 2008 when the U.S. brought down a national asset that was declared non-operational. In this case, the controversy was largely because of U.S. Navy Aegis system surface ship launched missiles that intercepted the asset and broke the asset into small enough pieces that none would survive re-entry. The reader may also recall the

[74]"Iridium Incident Highlights Growing Risk of On-Orbit Collisions," Space News Business Report, February 19, 2009, Becky Iannotta.

Soviet Union spacecraft that re-entered the Earth's atmosphere and crashed into Canada in the 1970s. That case of an assumed unintentional disposal was also extremely controversial because of the presence of a nuclear isotope power generation subsystem in the asset.

One key MA task related to satellite disposal is the vetting of the specific criteria that will determine when a satellite is at end of life (EOL). The most obvious and well-known criterion is fuel remaining in the satellite. An allocation in the fuel budget for disposal should be made back in the earlier design phases of the program. Indentifying fuel remaining as an MA task will depend largely on how close the satellite is to running out of fuel. However, even in cases for which satellites are nominally many years away from fuel exhaustion, the sustainment team should consider fuel remaining as a MA task. Propulsion subsystem modeling accomplished during the development phase should be refined, updated, or improved as satellites are fielded and operated. Various modeling and estimating techniques for fuel use are available. These techniques can use various observable or derivable mass properties to back out remaining fuel. The "bookkeeping" (debiting the remaining fuel "account"—a specific amount for each propulsion engine firing) technique alone may be used, but can suffer from a buildup of error over the life of the mission. Some Space and Missile Systems Center (SMC) programs have been caught by surprise when a satellite unexpectedly "ran out of gas." Other techniques should be employed when possible to mitigate the risk caused by inaccuracies in the bookkeeping method.

10.7 Government and Contractor Enabling Processes and Products

The transition from the acquisition/development phase to the mission operations and sustainment phases for major systems usually occurs over a relatively long time duration. Some of the elements, segments, or discrete products produced by the contractor will be delivered to and accepted by the government customer ahead of others. A program as a whole could still well be in the development phase, while a large number of products or elements of the system have already been delivered. This is especially true for follow-on systems that are fully or partially replacing or supplementing legacy or earlier generation predecessors. At the top level for DOD Space Systems, national security space (NSS) acquisition policy governs the acquisition process. AFSPCI 10-604, Space Operations Weapon System Management, serves to implement the Acquisition for Major Defense Acquisition Program (MDAP) programs under AFSPC purview. Non-MDAPs in the AFPEO/Space portfolio primarily use SMCI 63-102. Of direct interest for those engaged in MA support during Phase D, AFSPCI 10-604 Sections 2.8.12 and 2.8.13 define the roles and responsibilities for the Material Wing (e.g., SMC POs) and Operating Organization (Wing/Group/Squadron). These organizations need to closely coordinate and

interact with each other to achieve successful operations and sustainment of a system.

10.7.1 Satellite Control Authority and Initial Operational Capability

AFSPCI 10-604 and AFSPCI 10-1204 discuss at some length the processes employed in Phase D to include the process of turn-over and operational acceptance. For a satellite, transfer of SCA serves as the key practical turn-over event and essentially marks the beginning of mission operations at the satellite level. IOC is a higher-level event, and for MDAPs, typically means that multiple satellites, ground control, and user segments have been successfully fielded and are in operation. The declaration of IOC is also particularly important since it can mark a transition in funding.

10.7.2 Sustainment Sources/Depot Source of Repair/Source of Repair Assignment Process

An important and related aspect of sustainment is the determination of the type of source that will be used. Sustainment of systems can be defined as core, which must be performed by one or more government depots. Sustainment can alternatively be designated as contractor logistics support (CLS) in nature. DSOR should be identified for all ground HW and SW elements or subsystems as well as for all space segment SW elements or subsystems. DSOR planning actually is required to be initiated early in the system life cycle, but may not complete until sustainment draws near. Major programmatic changes such as changes in the length of program's life cycle; capability and sustainment modifications; cost or quantities of fielded systems; large increases in labor hours required; etc., can result in a reassessment of previous DSOR decisions. If a DSOR determination is made that sustainment (e.g., of satellite ground control system SW) is core or organic, a transition plan must be defined and implemented that ensures that the knowledge, tools, etc., of the developing contractor are replicated as appropriate at the government depot. For Air Force programs, the DSOR process involves the government program manager (PM) as well as the commander or representative of the appropriate Air Logistics Center (ALC). A major element of the DSOR is the SORAP. The overall goal is to identify the most beneficial source of repair. As AFI 63-101, Acquisition and Sustainment Life Cycle Management, cautions, the SORAP portion of the DSOR should be viewed as a decision point based on multiple factors rather than a competition between an organic government deport and a contractor source. Realities may be more complex as the developing contractor will likely view itself as the best source of repair as well as desire a potentially long-lived revenue stream.

10.7.3 Funding Transition/3600 and 3400 "Color of Money"

The money spent on DOD activities is divided into specific categorizations. In general, money allocated and approved by Congress for one category of DOD activity cannot, without further Congressional approval, be spent on a different category of activity. U.S. Air Force RDT&E funds have a 4-digit code of 3600, while the O&M category is assigned a 4-digit code of 3400. The 3600 "color of money" is the type most commonly encountered by POs supporting Air Force space programs. This color of money is used to pay for the FFRDCs and SETAs supporting Air Force space programs in development. Production is a different category than RDT&E and is the type of funding typically used by the Air Force when a space program is building large numbers of satellites (e.g., GPS). Note also that if an extended-duration transitional period is required before IOC can be declared, the program may enter a relatively short-term phase called interim contract support (ICS). This pseudo-phase still features 3600 color of money and the program is still considered in development. The program is labeled as such since the contractor has delivered some of their products and those must be sustained.

The transition from use of 3600 to 3400 color of money usually occurs right along with the declaration of IOC. A program continuing to build satellites will transition to 3020 money. However, the addition of new or changed capabilities on those production satellites would likely be considered new development and would be funded again on 3600 color of money. The key point is that a large program that has been in existence for several years or longer after CDR may likely have several "colors" of money active at once.

The change in color of money that comes along with the IOC declaration is of direct consequence to POs and supporting engineering staff (Aerospace). Program development is typically 3600. Once a program has declared IOC, the funding transitions to 3400 money for any support to sustainment and normal mission operations. In addition, the customer interface and the specific set of customer offices/individuals change with the transition to post-IOC. POs facing an IOC declaration need to understand the customer interface change and determine the level of 3400 funding planned for MA tasks expected by the customer. Almost certainly, the level of funding will decrease (possibly dramatically) once IOC has been achieved. Additional discussion on the likely reduction in funding or resource is provided in Section 10.7.4. Initial and then detailed dialogue with appropriate customers and higher headquarters charged with post-IOC support should ideally occur well before (i.e., years before) the IOC event. Ideally, users should be part of that dialogue. In particular, the government PO needs to ensure that 3400 color of money for engineering sustainment support is included in program office memorandum (POM) submittals along with all other aspects of support needed for the sustainment/normal operations phase.

The same color of money transition will occur for any development contractor who continues on supporting a program/system post-IOC. In a similar fashion as for the FFRDC/SETA support, the development contractor will be expected to support at a lower level of funding and staff. Decisions on what tools, environments, simulations, etc., that each respectively has built up during development should be made with respect to fully scope resources required in the sustainment phase.

10.7.4 Budget and Resource Constraints

Government funding comes in different colors of money. Phase D3 of the program should include separate budgets for the operations, maintenance, and sustainment functions. The PO (composed of government personnel, FFRDC, and SETA support) post-IOC will almost certainly be at a much reduced funding/engineering heads budget level compared to the development phase. While there is no specific formula governing the amount of reduction, some programs have experienced greater than a ten-fold shrinkage in government PO engineering resources over the life cycle. Figure 10-2 shows the time history for the FFRDC member of technical staff (MTS) budget for a representative long-lived major SMC program. Note that this program continued to experience declines in FFRDC resource budgets until a steady-state level of approximately six MTS was achieved after year L+10 (post-IOC declaration). A rule of thumb of 90 to 95 percent reduction from the peak CDR resource level would be reasonable.

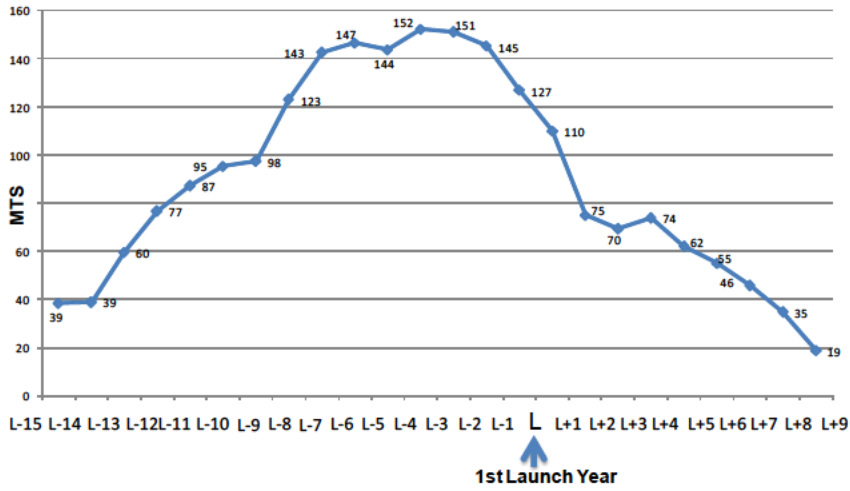


Figure 10-2. Example Reduction in Government PO FFRDC Resources

10.8 Example of Mission Assurance in Operations and Sustainment Phase

Many SMC programs are in the Operations and Sustainment phase of the life cycle. An example of MA in the Operations and Sustainment phase is described here. This program had a long development phase as well as an extended deployment or fielding phase. Today, multiple operational satellites are providing mission area support for the warfighter and various echelons of the government. The satellite mission control ground elements are of course also in the same phase. The development-phase prime contractor provides a substantial amount of the sustainment support, as does the development-phase mission payload subcontractor. Government PO, FFRDC, and SETA resources also continue to support the program from El Segundo as well as at Schriever and Peterson Air Force Bases in Colorado Springs, Colorado.

A simplified work breakdown structure (WBS) for this program in the Operations and Sustainment phase is shown in Table 10-1.

Table 10-1. Simplified WBS

Level 1	Level 2	Level 3
System Sustainment	Space Segment	• PL SW MA • SC SW MA • Fault Mgt System MA • Select HW Box/Subsystem Performance Trending • Select Unit Characterizations • Space Segment Anomaly Resolution and Corrective Action (CA) Support
	Ground Control Segment	• Ground Control SW MA • HW Platform MA • Ground Segment Anomaly Resolution and CA
	System Engineering and Integration Test (SEIT)	• COLA/System Safety • Reposition Analysis, Planning, and Execution Support

Level 1	Level 2	Level 3
		• End-of-Life Planning • Reliability Model, GAP, and Functional Availability Updates • Specs, ICDs, and Requirements Satisfaction Support • Information Assurance Support • User Terminal Support • User and System Level Anomaly Resolution and CA

One key activity is the biannual sustainment releases of payload mission SW. These releases are built and tested by the payload subcontractor and delivered to the prime contractor for preparation and upload to the operational satellites. In general, the releases provide “fixes” to observed discrepancies and diagnosed anomalies. The content of the release, as well as the basic authorization to build and test the release, are all governed by a program-specific version of the requirements satisfaction process shown in Figure 10-1. In some cases, mission payload SW changes are introduced that do not correspond to any observed discrepancy or anomaly. Rather, this second type of change is either diagnostic in nature or represents implementation of a change in requirements. Government resources provide independent MA relative to the adequacy of the SW fixes, testing of the fixes, regression testing, and delta flight qualification testing. The government PO team embedded at the Mission and Satellite Operations Center support the preparation and execution of the uploads. The same basic set of processes occurs on a less frequent basis for the spacecraft bus SW, and ground control SW.

In parallel with the above SW sustainment, satellite HW states of health and performance trending/characterization tasks occur on a periodic basis. In this example, states of health and trending are performed by both the government operating squadron as well as by the contractor staff embedded in the operating squadron facility. FFRDC personnel perform select independent trending as well as responding to anomaly recalls and mission capability restoration. COLA screenings are performed as required. In addition, the trending and characterization serve as an early warning of coming failures. Any realized failures (and “consumption” of redundancy) generate updates in the satellite reliability models. Fuel remaining and other “wear-out” item (e.g., solar array, batteries, mechanisms) projections are also updated yearly as part of this process and serve to define satellite end-of-life truncations in the reliability models. The

reliability model updates are in turn ingested into the GAP program in support of yearly updates in the functional availability report for this particular mission area.

A sample set of MA and verification tasks as described in Sections 10.4 and 10.6 is provided in Table 10-2. A more complete articulation of Operations and Sustainment D3 phase MA and verification tasks is planned for the standard template/baseline of the Aerospace Integrated Mission Assurance Tool (iMAT).

Table 10-2. Sample MA Verification Task Set

MA Tasks	Verification Task	Phase							Description	Source
		0	A	B	C	D1	D2	D3		
Assess requirements satisfaction	Assess operational requirements							X	Perform proactive predictive trend analysis of the readiness of the systems	
Assess requirements satisfaction	Assess risks and potential need for product development							X	Based on a requirements assessment, a risk may be identified that may be validated for product development (i e , hardware fix/buy, software update)	
Assess software updates								X		
Assess hardware updates								X		
Perform reliability model updates								X		
Assess end-of-life								X		
Perform COLA								X		
Assess risk identification, management/ mitigation	Assess potential impacts to the operational systems							X	Ensure contractor and government perform reviews for major program concerns Ensure that	SVSE (TOR-2006(8506)-4494

MA Tasks	Verification Task	Phase							Description	Source
		0	A	B	C	D1	D2	D3		
									independent reviews be considered for anomalies, new design implementations, schedule and performance concerns, etc	

Use of the iMAT is in progress in various SMC Aerospace POs. A key part of iMAT risk assessments are the definitions for risk likelihood and consequence. The iMAT risk definitions are as follows:

Likelihood	**Consequence**
1. Remote	1. No more than negligible loss of margin
2. Unlikely	2. Loss of redundancy or some margin
3. Likely	3. Loss of little used capability or temporary loss of mission
4. High Likely	4. Major loss of mission
5. Near Certainty	5. Complete loss of mission

An early application of the iMAT for the Milstar program is shown in Figure 10-3. MA verification tasks shown are primarily for payload and spacecraft SW sustainment releases. Evaluation points correspond to major reviews or deliveries/product acceptance. Note that as an early application of the iMAT, the risk ratings shown did not benefit from a recent change in the Consequence Level 3 definition of "*or intermittent loss of mission.*" Instead, Consequence Level 4 was determined to be the most appropriate choice. The same assessments done today would see residual risk assessed as "C1" rather than "D1."

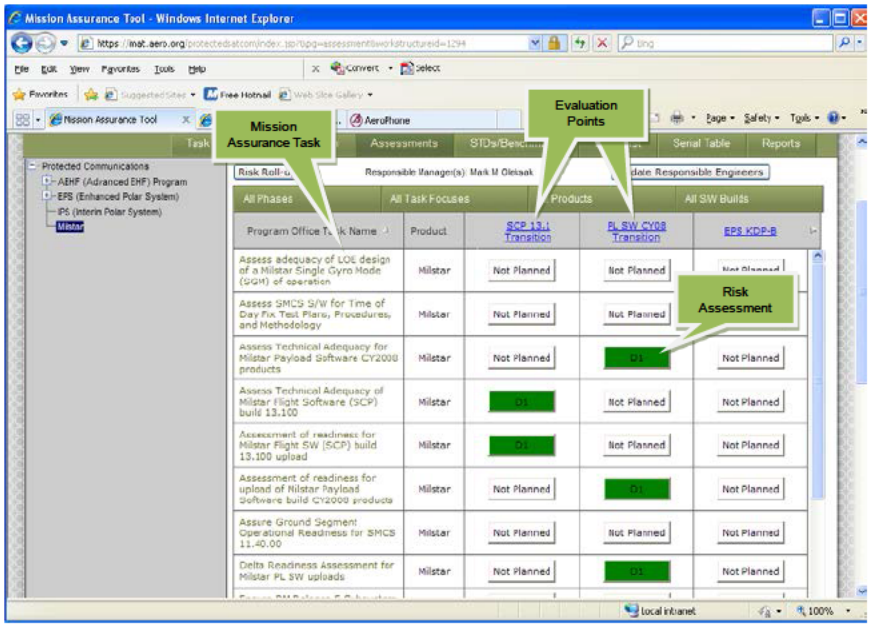


Figure 10-3. Application of iMAT for MA of a Program in Sustainment

The iMAT approach has also been used extensively by EHF Systems Directorate for the Advanced Extremely High Frequency (AEHF) development program. Tutorial materials extracted from the 2010 AEHF SV1 Aerospace President's Review are provided in Figure 10-4. The key point in this chapter is that the iMAT process (as shown) is equally applicable to programs in sustainment as well as in development.[75]

[75] iMAT tutorial provided courtesy of Mr. Andrew Dawdy, The Aerospace Corporation/ MILSATCOM Division, EHF Systems.

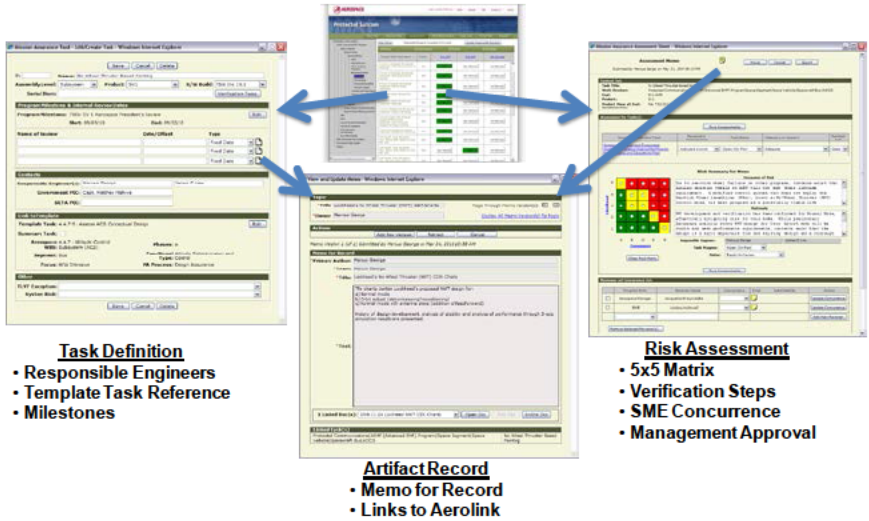


Figure 10-4. iMAT Data Organization

10.9 References

Policy-Related

Key government (Air Force) command media for this phase of the program life cycle are listed below. The following website should be checked for the current versions as these documents are often revised and updated: www.e-publishing.af.mil. Acquirers other than Air Force programs should consult with their acquisition authority for policy, practices, and instructions that guide and dictate relevant requirements for acquisition, development, and sustainment activities.

AFI 63-101	Acquisition and Sustainment Life Cycle Management
AFI 63-131	Modification Program Management
AFI 91-217	Space Safety and Mishap Prevention Program
AFI 63-1201	Life Cycle Systems Engineering
AFSPCI 10-140	Satellite Functional Availability Planning

AFSPCI 63-104	Modifications to Systems and Implementation Approval Process
AFSPCI 10-604	Space Operations Weapon System Management
AFSPCI 10-1204	Satellite Operations
DODI 5000.2	Operation of the Defense Acquisition System, 2 December 2008
SMCI 63-102	Space Acquisition Board Process, 7 September 2006

Handbooks

TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, 31 January 2006

Other

Iannotta, Becky. 2009. “Iridium Incident Highlights Growing Risk of On-Orbit Collisions.” *Space News Business Report.*

Dawdy, Andrew. iMAT tutorial The Aerospace Corporation/MILSATCOM Division, EHF Systems.

Chapter 11
Mission Assurance Reviews and Audits

Dan W. Hanifen
GEOINT Development Office
Andrew Y. Hsu
Acquisition Risk and Reliability, Engineering Department
Jeff B. Juranek
Product and Process Assurance Department
Arthur L. McClellan
Product and Process Assurance Department

11.1 Introduction

The purpose of conducting mission assurance (MA) reviews is to assess the technical maturity within a program, evaluate program risks and opportunities, understand stakeholder expectations, and ensure readiness for the next phase in the overall program life cycle of events and milestones. As part of any rigorous systems engineering (SE) process, technical reviews are conducted at logical points in the program or at key milestones. For most space programs, the review process begins during Mission Assurance Guide (MAG) Phase A—concept/ architecture development, and continues until the system is operational in MAG Phase D. MA reviews are designed to ensure that a series of detailed technical and readiness entrance/exit criteria are met and the program is ready to proceed to the next phase. Figure 11-1 lists the major reviews and audits in the time sequence. As the acquisition program moves through the life cycle, the reviews and audits become more detailed and definitive. SMC-S-021[76] is the source requirement for most technical reviews and audits.

[76]SMC-S-021 (2009) Volume 1 [TOR-2007(8583)-6414 Volume 1, Rev. A].

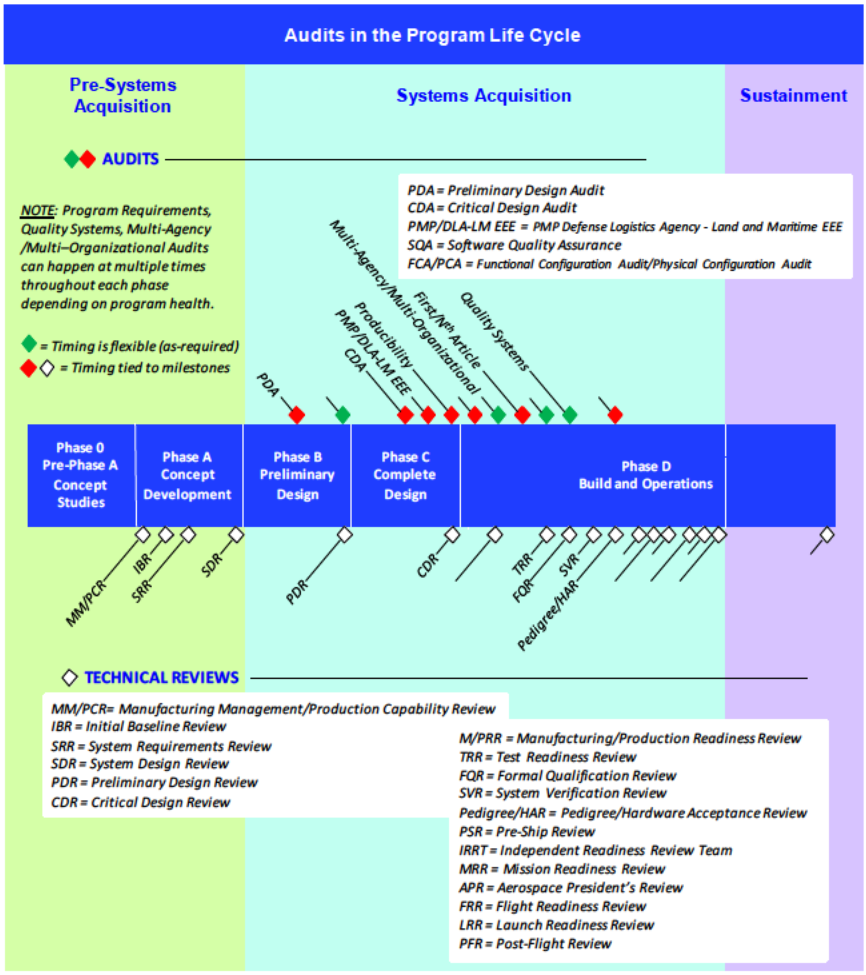


Figure 11-1. Technical Reviews and Audits

The purpose for MA audits is to assess the effectiveness of a contractor's overall internal policies, procedures, processes, organization, and personnel to ensure the product/service will meet contractual requirements and that contractual requirements (including best practice design and manufacturing standards) continue to be consistent with delivering capabilities providing long-term mission success. Audits basically fall into one of three categories: system, process, and product. Within each audit category, the focus is on either compliance or capability. Compliance refers to the ability to meet a set of requirements, standards, or regulations, and is used to measure a contractor's systems or delivered products. Capability refers to the potential to meet a set of

expectations or controls as a measure of both product quality and production capacity. The system audit is the largest in scope and is used to assess the effectiveness of management controls and continuous improvement practices in-place at a contractor. Quality system audits fall into this category, and include programmatic-specific audits; both are compliance focused. Process audits serve to evaluate the capability of a contractor to meet processing standards, methods, or other special requirements. The most common types of process audits are producibility audits and process capability/proofing audits, which review the processes used to produce the product (software quality assurance audits may also fall into this category). The product audit is the most narrowly directed audit, focusing on evaluating a product's "fitness-for-use" or compliance against its specific/unique requirements. Product audits comprise design audits; parts, materials and processes (PMP)/Defense Logistics Agency (DLA) Land and Maritime electronic, electrical, and electromagnetic (EEE) audits; first/Nth article audits; configuration audits (functional configuration audit [FCA]/physical configuration audit [PCA]); pedigree/hardware acceptance reviews; and software quality assurance audits. Each type of audit varies by purpose, scope, depth, and time phasing through the life cycle. Figure 11-2 shows the relative scope and depth of the various audits.

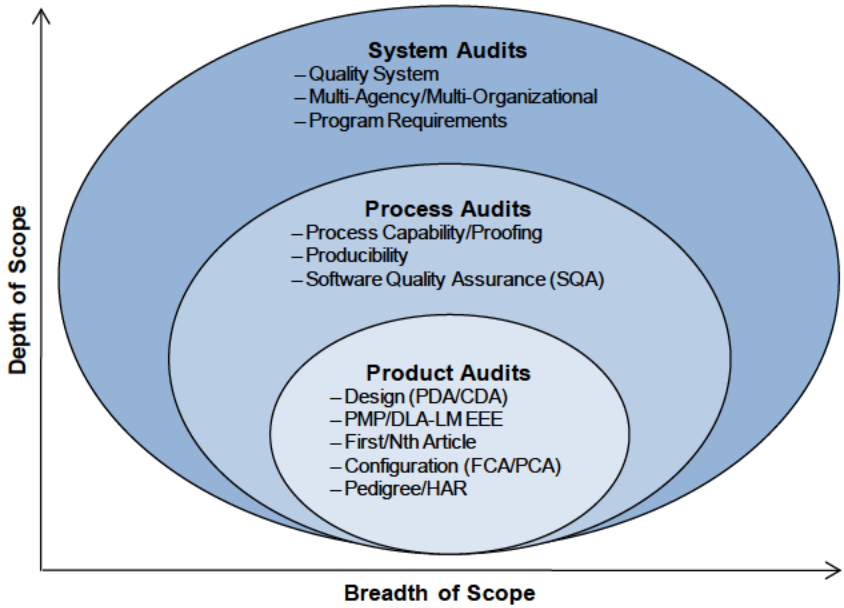


Figure 11-2. Audit Types

Inconsistent application of these reviews and audits has shown to significantly increase a program's susceptibility to mission and programmatic risks.

Therefore, technical reviews and audits are integral pieces to a successful MA campaign and are applicable to all components, assemblies, and systems of the mission's value chain—including lessons learned. As such, reviews and audits are typically conducted as outlined in the contractual statement of work (SOW) and the contract data requirements list (CDRL). Table 11-1 lists the major reviews and audits in the *time order* in which they are typically conducted on space programs (different from Figure 11-2).

NOTE: Table 11-1 shows the various reviews and audits in time order relative to each phase—within each phase the time ordering is fixed for reviews, but for audits the time ordering is flexible and can happen at different times depending on the maturity of the program.

Table 11-1. Reviews and Audits

Review or Audit	Phase	Key References	Secondary References
Manufacturing Management/Production Capability Review (MM/PCR)	A	AFMCP 844	MIL-STD-1528A
Integrated Baseline Review (IBR)	A	Department of Defense (DOD) Program Managers' Guide to the Integrated Baseline Review Process	DOD 5000.2-R
		Secretary of the Air Force/Acquisition (SAF/AQ) Policy 94A-015, September 1994	
Systems Requirements Review (SRR)	A	SMC-S-021 (2009) Volume 1	TOR-2004(3909)-3360
		TOR-2009(8583)-8545	MIL-STD-499B
		SMCI 63-1202	
System Design Review (SDR)	A	SMC-S-021 (2009) Volume 1	TOR-2004(3909)-3360
		TOR-2009(8583)-8545	
		SMCI 63-1202	
Preliminary Design Audit (PDA)	B	TOR-2004(3909)-3360	TOR-2005(8617)-4204
Preliminary Design Review (PDR)	B	SMC-S-021 (2009) Volume 1	TOR-2004(3909)-3360

Review or Audit	Phase	Key References	Secondary References
		TOR-2009(8583)-8545	TOR-2005(8617)-4204
		SMCI 63-1202	
Critical Design Audit (CDA)	C	TOR-2004(3909)-3360	TOR-2005(8617)-4204
PMP/DLA Land and Maritime EEE Audits	C	SMC-S-009 (2009)	
		SMC-S-010 (2008)	
Critical Design Review (CDR)	C	SMC-S-021 (2009) Volume 1	TOR-2004(3909)-3360
		TOR-2009(8583)-8545	TOR-2005(8617)-4204
Process Capability /Proofing Audits	C	MIL-STD-1528A	SAE J1739
Producibility Audit	C	MIL-STD-1528A	
Manufacturing/Production Readiness Review (M/PRR)	D1	SMC-S-021 (2009) Volume 1	MIL-STD-1528A
		TOR-2009(8583)-8545	SMCI 63-1202
First/Nth Article Audits	D1	TOR-2005(8583)-3859	SAE AS9100B
Software Quality Audits	D1	SMC-S-012 (2008)	MIL-STD-498
Quality System Audits	D1	SAE AS9100B	TOR-2005(8583)-3859
Multi-Agency/Multi-Organizational Audits	D1		
Program Requirements Audits	D1		
Test Readiness Review (TRR)	D1	SMC-S-021 (2009) Volume 1	
		SMCI 63-1201	MIL-HDBK-340A
		SMCI 63-1202	MIL-STD-810F
		TOR-2009(8583)-8545	
Formal Qualification Review (FQR)	D1	MIL-STD-1521B	
		SMCI 63-1202	MIL-HDBK-340A
System Verification Review (SVR)	D1	SMC-S-021 (2009) Volume 1	MDA-QS-001-MAP
Functional Configuration Audit (FCA)	D1	SMC-S-002 (2008)	
Physical Configuration Audit (PCA)	D1	SMC-S-002 (2008)	

Review or Audit	Phase	Key References	Secondary References
Pedigree/HAR Reviews	D1	SMCI 63-1203	TOR-2005(8583)-3859
Pre-Ship Review (PSR)	D1	SMC-S-021 (2009) Volume 1	SMCI 63-1204
Independent Readiness Review Team (IRRT)	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	SMCI 63-1203
		SMCI 63-1201	
		SMCI 63-1202	
Post-Flight Review (PFR)	D3	SMCI 63-1204	SMCI 63-1203
		SMCI 63-1201	
		SMCI 63-1202	
		SMC-S-015 (2010)	
		SMC-S-022 (2010)	

11.2 Definitions

A **technical review** is defined as a set of activities led by technical experts 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; to recommend steps to resolve risks/issues affecting mission success; and to approve promoting the hardware, software, and data to the next phase of the program.

An **audit** is an independent examination of a sample of records/artifacts pertaining to a system, process, and/or product by a set of experts from various disciplines against a set criteria, requirements, or controls. For a system audit, it is used to verify compliance with the contractor's internal systems/command media and the ability to produce quality products consistently. For a process audit, it is used to verify that a contractor has the necessary process capability, as well as that the product is producible. For a product audit, it is used to verify

that the functional characteristics and physical attributes comply with relevant specifications, standards, and concept of operations (CONOPS).

A **readiness review** is a formal gate that is used to approve a transition to operational status (flight or mission) to the next program phase. In addition, it requires the government program office and launch/mission operations personnel satisfaction that all requirements that can be verified prior to launch have been (including documentation), and that operations personnel have been trained and certified, and are available to support the launch and operations.

Lessons learned refer to a process for documenting and communicating a series of operational steps that have been proven safe, reliable, and repeatable. Typically, these lessons learned activities are conducted at the end of a milestone or event to ensure knowledge transfer is fresh in the minds of the participants. Part of the lessons learned process entails storytelling and reflecting on "what should have been done differently or what didn't work out well." By documenting this important knowledge it often becomes a "best practice" or standard process.

11.3 Objectives

The objective of technical reviews and audits is ultimately to ensure a product will meet the planned mission objectives and performance requirements throughout the life cycle at predetermined milestones. These reviews/audits provide a guide for the contracting agency/Government to determine whether a prime contractor and subcontractors have attained the necessary technical maturity to move to the next phase of the program with an acceptable amount of managed risk. Additionally, they provide a method for those teams to determine progress to-date, assess predicted or actual performance against the requirements, and realize mitigation plans to avert cost growth and schedule delays to the program.

Technical reviews ensure that:

- The CONOPS is acceptable and meets users' needs
- The requirements are properly defined and allocated to configuration items (CIs)
- The product baseline is established and uses formal configuration management practices to track changes to the baseline, and its requirements can be verified in the projected time
- All internal and external interfaces are clearly defined, complete, and verifiable

- The design(s) is (are) capable of being built in the projected time and satisfies stated requirements
- The product is compliant with all security and environmental health and safety (EH&S) regulations
- Contractor risk assessments are complete and proposed corrective actions adequate and doable
- The contractor's design, risk, cost, schedule, and/or resource information is supportable and achievable
- Test planning supports the "pyramid test philosophy," "test as you fly," and system-level testing and test flows
- The end-item unit-to-unit variation and deviations are acceptable
- The contractor's design and engineering are sufficiently mature and sufficient resources exist to move to the next phase

Audits ensure that:

- The specifications, technical data, engineering drawings, design documentation, quality control records, and manuals adequately describe the product baseline
- The supply-base has properly qualified all parts and materials to meet specified space performance, quality, and reliability requirements
- The tests were adequately defined, scoped, and executed to verify that the test article's performance and interfaces comply with requirements and specifications
- Prior to building flight hardware, the product is producible, and the processes are qualified and do not adversely affect quality and reliability
- The CI as-built version is according to the specifications, physical layouts in drawings, and manufacturing processes and procedures
- A facility has implemented a quality system that is capable of consistently producing quality products

Readiness reviews ensure 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 flightworthy

Lessons learned ensure that:

- Critical knowledge gained from diverse sources is retained and disseminated
- Mistakes are not repeated and "wheels are not reinvented"
- Proper MA policies and practices are established and highlighted

11.4 Practices

Technical reviews and audits are usually outlined in a program's integrated management plan (IMP), integrated master schedule (IMS), and/or a systems engineering management plan (SEMP). The amount of reviews/audits scheduled is a function of the type of program contracted. The type of space program contracted falls into one of four categories: Technology Development (TD), System Development and Demonstration (SDD), Engineering Development (ED), and Risk Reduction and Design Development (RRDD).

The following reviews are generally followed[77] for all space program categories 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.

[77]SMC-S-021 (2009) Volume 1, "Technical Reviews and Audits for Systems, Equipments, and Computer Software," 15 September 2009 and Aerospace TOR-2002(3105)-1668, *Acquisition Strategy Considerations*, 31 March 2002.

11.4.1 Core Activities: Technical Reviews[78]

11.4.1.1 Manufacturing Management/Production Capability Review[79]

The Manufacturing Management/Production Capability Review (MM/PCR) is conducted during source selection by the government PO at the prospective contractors' facilities to evaluate competing contractors' capability to meet all immediate and future production requirements of proposed systems.

11.4.1.2 Integrated Baseline Review

The Integrated Baseline Review (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 milestone 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.

11.4.1.3 System Requirements Review

The System Requirements Review (SRR) determines if the contractor's efforts to understand and translate mission requirements into system requirements and operations concept were 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 generally completed within MAG Phase A (concept exploration) or, at the latest, soon after development contract award (MAG Phase C).

---

[78]SMC-S-021 (2009) Volume 1, "Technical Reviews and Audits for Systems, Equipments and Computer Software," 15 September 2009, 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.

[79]MIL-STD-1528A, "Manufacturing Management Program," 9 September 1986, page 4.

11.4.1.4 System Design Review

The System Design Review (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.

11.4.1.5 Preliminary Design Review

The Preliminary Design Review (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), 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 (assembly level), subsystem, element, and segment building to the system level as appropriate.

11.4.1.6 Critical Design Review

The Critical Design Review (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[80]; 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 the system level, as appropriate.

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

11.4.1.7 Test Readiness Review[81]

The Test Readiness Review (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. The TRR confirms that the products' readiness to start acceptance testing.

11.4.1.8 Formal Qualification Review

The Formal Qualification Review (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.

11.4.1.9 Manufacturing/Production Readiness Review[82]

The Manufacturing/Production Readiness Review (M/PRR) evaluates the contractor and the contractor's design readiness to begin manufacturing.[83] The PRR is conducted by the government program office and supported by the contractor. The M/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 becomes more focused and refined, dealing with production planning, facilities, personnel, allocation, identification, and fabrication of tools/test equipment, long lead acquisitions, and the incorporation of producibility-oriented changes.

[81]TRR as documented in SMC-S-021 (2009) Volume 1 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.

[82]The term production readiness review (PRR) is used interchangeably with manufacturing readiness review (MRR). The acronym MRR is also designated for mission readiness reviews and should not be confused with it.

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

11.4.1.10 System Verification Review[84]

The System Verification Review (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.

11.4.2 Core Activities: Audits[85]

11.4.2.1 Design Audits: Preliminary Design Audit

Preliminary Design Audits (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 space 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.

11.4.2.2 Design Audits: Critical Design Audit

Critical Design Audits (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 space 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

[84]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.
[85]PCA and FCA definitions are found in SMC-S-021 (2009) Volume 1, "Technical Reviews and Audits for Systems, Equipments, and Computer Systems," 15 September 2009, Appendices G and H.

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.

11.4.2.3 PMP/DLA Land and Maritime EEE Audits

Space-level parts form the core of all space programs. The Defense Logistics Agency (DLA) Land and Maritime[86] is responsible for maintaining a known-good supplier base that has successfully demonstrated their products meet the specified performance, quality, and reliability levels via the DOD product qualification program. These suppliers are listed on the qualified product list (QPL), qualified manufacturers list (QML), or qualified product database (QPD) after successfully completing a qualification program and/or conformance audits defined in various military specifications or standards. For EEE parts, printed circuit boards, and laboratories that provide services such as testing and destructive physical analysis, the DLA Land and Maritime audits to determine compliance with the qualification requirements, to verify product performance/quality/reliability, and to assist in interpreting technical specifications and determining manufacturing capabilities.

To verify conformance with requirements for space flight applications, The Aerospace Corporation (Aerospace) and NASA team with DLA Land and Maritime to perform periodic audits. Aerospace and NASA provide various subject matter experts (SMEs) to assist DLA Land and Maritime during the audit and/or qualification program. The SMEs provide detailed knowledge in areas such as qualification of new technology, electrostatic discharge protection, destructive physical analysis, radiation requirements, and manufacturing technology for the specific EEE part, printed circuit boards, etc. being audited to verify the following:

- The product is designed, qualified, and tested (or screened) to the appropriate requirements to prevent premature failures during its intended use
- The materials, processes, and manufacturing methods used to produce the product are adequate to obtain the reliability required for space flight applications

[86]The DLA Land and Maritime was formerly known as the Defense Supply Center Columbus—Sourcing and Qualifications Division.

11.4.2.4 Producibility Audit

The main purpose of a producibility audit is to verify the producibility of the design and fabrication processes to product a high-quality product, as well as check design details for assembly ease and potential failure modes. These audits focus on assessing the in-process difficulties and workmanship of the product right from the start of development. Producibility audits occur on engineering models, development units, “pathfinder” units, and/or qualification units—but before the first flight unit is produced. This typically would occur just prior to the start of environmental testing (for the engineering model/development unit), when the units’ major assemblies can be displayed in convenient segments. The following subject matter is addressed at a producibility audit: (1) visual inspection of the hardware to assess workmanship, clearances, hazards to parts, interconnects, and card installation; (2) review of documentation—including engineering drawings (top assembly and detail), manufacturing work instructions and shop orders, and test procedures—to appraise the effectiveness of controls to produce repeatable hardware; (3) review of discrepancy and failure reports for evidence of trends, poor cause and corrective action, etc.; (4) interview of electronics assemblers/mechanical technicians/inspectors/test personnel to examine difficulties with assembly/inspection/test methods impacting performance; and (5) review manufacturing and test devices such as handling fixtures, special tooling, electrostatic discharge (ESD) protection, storage containers, test fixtures/adapters/break-out boxes (BOB), and general working conditions that could impact effect overall effectiveness. The value of a second pair of eyes finding a potential failure, or recommending possible improvements to procedures/ease-of-assembly, or implementing a necessary change to enhance reliability and/or ensure program requirements are met—pays dividends many times over.

11.4.2.5 Process Capability/Proofing Audits

Before flight hardware is manufactured, all processes and equipment are qualified to ensure that they: (1) meet specifications; (2) are repeatable and reproducible; (3) do not affect the reliability of the hardware; and (4) do not cause damage to the hardware. A process capability/proofing audit is used to verify that inherent quality and reliability are maintained when designs are transformed into flight hardware during the manufacturing and testing phases. If adverse findings are made, the processes/equipment used in manufacturing and testing are changed to eliminate them. One technique that is used in a process capability/process proofing audit is a process/equipment failure modes and effects analysis (FMEA). This technique, which is similar to a design FMEA used on the prime hardware, is applied to the manufacturing and test processes/equipment and does the following:

- Identifies potential product/process interface-related failures (e.g., electrical overstress to flight hardware from test equipment)
- Identifies potential manufacturing/assembly failures
- Identifies process variables that require specific process controls
- Develops a ranked list of potential failure modes and preventive/corrective action considerations

The process/equipment FMEA is conducted before an M/PRR and TRR to ensure the safety of the built and tested flight hardware, and is updated any time there is new processes/equipment resulting in a change to a qualified production line. Test equipment is also proofed and demonstrated by analysis or test that the test equipment/software perform as designed and do not have the potential to damage the flight hardware. Once the test equipment has been proofed, it is sealed with break-of-inspection seals/stickers to let personnel know that the test equipment has been set up and qualified, and is not to be tampered with (which could invalidate it).

11.4.2.6 First/Nth Article Audits

The primary purpose of the first article audit is to evaluate the success of the design implementation and manufacturing. The first article audit occurs on the first qualification unit or flight unit after M/PRR. The qualification unit should be fabricated to flight specifications and generally precedes any flight unit. The first article audit is also known more commonly as a first article inspection (FAI), and is an in-depth physical and functional inspection process to verify that the prescribed production methods have produced an acceptable item as specified by the engineering drawings, engineering specifications, build work instructions/planning/test procedures, purchase order, and any other applicable design documentation. Typically, a multi-disciplinary team consisting of quality assurance personnel, cognizant engineering personnel, manufacturing/operations personnel, and PMP personnel is responsible for reviewing the following activities as part of a first article inspection:

- Verifying that all analyses /inspections/tests/demonstrations were completed and all functional requirements were met
- Verifying that each item is within proper dimensional tolerances and identified/marked properly as specified on the drawings
- Assessing that the item is compliant with workmanship requirements and no hardware safety issues exist with respect to defects/failures/change history

- Verifying that parts and materials were approved and all screening/specification requirements were met
- Verifying that manufacturing processes/procedures (including test) are acceptable, approved, and released
- Ensuring that supplier-built hardware meets all form, fit, and function requirements at that next higher integration level, and the supplier certificate of conformance/compliance (CoC) paperwork is present
- Verifying that packaging and handling is sufficient to protect the hardware during shipment
- Verifying that the Quality purchase order attachments /provisions guidelines were met

Similar to a first article audit, the N^{th} article audit occurs after the initial hardware build has been qualified and has continued to be built on the same production line for an extended period of time. As such, many programs, because of product complexity, can extend out for several years in the making. The intent of the N^{th} article audit is to ensure the products are still being built to the same specifications and rigor, and that the overall processes/personnel have not changed to a significant degree and without the proper reviews/approvals. The same content is typically covered in N^{th} article audit as in the first article audit however the timing is different. This type of audit is usually conducted on several random items of a qualified hardware line. Yield issues and repeat discrepancies are reviewed carefully in the N^{th} article audit.

11.4.2.7 Software Quality Assurance Audits

Software development, like many complex hardware development activities, is a process full of risks. The risks are both technical and programmatic—that is, risks that the software will not perform as intended or will be too difficult to operate, modify, or maintain. The goal of software quality assurance (SQA) is to reduce these risks. For example, coding standards are set to specify a minimum quality of code. If no standards are set, there exists some risk that the code will not come up to a usable minimum standard and will require rework. If standards are set but there is no explicit process for ensuring that all code meets the standards, then there is some risk that the coders will produce code that does not meet the standards. Similarly, the lack of a proper nonconformance reporting and corrective action system increases the risk that problems in the software will be forgotten and not corrected, or that important problems will not get priority attention. In addition, the relationship of criticality to assurance is as one would expect—the more critical the software, the more important and formal the software quality assurance effort must be. The projected size of the software to be produced also influences the level of assurance required. A large project

requires explicit and detailed standards for all of the products in order to get at least a minimum standard of quality from the varied ideas and experience of many programmers. In short, just due to the size of the activity, a significant and formal software quality assurance program must be established or risks of poor quality must be accepted. Therefore, to have no SQA strategy that involves auditing is to increase the risk that unacceptable code will be produced.

Software quality assurance is a technique that is used to examine the conformance of a development process to procedures, and the conformance of products to standards. An SQA audit can examine the conformance of the actual status of the development activity to the reported status. Status auditing is most effective if there are objective and consistent criteria for evaluating the level of product completeness. The actual processes and products examined by an audit can vary—a general audit provides a comprehensive overview, while a limited audit might be an examination of certain procedures (e.g., “Are coding standards being followed?”). All projects generate code and documentation, but if there are no written standards, the products will be in the style of the individual technical performers or their managers. The role of SQA is to discover and document the “standards” and “procedures” that are actually followed.

Documentation standards specify the form and content for planning, control, and product documentation—providing consistency throughout a project. *Design standards* specify the form and content of the design product and provide the rules/methods for translating the software requirements into the software design and for representing it in the design documentation. *Code standards* specify the language in which the code is to be written and define any restrictions of use of language features. They define legal language structures, style conventions, rules for data structures and interfaces, and internal code documentation.

11.4.2.8 Quality System Audits

When a quality system (QS) audit is conducted, the focus is on the overall quality system, which is the result of the management-directed activities and processes used to build the product. Quality system audits are usually the broadest and most extensive of audits, and are performed to verify, through objective evidence (facts and data), whether or not the quality management system and the underlying organizational processes are executed adequately and effectively. The interacting quality structure of the organization as a whole is examined as is the effect of the systems in-place on the product. Quality system audits may be *external* to the organization building the product (typically conducted by the prime contractor or a third-party registrar), or may be *internal* (conducted in-house, usually by the quality assurance [QA] function).

The QA organization at a prime contractor or a subcontractor typically performs a series of quality systems audits to assess the effectiveness and compliance to the applied requirements. These quality systems audits are conducted in all areas where program work is conducted—internally on the program, at key subcontractors, and at critical subtier suppliers (e.g., those producers that can have a significant effect on end-item quality/reliability). Audits for general industry are based on the ISO 9001 standard, while aerospace hardware is based-on the SAE AS9100 standard—facilitating development of a single quality system and enabling customers to have a common basis for understanding the results of audits. The quality management system requirements specified in this standard are complementary to the organization's own requirements, as well as to regulatory and special customer requirements. Quality system audits cover the following general topics:

- Quality management systems
- Management responsibility
- Resource management
- Product realization
- Measurement, analysis, and improvement

In addition to the AS9100 quality standard, Aerospace has developed another quality requirements document (SMC-S-003, "Quality Assurance Requirements for Space and Launch Vehicles") which is even more rigorous and focused specifically on the unique requirements demanded by space hardware. Since acquisition reform ended, many space programs interested in instituting reinvigorated quality requirements have utilized the SMC-S-003 (TOR-2005(8583)-3859) standard. SMC-S-003 contains very specific and detailed quality requirements/processes, above and beyond AS9100—ranging from the independence of the quality organization to the inclusion of required pedigree/hardware acceptance reviews (HAR) to the required customer decision authority (voting authority) on material review boards (MRB)/failure review boards (FRB)/corrective action boards (CAB).

Quality system audits should be planned taking into consideration the requirements/processes and areas to be audited. The frequency of the audits is based on the importance of criteria derived from one of the following sources:

- Provisions identified in the SOW, quality plan, or other contractual documentation
- The analysis of previous audit results
- The attributes and criticality of the products

- Items that require special attention because of complexity, application of state-of-the-art techniques, impact of potential failure, limited operating life, or the anticipation of reliability problems
- Products going through development due to obsolescence or new designs

The audit criteria, scope, frequency, and methods are defined prior to conducting any of these audits.

11.2.4.9 Multi-Agency/Multi-Organizational Audits

Although the concept of performing multi-agency/multi-organizational audits has been around for a long time, only recently have various government agencies/companies begun to utilize this approach. In particular, NASA has utilized multi-agency/multi-organizational (or Joint) audits across multiple programs to eliminate each division coming in to audit each and every program. With the establishment of an agency-wide Joint Audit Planning Committee (JAPC), this committee coordinates the planning, scheduling, monitoring, and management of supplier audit activity. The JAPC focuses on coordinating audit activities between NASA and the prime contractors of subtier suppliers. The JAPC goals include:

- Eliminating duplicative audits and reducing supplier costs and work interruptions related to customer audits
- Enhancing the capability to identify supplier risks and tailor quality assurance actions
- Reporting agency-wide quality metrics and trends
- Standardizing supplier auditing practices
- Sharing best practices and lessons learned
- Reducing committee companies' costs by combining auditing resources

Within NASA, the NASA Audit Management Team (NAMT) coordinates activities among centers auditing prime contractors, with other government agencies, and within the industry sector in order to reduce unnecessary duplication of limited resources while improving viability into available data. Both committees utilize the NASA supplier assessment system (SAS) as a database that focuses on providing information about supplier utilization, certification status, and status of assessment activities. Because NASA has adopted the AS9100 standard for quality systems, this has enabled them to share information across the agency as they face the challenge of ensuring quality and integrating products from all over the country and at all levels within the supply chain.

Some of the prime contractors also have been experimenting with coordinating their audit activities across their space programs. On a case-by-case basis prime contractors have looked across space programs that contain requirements for similar type hardware (e.g., unit electronics, part commodities, etc.), and where the number of suppliers is limited. Because the aerospace supply base is shrinking this presents unique challenges to space programs going forward. Also, from a supplier perspective, at some point it may not make sense to conduct system-wide audits every time the same prime contractor (for multiple programs) buys another unit on the same qualified production line. However, this does not mean that program- or project-specific requirements or needs, quality issues at a facility, schedule concerns, and new technology introduction can be overlooked in the product life cycle.

11.2.4.10 Program Requirements Audits

The program requirements audit is similar to a system audit in that it is focused on verifying the compliance of the systems in-place that govern the program. Typically, the program requirements audit is a smaller subset of the larger-scoped system audit. While the quality systems audit is looking to see if the systems in an organization are compliant with the internal command media (directive documents)—the program requirements audit is looking to see if the program is compliant to contractual requirements and/or specific program directives (program command media). Overall, the program requirements audit is useful to explore items that are of high risk and/or for exploring important issues relevant to the program.

Depending on the phase of the program, one common use for the program requirements audit is to investigate the proper flowdown of contractual requirements. This is useful during the requirements and design phases to ensure that all requirements from the contractual documents and/or requirements database tools are flowed down into the corresponding specifications/plans/drawings/purchase orders. For example, a program requirements audit might consist of reviewing various program requirements documents to ensure system verification plans are linked to test plans and below that to test procedures (for backward and forward traceability down to its lowest level) in order to avoid hardware overstress. Another variation of the program requirements audit might focus on the program review process used for proper development of test procedures and their checkout—identifying the number of peer reviews and table-top reviews, as well as the required functional organization inputs required, before release into the configuration management (CM) system. The program requirements audit is highly flexible in the range of topics it can cover, and is part of a planned forward-looking process focused on prevention, versus a reactive backward-looking result.

11.2.4.11 Configuration Audits: Functional Configuration Audit

The functional configuration audit (FCA) is a formal audit to demonstrate that the hardware and/or software CIs have achieved their functional and performance requirements, as outlined in their development/product specifications using the designated verification methods. This audit examines the CONOPS, design review action items, verification and test plans, analysis and inspection reports, as-used qualification test procedures, acceptance test procedures, test data, test FRB actions, drawings, verification compliance requirements matrix (VCRM), and other supporting documentation. An FCA is conducted on either the first production unit or a preproduction representative of the configuration to be released as an operational production unit. The final FCA occurs at the completion of CI qualification testing. Typically the FCA is supported by the prime contractor and subcontractors for lower-level CIs, while the customer would support the system-level CI.

11.2.4.12 Configuration Audits: Physical Configuration Audit

The physical configuration audit (PCA) is a formal audit to verify that each CI "as-built" configuration conforms to the physical and design requirements defining the CI—represented by the product baseline. The PCA confirms that no variations exist between the "as-designed" configuration and the "as-built" configuration. Customer formal acceptance of product specification and successful completion of the PCA results ensure that any variations do not pose unacceptable risk to mission success. A complete PCA is conducted on the first production unit and is not repeated unless significant engineering changes and resulting modifications to the CI have occurred. The PCA includes a detailed examination of engineering drawings, process specifications, manufacturing documentation (work instructions), MRB actions, technical data/test data, and all operational support documentation (e.g., user manuals, diagnostic manuals, and firmware support manuals). The PCA is conducted jointly with the FCA as a combined audit.

11.2.4.13 Pedigree/Hardware Acceptance Reviews

Pedigree/hardware acceptance reviews (HARs) 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, MRB and FRB actions, environmental exposure, operating

time or number of cycles, resolution of any unverified failures, out-of-family test results, 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 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 that documented procedures and processes were followed, any out-of-sequence work maintained the product's integrity, engineering changes were proper, and deviations and "use as is" MRB decisions were adequately justified. Pedigrees ensure new processes, materials, and design changes do 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.

11.4.3 Core Activities: 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 milestones 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.

11.4.3.1 Independent Readiness Review Team

Independent readiness review teams (IRRTs) 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 can be done incrementally with the final review occurring before launch. As such, the extent of each review is negotiable depending on the hardware (HW)/software (SW) design and development stage of the program, HW/SW performance history, and resources available for the review, changes since the last review, and scope of the last review. The scheduling of final IRRT activity should provide sufficient time for a complete review and for any corrective actions to take place and critical recommendations to be implemented.

11.4.3.2 Mission Readiness Review[87]

The Mission Readiness Review (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 HW (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”).

11.4.3.3 Aerospace President’s Review

In support of the SMC commander’s FRR (section 11.4.3.5), the Aerospace president conducts an 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. The space vehicle Aerospace President’s Review (APR) is held prior to shipment to the launch site, and a status update is provided at the launch APR, which occurs 2 to 3 days prior to the flight readiness review. Aerospace corporate vice presidents of the appropriate Space Launch Operations, Space Program Operations or National Systems Group, or Engineering and Technology Group support the president’s review. In accordance with SMCI 63-1201, the Aerospace president’s review

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

findings are presented to the SMC commander during the FRR and the Aerospace president participates in the readiness poll.

11.4.3.4 Pre-Ship Review

The program conducts a HW pre-ship review (PSR) to ensure 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 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 ensure the latter is ready to receive program HW, receiving support has been appropriately scheduled, and receiving facilities are prepared to support HW arrival and post-shipping inspection activities.

11.4.3.5 Flight Readiness Review[88]

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 of the FRR is to ensure the prime contractor, Aerospace, the spacecraft program office, launch programs, and the SMC commander agree that the launch vehicle is flightworthy 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.

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

11.4.3.6 Launch Readiness Review

A Launch Readiness Review (LRR) is an operations readiness review organized by the government Launch Decision Authority (e.g., 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.

11.4.3.7 Post-Flight Review

A Post-Flight Review (PFR) is conducted for all missions requiring an MRR and the results are presented to the government SM 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. PFRs are held approximately 60 days after launch and early on-orbit testing is completed.

11.4.4 Core Activities: Lessons Learned Process

Aerospace has participated in a wide range of government and commercial space systems for close to 50 years. Drawing on its broad expertise, and following a period of expensive failures after acquisition reform, the U.S. government tasked the Air Force Space Command (AFSPC) to convene a launch vehicle broad area review (BAR) in 1999. The BAR representatives were tasked with the creation of a formal process to capture and disseminate lessons learned among programs and contractors to avoid the repetition of mishaps. In response to the BAR and SMC tasking, a formal system to facilitate lesson learning and sharing across the enterprise was developed and is outlined in Figure 11-3.

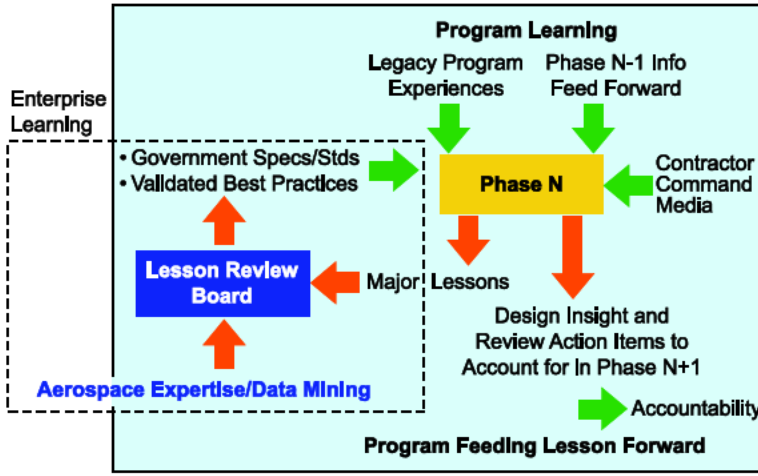


Figure 11-3. A Closed-Loop Learning Process

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). The goal of incorporating lessons learned is to reduce the risk and improve mission success. Sharing lessons from prior programs, to identify, communicate, and record good practices and adverse experiences with implications broader than localized corrective actions, is an important MA mechanism that benefits future programs, especially in the prevention of recurrence of mission-limiting failures. Relevant experiences can be drawn both vertically and horizontally; at each stage of the program, the PO can extract experiences from legacy programs and earlier phases of the current program, as well as applying cross-program wisdom to improve the outcome, thus reducing risk. Lessons learned captures the risks and consequences of flawed technical and management practices and processes, and the benefits of refinements to current practices and processes. The process by which Aerospace captures lessons learned is sustainable only if all programs diligently collect, assess, document, and infuse pertinent lessons at every phase.

Evolving from the initial investigation on launch vehicles, Aerospace has issued a series of lessons learned from on-orbit and in-factory histories that, together with NASA, can be made available to PO and engineering personnel who are supporting any potentially affected program activities.[89] The scope of these lessons covers design, systems engineering, specialty engineering (such as PMP), software acquisition, manufacturing, integration, test, and operations. Aerospace has prepared numerous Lessons Learned volumes that, together with numerous validated lessons from other sources such as NASA, can be made

[89] TOR-2008(8617)-1, "Space Systems Engineering Lessons Learned," Volume Twenty-One (31 March 2008) of the Aerospace Lessons Learned documentation.

available to program office and engineering personnel who are supporting any potentially affected program activities. Aerospace's "Lessons Learned" database continues to capture key lessons that will enhance how future programs are acquired and managed.

11.4.5 Standards/Recommended Practices

Technical reviews and audits demonstrate that the required accomplishments have been successfully completed before proceeding beyond critical events and key project milestones, as well as are compliant with established systems-in-place. Major technical reviews occur at key events identified in program plans upon completion of all the accomplishments associated with the event, as measured by their acceptance criteria or exit criteria. It is recommended that at the time of the request for proposal (RFP) the customer/contractor includes SMC-S-021 (2009) Volume 1 [TOR-2007(8583)-6414, Volume 1, Rev. A] and formalizes it as a contract data requirements list (CDRL) item. For audits, most contractors have corporate command media and/or program plans that describe their audit processes and can be found in QA manuals/plans, CM manuals/plans, design standards, PMP plans, hardware plans, software development plans, SQA, etc.

11.5 Key Lessons Learned

To a large extent, the system engineering processes—and, in general, the mission assurance (MA) processes—were created and have evolved to bring discipline to the business of producing very complex systems. It is intended to ensure that requirements are carefully analyzed, and that they flow down to detailed designs. The process demands that the details are understood and managed. The problem is that in too many cases a program is not mature enough to proceed to the next level, and ends up taking on inherently too much risk. Technical reviews and audits can serve to:

- Provide a means to improve vertical and horizontal communication between diverse groups of engineering disciplines and managers
- Provide a rigorous means to collect, organize, and review cost/schedule/engineering information to ensure proper engineering maturity exists and risks are understood/managed before moving to the next phase
- Provide a process to synchronize the engineering and manufacturing efforts of complex multi-disciplinary geographically separated contractor and government teams

If the design and development are managed in a way that takes advantage of the expertise resident within both the government and the contractors, this could translate into the government stating its needs in terms of performance outcomes desired rather than in terms of specific design solutions required; likewise, having contractors select detailed design approaches that deliver the performance demanded, and then taking responsibility for the performance actually achieved. However, various case studies have shown that when the government stepped back from a less directive role in design and development, the contractors did not take on the government's role and ignored important system engineering and MA elements. The problem seems to have been a lack of communication of expectations between the government and the contractor, and while tailoring of systems engineering elements specific to the program, there is great risk in ignoring key elements of the process. Before a program decides to skip phases, eliminate reviews, or reduce audits to save schedule/ costs, they must ensure those decisions are appropriate for the level of risk inherent to the program.

MA technical reviews and audits 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 synchronize the government and contractor expectations. The reviews and audits permit the MA experts to work in concert with program development resources and within the program's chain of command to fulfill their roles.

11.6 Task Execution by Phase

MA reviews and audits are organized by phases according to program planning and systems engineering tasks. Several objectives are accomplished by performing the needed reviews and audits for a typical space program:

- In Phase 0, the tasks ensure 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 RFP, SOW, CDRL, data item descriptions (DIDs), etc., to prospective contractors. This is critical to ensure MA has the necessary information to assess risks to mission success.
- In Phase A, the tasks ensure 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. MA ensures the MA requirements are part of the baseline and tailoring has been done prudently according to program constraints. MA also ensures there is a visible risk

management process that includes mitigation plans to reduce long-term mission risks.

- In Phase B, the tasks ensure the requirements have been properly flowed down to all levels of the WBS and they will be met by the design by verification during the PDAs and design reviews. Entrance gates for future major reviews are established to prevent reviews if the contractor is ill-prepared. MA ensures MA requirements were adequately flowed down to all levels of the WBS and contractors and suppliers are accommodating those requirements in their baselines.
- Phase C reviews share the same objectives as in Phase B, but at a more detailed level. CDAs, the system design, manufacturing readiness, incremental space-flight worthiness reviews, and the CDR work to ensure the design will meet requirements. MA ensures the MA requirements were adequately flowed down to all levels of the WBS and contractors and suppliers are accommodating those requirements in their baselines.
- In Phase D1, the tasks ensure the HW is fabricated as designed, testing is properly planned and executed, and the HW actually performs as intended under testing. Major objectives that must be met are included in TRRs, FQRs, M/PRRs, and FCA/PCAs. MA ensures the HW is tested according to prescribed MA standards, retest is done correctly after test anomalies are corrected, and lifetime limits on hardware are observed.
- In Phase D2, the tasks ensure 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.
- In Phase D3, the tasks provide an assessment of ground segment and flight SW contract changes, block upgrades, and operational patches. At end-of-life, the mission payload and vehicle health are reviewed for disposal considerations to reduce potential frequency interference and spacecraft collisions.

11.7 Government and Contractor Enabling Processes and Products

Key government and contractor enabling products are summarized as follows for each phase in Table 11-2.

Table 11-2. Key MA Reviews and Audits

Phase	Government Enabling Products	Contractor Enabling Products
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 PMP/DLA Land and Maritime EEE Audits	Completion of CDRs Completion of CDAs Completion of PMP/DLA Land and Maritime EEE Audits Completion of Producibility and First/Nth Article Audits
Phase D1	Completion of Phase D1 Technical Reviews (e.g., TRR, FQR, M/PRR) Completion of Phase D1 technical audits (e.g., FCA/PCA) IRRT assessments Completion of Pedigree/HARs	Completion of Phase D1 technical reviews Completion of Phase D1 technical audits Completion of Quality System Audits (includes Program Requirements and Multi-agency/Multi-organizational Audits) Completion of SQA Audits Completion of Pedigree/HARs
Phase D2	Completion of technical reviews (e.g., SVR, MRR, LRR, FRR, PSR, IRRT assessments)	Completion of technical reviews and audits

11.8 Practice Review and Audit Application Example

When developing a review and audit strategy for a PO, the initial step is to look at what phase the program is in and where the respective WBS elements are managed from. The WBS defines the organizational structure of the program, as well as the elements that comprise the system, and the tasks to be performed

within each element. Once this is done, the PO can decide which tasks are needed, using the reference set of tasks identified in Table 11-3 as a baseline. Although the table suggests some of the most important tasks, ultimately the PO may want to utilize a cross-functional team with different expertise to develop a more comprehensive list of tasks appropriate to the type or size of the program. Additionally, prior lessons learned should be reviewed for new programs/ follow-on efforts with similar scope, to minimize overall risk and aid in assessing how mature the program is at each phase.

Table 11-3. Reference Set of Technical Review and Audit Tasks

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Contractual Implementation of Review and Audit Requirements							
Assess negotiated contract review and audit requirements sections for completeness in regards to RFP, SOW, CDRLs, DIDs, WBS, etc.	X	X					
Assess Review and Audit Program Plans and Processes							
Assess SEMP, MA Plan, Risk Management Plan, Quality Assurance Plan, Software Development Plan, and internal command media policies and procedures for adequacy and completeness	X	X					
Assess Program Review and Audit Implementation							
Assess review and audit flowdown of requirements to subcontractors		X	X	X	X		
Evaluate the effectiveness of review and audit processes		X	X	X	X	X	

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure Review and Audit Control Activities							
Verify compliance with internal command media policies and procedures			X	X	X	X	X
Verify compliance with internal/independent review and audit processes for maturity			X	X	X	X	X
Verify compliance with SEMP, MA Plan, Risk Management Plan, Quality Assurance Plan, Software Development Plan and other Program Plans			X	X	X	X	X
Audit Review and Audit Process							
Assess review and audit process and lessons learned	X	X	X	X	X	X	X

11.9 References

Policy-Related

DOD Directive 5000.2-R	Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs, 5 April 2002
SAF/AQ Policy 94A-015	September 1994
SMCI 63-1201	Assurance of Operational Safety, Suitability, and Effectiveness for Space and Missile Systems, 21 May 2001
SMCI 63-1202	Space Flight Worthiness, 1 April 2004

SMCI 63-1203	Independent Readiness Review Team, 16 January 2004
SMCI 63-1204	SMC Readiness Review Process, 1 August 2002

Specifications and Standards

MIL-STD-810F	Test Method Standard for Environmental Engineering Considerations and Laboratory Tests, 14 July 1989
MIL-STD-1521B	Technical Reviews and Audits for Systems, Equipments, and Computer Software, 4 June 1985
MIL-STD-1528A	Manufacturing Management Program, 9 September 1986
SAE AS9100B	Quality Management Systems—Aerospace Systems, January 2004
TOR-2006(8583)-1 [also published as SMC-S-002 (2008)]	Configuration Management, 13 June 2008
TOR-2005(8583)-3859 [also published as SMC-S-003 (2008)]	Quality Assurance Requirements for Space and Launch Vehicles, 13 June 2008
TOR-2006(8583)-5235 [also published as SMC-S-009 (2009)]	Parts, Materials and Processes Control Program for Space and Launch Vehicles, 12 January 2009
TOR-2006(8583)-5236 [also published as SMC-S-010 (2008)]	Parts, Materials and Processes Technical Requirements for Space and Launch Vehicles, 13 June 2008
TOR-2004(3909)-3537, Rev B [also published as SMC-S-012 (2008)]	Software Development for Space Systems, 13 June 2008

TOR-2006(8583)-4474 [also published as SMC-S-015 (2010)]	End-of-Life Disposal of Satellites in Geosynchronous Altitude, 19 March 2010
TOR-2007(8583)-6414 Volume 1, Rev A [also published as SMC-S-021 (2009) Volume 1]	Technical Reviews and Audits for Systems, Equipments, and Computer Software, 15 September 2009
TOR-2007(8506)-7164 [also published as SMC-S-022 (2010)]	End-of-Life Disposal of Satellites in Low-Earth Orbit, 19 March 2010

Handbooks

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

MDA-QS-001-MAP	Missile Defense Agency Mission Assurance Provisions (MAP), 2 February 2004
MIL-HDBK-340A	Test Requirements for Launch, Upper Stage, and Space Vehicles, 1 July 1985

Best Practices

MIL-STD-499B	Systems Engineering, draft dated 6 May 1994
SAE-J1739	Potential Failure Mode and Effects Analysis in Design, Manufacturing and Assembly Processes, and Machinery, August 2008
TOR-2002(3105)-1668	Acquisition Strategy Consideration, 31 March 2003
TOR-2004(3909)-3360 Rev. 1	Systems Engineer's Major Reviews for National Security Space System Programs, 2 February 2005
TOR-2004(8617)-4204	100 Questions for Technical Review, 30 September 2005

TOR-2009(8583)-8545	Guidelines for Space Systems Critical Gated Events, 9 May 2008
TOR-2008(8617)-1	Space Systems Engineering Lessons Learned – Volume Twenty-One, 31 March 2008

Other

Critical Process Assessment Tool (CPAT)	14 August 1998
Proceedings of the First International Forum on Integrated System Health Engineering and Management in Aerospace	"From Data Collection to Lessons Learned—Space Failure Information Exploitation at The Aerospace Corporation," November 7–10, 2005, Napa, California, and references cited therein.

Chapter 12
Risk Management

Sergio B. Guarro
Systems Engineering Division
Andrew Y. Hsu
Acquisition Risk and Reliability Engineering Department

12.1 Introduction

Risk management (RM) is a structured process that has as its objective the identification and evaluation of risk throughout 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 (MS) to all decisionmakers and program stakeholders at all levels.

12.2 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.

12.3 Objectives

RM provides assurance that program and system risks have been thoroughly analyzed and impacts identified and allocated to lower-tier subsystems, components, interfaces, etc., 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, and Effectiveness for Space and Missile Systems) states that it is a part of the program 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 MA actions are necessary with respect to any identified risk issues
- Selection and execution of MA interventions that balance the scale of risk reduction with its cost 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.

12.4 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 (PM) or director, that 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 and by the Department of Defense (DOD) Risk Management Guide (see also Section 12.6).

Many applications of RM are relatively unstructured and qualitative. However, several formal technical tools can be used to support key RM 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 Sections 12.4.1 through 12.4.5. An overview of the PRA framework as an integrated risk assessment tool is given in Section 12.4.4. The reader can find more detailed technical discussion of the techniques introduced below listed as reference documents in Section 12.10.

12.4.1 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 from which risks may originate—which in the case at hand are risk initiators (initiating conditions or events)—and impact areas (the program assets that would be affected by the occurrence of the risk). MLD risk models are used to ensure the organization of risk sources (or risk-initiators) 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 Section 12.4.4.

12.4.2 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 12.4.4). 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.

12.4.3 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 MS or safety performance (e.g., in consideration of potentially defective parts and their impact on the launch success probability for a launch vehicle (LV) 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 in Section 12.4.2.

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 for special modeling needs. For example, influence diagrams and Bayesian belief networks are well suited to model situations involving multiple influences and conditional probabilities.

12.4.4 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 (FTA) 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 in Section 12.4.4 do apply.

12.4.5 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 implementing that design modification. Any combination of the risk-reduction models discussed in Sections 12.4.3 through 12.4.5 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, considering the risk-reduction worth vs. cost for each of these permits the identification of a mission-optimal or program-optimal risk-reduction solution. It is then also possible to choose a set of such design improvements, given an amount of resources available for risk reduction, that provides the greatest possible risk reduction, i.e., the greatest possible MS/MA benefit.

12.5 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 (Aerospace).

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 should 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 pre-Phase A, 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”:

1. Risk planning
2. Risk assessment
3. Risk handling
4. Risk monitoring

12.6 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 Section 12.5, as further explained in Sections 12.6.1 through 12.6.6.

12.6.1 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 Federally Funded Research and Development Center (FFRDC)/systems engineering and technical assistance (SETA) support as well as by the prime contractor(s) and major subcontractors. Accordingly, the MA task database includes groups of tasks aimed at directly supporting 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).

12.6.2 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 each identified risk, the likelihood that the risk will occur, and the severity of the consequences to the program should it occur.

Similar 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.

12.6.3 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 handling plans that implement the selected options

In accordance with the above, the MA task database includes groups of tasks that are in support of government activities in the 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.

12.6.4 Risk Monitoring and Updating Tasks

In addition to the basic risk planning, assessment, and handling-related activities addressed in Section 12.6.3, 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. Tasks involving the monitoring of risk handling plans include not only monitoring the completion of the steps outlined in the plan, but also monitoring the success of each step and the level to which the predicted risk reduction was achieved.

12.6.5 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 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

12.6.6 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.

12.7 Core Mission Assurance Processes 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 core mission assurance process (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 would be identified that relate to tasks of the design assurance CMP that are to be executed in the following preliminary design phase (Phase B).

In general, because RM addresses both "programmatic" (i.e., cost and schedule) and "technical" (i.e., MS 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 Section 12.8.

12.8 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 decisionmaking, and from the prime contractor. The latter 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 scope of the RM process planned for execution by a specific program, but in general shall at a minimum include the key elements discussed in Sections 12.8.1 and 12.8.2.

12.8.1 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 in item 2.

Items 1 through 3 usually require the execution of specific tasks 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 (DIs) as “government enabling products.”

As a more common alternative, the program RM process may be established according to the second of the two paradigms. In this case the MA organization will itself participate in the generation of the government RM information and results listed in 1 through 3. 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.

12.8.2 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 on 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 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 be reviewed for concurrence by the MA organization to ensure 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 ensure the documentation 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 items 1 and 2 – 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 items 1 and 2 – 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.

12.9 Example Risk Management Tasks

Table 12-1 contains examples of risk management tasks by phase.

Table 12-1. Tasks by Phase

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Program Risk Management Plan							
Ensure key elements of the government's Risk Management Plan are identified and defined.		X	X	X	X		
Ensure a risk management board is established to include program office (PO) participation.		X	X	X	X	X	
Assess Risk Management Training							
Ensure risk management training planned and provided to all PO personnel.		X	X	X			
Ensure risk management training planned and provided to contractor personnel.		X	X	X			
Assess Program Risk Baseline							
Ensure contractor-defined risks are reviewed and validated.		X	X	X	X		
Ensure review and validate identification of government-defined risk items.		X	X	X	X		
Ensure independent assessment conducted for critical mission impacting risks.		X	X	X	X		
Ensure PO membership in mission technical and management working groups.		X	X	X	X		
Assess Program Risk Handling Plans							
Ensure contractor risk handling plans are reviewed, validated, and implemented.		X	X	X	X		

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure mitigation plans are incorporated into the baseline.		X	X	X	X		
Ensure government program risk handling plans are defined and implemented.		X	X	X	X		
Ensure completion status of contractor and subcontractor risk handling plans.			X	X	X		
Ensure completion status of government risk handling plans.			X	X	X		
Ensure residual contractor risk items are updated and validated against the program baseline.			X	X	X		
Ensure residual government risk Items are updated and validated against the program baseline.			X	X	X		
Assess Pre-Launch Risk Resolution							
Ensure residual mission risk is identified and assessed.						X	
Ensure handling and close-out status of contractor and subcontractor risk items.						X	
Ensure handling and close-out status of government and subcontractor risk items.						X	
Ensure review and assessment of new contractor risk items.						X	
Ensure identification and assessment of new government risk items.						X	
Ensure assessment of risk items identified in MA reviews and audits.						X	

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure residual deployment/flight risk is mitigated or accepted.						X	
Assess Operational Risk Items							
Ensure operational data is reviewed to identify potential risks.							X
Ensure assessment performed on identified operational risk items.							X
Ensure mitigation plans/actions are defined for identified operational risk items.							X
Compile and Record Operational Lessons Learned for Continuing Utilization							
Ensure operational lessons learned are documented for continuing utilization.					X	X	X

12.10 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:

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, 7 February 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, and Effectiveness for Space and Missile Systems," 21 May 2001

Handbooks

TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, 31 January 2006

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

NASA Risk-Informed Decision Making Handbook, v.1.0, Office of Safety and Mission Assurance, NASA Headquarters, April 2010

Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, Second Edition, Office of Safety and Mission Assurance, NASA Headquarters, Washington, DC 20546, 13 January 2012

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

Chapter 13
Reliability Engineering

Roland J. Duphily
Acquisition Risk and Reliability Engineering Department

13.1 Introduction

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. A reliability plan (SMC-S-013 tailored) that defines the process is prepared and submitted as a program contract data requirements list (CDRL) item with periodic updates. Software (SW) reliability is not discussed here, but is addressed in Chapter 18.

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 (MA) function outside of the programs. While independent, it needs to work closely with system engineering (SE) 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.

13.2 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 ensuring the reliability level specified (numeric value) for a system or device will be achieved in its actual operation by the user.

13.3 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 (PMP), system safety, subcontractors, quality assurance (QA), I&T engineering, and configuration management (CM). 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 (HW) 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.

13.4 Practices

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 (CA). 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 HW, and the assessment of failures during I&T.

13.4.1 Core Activities

13.4.1.1 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. Reliability performance requirements should be stated in terms of the required results and the criteria for verifying compliance should be provided.

13.4.1.2 Reliability Predictions and Tradeoff Studies

Reliability block diagrams (RBDs) graphically represent the HW and SW needed for success, operating duty cycles, redundancy types, and any available workarounds. 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 should 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. Numerical results are reviewed for reasonableness when compared to similar systems.

13.4.1.3 Failure Modes Effects and Criticality Analysis

The FMEA or FMECA process is an effective tool in the decision making process, provided it is a timely iterative activity. An FMECA is identical to an FMEA except for the additional consideration of criticality, and is typically called a bottom-up analysis that looks at each HW 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 HW 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 ensures 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. After CDR, all design changes processed through change control boards (CCBs) should be evaluated by reliability and the FMECA should be updated when necessary to ensure no new unknown failure modes are introduced.

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. See TOR-2009(8591)-13 for guidance on FMECA process.

13.4.1.4 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 MA.

13.4.1.5 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. See TOR-2009(8583)-8929 for more details.

Electrical/electronic parts 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 parts stress analysis is conducted using nominal and worst-case environmental conditions. Unacceptable stress conditions based on derating criteria are eliminated. See SMC-S-010 for parts derating criteria.

13.4.1.6 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-217F, 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 (SMC-S-010), parts stress analysis, participation in government industry data exchange program (GIDEP) alerts, and nominal junction temperature limits less than 105°C. 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 PMP and reliability to validate the design.

13.4.1.7 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 parts, 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 CA.

13.4.1.8 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.

13.4.1.9 Failure Reporting Analysis and Corrective Action System

A closed-loop FRACAS is established to ensure that all failures are documented and analyzed for root cause, and that timely CAs are taken to reduce or prevent recurrence. It serves as a management tool to identify, correct, and prevent further recurrence of failures occurring in HW and SW during system debugging, engineering tests, qualification tests, ESS, receiving I&T, fabrication, acceptance tests, flight tests, and on-orbit failures. The program office (PO) should 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 CA results should 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 PO for review prior to the FRBs. Summaries of open failure report status are generally presented at regular contractor program reviews. In addition, delivered HW typically includes completed test failure reports as part of its end-item data packages (EIDPs). A good FRACAS process:

- Ensures that as a minimum, timely reporting begins at first power on of flight hardware.
- Ensures that a formal, documented and automated system is in place to capture track and close all testing failures of flight HW and SW. Look for FRBs or Material Review Boards (MRBs) (with reliability input) to close out failures.
- Ensures that every problem or failure is reported in a timely manner, and that the CA will preclude the recurrence of the problem/failure. Drive to the root cause.
- Ensures that for those special cases in which effective CA has not been fully implemented, the residual risk is identified and is acceptable to project/task managers.

13.4.1.10 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 (SOS) 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 (MS) probabilities.

13.4.2 Standards/Recommended Practices

When formalizing requirements for inclusion in a Request For Proposal (RFP), see Space Missile Systems Center Standard SMC-S-013, “Reliability Program for Space Systems.”

For detailed descriptions see SMC-S-010, “Parts, Materials, and Processes Technical Requirements for Space and Launch Vehicles”; TOR-2006(8506)-4494, “Space Vehicle Systems Engineering Handbook, Chapter 21, “Reliability Engineering”; TOR-2009(8583)-8929, “Space Vehicle Reliability Engineering Tutorial for SMC-University”; and TOR-2009(8591)-13, “Space Vehicle Failure Modes, Effects, and Criticality Analysis (FMECA) Guide.”

Most contractors have corporate manuals that describe their reliability engineering process. They also use commercial or home-grown SW tools to manage their reliability prediction, FMECA, and FRACAS activities.

13.5 Key Lessons Learned

13.5.1 Reliability Predictions

The value of MIL-HDBK-217 based predictions is greatest as a comparison tool. It is useful in comparing components against each other, more than providing an absolute value of component reliability.

The parts count method is conservative relative to the parts stress method as long as the parts stress analysis shows that parts meet the derating criteria.

13.5.2 Failure Modes Effects and Criticality Analysis

The most common weakness in FMEAs is keeping at too high a level. Performing the analysis at too high a level increases the risk of missing critical failure modes. Many internal failure modes can have effects on combinations of outputs which can be missed if the system is assessed only at a high level. The FMECA planning needs to be definitive on going to the level necessary to address critical modes such as failure propagation across component interfaces. The other weakness is starting the effort too late and the resultant loss of opportunity to impact the design.

13.5.3 Failure Reporting and Corrective Action System

Failure reporting should begin with first power on of flight HW and well documented within an automated closed loop process. A well represented and formal closure process such as an FRB that ensures all has been done to drive to root cause. When done properly, FRACAS is a failure recurrence prevention process that maximizes MS.

13.6 Strategies and Execution by Phase

Within the Mission Assurance Baseline (MAB) reliability engineering tasks are assigned to one of the following seven Mission Assurance Guide (MAG) phases first:

1. Phase 0: Pre-Phase 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 maximize mission probability of success and minimize single-point failures, reliability tasks (Table 13-1) begin in pre-Phase A to ensure that the 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 through 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 through C reliability analysis occurs during Phase D as a result of design and part changes that have been driven by CAs 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 through D2. The contractors FRACAS is reviewed along with participation as needed at MRBs and FRBs. Testing failure reports are reviewed for completeness and verification that all has been done to determine the root cause with adequate CA.

Participation at pedigree reviews, hardware acceptance reviews (HARs), and physical configuration audits (PCAs) are also accomplished to ensure that all documentation is adequately closed. During Phase D3, on-orbit failures are analyzed to determine the root cause and the space vehicle (SV) reliability

model/prediction updates are reviewed after redundancy losses in support of MLEs.

Table 13-1. Key Task by Phase

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Reliability input to RFP, Program reliability and availability requirements verification	X						
Assess negotiated contract reliability sections		X					
Assess system/subsystem/unit reliability requirements		X					
Assess reliability management plans		X					
Preliminary system/subsystem/unit reliability prediction, preliminary FMECA, CIL, LLIL			X				
Final system/subsystem/unit reliability prediction, final FMECA, single-point failure list, critical item control plans, worst-case analysis, parts stress analysis, accelerated life testing assessment				X			
System/subsystem/unit anomaly resolution verification					X		
Participate in contractors' failure analysis and corrective action boards (CABs)					X		
ESS verification					X		
Field anomaly resolution verification						X	
Launch/on-orbit anomaly resolution verification							X

For each life cycle phase, the process can be summarized by the following categories: program planning, SE, and space systems reliability engineering.

Program planning includes an evaluation of the contractor's reliability plan, to ensure that a good reliability engineering process is in place and accessible by the system PO technical team.

Systems engineering includes a series of tasks to ensure that the reliability engineering process integrates to all interfacing processes and that adequate participation and flowdown of reliability requirements exists. Ongoing assessments of reliability engineering processes throughout all the team players are also addressed in SE.

Space systems reliability tasks are required to evaluate whether the contractor's reliability engineering process at lower levels successfully flow up to the system and possible impact.

13.6.1 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 flowdown 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 (ORA), reliability engineering assists with the collection, review, and analysis of launch and on-orbit anomalies.

During MA reviews and audits, reliability engineering is an agenda item at SRR, PDR, CDR, and flight readiness review (FRR), and participates in functional configuration audits (FCAs) and PCAs.

13.7 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 data packages, and EIDPs are also needed. Table 13-2 contains a list of enabling reliability products.

13.8 Practice Reliability Task Application Example

When assessing reliability on a program, the first step is to determine the phase of interest and where in the PO WBS the reliability engineering activities are managed. The appropriate reliability subject matter expert (SME) assists the PO in determining what reliability tasks are needed using this guide as a roadmap. To assist the PO, a standard reference set of reliability tasks (Table 13-3) can be tailored to the program class (A, B, C, D). The reliability task products are then archived over the life cycle. This assist in the verification of accomplishment criteria associated with major milestones defined in gated processes such as the Integrated Master Plan (IMP).

Table 13-2. Enabling Reliability Products

Phase	Government Enabling Products	Contractor Enabling Products
Phase 0	RFP, SOW, CDRL, DIDs, WBS	
Phase A	Final Contract Criteria for SRR and SDR	Completion of Integrated Baseline Review (IBR), SRR, SDR, Reliability Plan
Phase B	Entrance/Exit Criteria for PDR	Completion of Preliminary Design Audit (PDA), PDR Completion of CDRLs

Phase	Government Enabling Products	Contractor Enabling Products
Phase C	Entrance/Exit Criteria for CDR and PRR	Completion of Critical Design Audit (CDA), CDR, Engineering Review Board (ERB)/CCBs Completion of CDRL
Phase D1	FRACAS Criteria	FRACAS Plan, FRB data packages, Completion of CDRL
Phase D2	Failure Reporting and Corrective System Criteria	FRB data packages, Completion of CDRL
Phase D3	Failure Reporting and Corrective System Criteria	FRB data packages, Completion of CDRL

Table 13-3. Reference Set of Reliability Tasks

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure reliability input to RFP is complete	X						
Ensure requirements for program reliability and availability are accurate and complete	X						
Assess negotiated contract reliability requirements		X					
Ensure system/subsystem/unit reliability requirements are allocated and complete		X					
Ensure reliability management is executed		X	X	X	X	X	X
Ensure Preliminary (Phase B)/Final (Phase C) system/subsystem/unit reliability predictions are complete and accurate			X	X			
Ensure worst-case and parts stress analysis is complete			X	X			

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure parts reliability analysis is complete			X	X			
Ensure accelerated life testing is complete			X	X			
Ensure preliminary (Phase B)/final (Phase C) FMEA is complete			X	X			
Ensure preliminary (Phase B)/final (Phase C) critical/limited life item control is executed and complete			X	X			
Ensure system/subsystem/unit anomaly resolution verification is tracked and complete					X		
Ensure FRB and CA board processes are executed and worked to closure with root cause identification					X		
Ensure ESS verification is executed and complete					X		
Ensure field anomaly resolution verification is completed to closure						X	
Ensure launch/on-orbit anomaly resolution verification is completed to closure							X

13.9 References

Policy-Related

AFI 10-602	Determining Mission Capability and Supportability Requirements, 20 September 2000 (contains reliability metrics definitions)

Specifications and Standards

IEEE STD 1413.1-2002	IEEE Guide for Selecting and Using Reliability Predictions Based on IEEE 1413, 2003
MIL-STD-756B	Reliability Modeling and Prediction, 18 November 1981
MIL-STD-1629A	Procedures for Performing a Failure Modes, Effects and Criticality Analysis, 24 November 1980
SMC-S-010	Parts, Materials, and Processes Technical Requirements for Space and Launch Vehicles, 13 June 2008
SMC-S-013	Reliability Program for Space Systems, 13 June 2008
TOR-2009(8583)-8929	Space Vehicle Reliability Engineering Tutorial for SMC-University, 13 January 2009

Handbooks

MIL-HDBK-217F	Reliability Prediction of Electronic Equipment, 2 January 1990
MIL-HDBK-338B	Electronic Reliability Design Handbook, 1 October 1998
TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, Chapter 21, Reliability Engineering, 30 November 2005
TOR-2009(8591)-13	Space Vehicle Failure Modes, Effects, and Criticality Analysis (FMECA) Guide, 15 June 2009

Best Practices

NASA Technical Memorandum 4322	NASA Reliability Preferred Practices for Design and Test, 8 December 2011

Deliverables

DI-RELI-80255	Failure Summary Report, June 1986
DI-RELI-80685	Critical Items List, September 1998
DI-RELI-80687	Failure Modes Effects and Criticality Analysis (FMECA), June 1986
DI-RELI-81315	Failure Reporting and Corrective Action System (FRACAS), 1989
DI-RELI-81496	Reliability Block Diagrams, April 1989
DI-RELI-81497	Reliability Prediction, April 1989
DI-SESS-81613	Reliability and Maintainability (R&M) Program Plan, October 2001

Chapter 14
Configuration Management

Roland J. Duphily
Acquisition Risk and Reliability Engineering Department'

14.1 Introduction

The primary purpose for **configuration management (CM)** is to establish and maintain control over a program's technical, hardware (HW), and software (SW) baselines consisting of requirements, specifications, designs, interfaces, data, and supporting documentation. The CM discipline provides a structured systems engineering (SE) approach to controlling baseline changes and conducting impact (e.g., performance, cost, and schedule) analysis to maximize mission success (MS) 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] [POs], and operations) to successfully implement those changes (e.g., databases, HW, SW, interfaces, drawings, requirements, supporting documentation) to maintain or evolve the system. CM plays a prominent role during a program's physical configuration audits (PCAs) and functional configuration audits (FCAs) as described in Chapter 6, Design Assurance.

14.2 Definitions

During system development, CM[90] 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 HW, SW, data, interfaces, procedures, and processes throughout a system's entire life cycle. CM of systems is based on the concept of configuration items (CIs).

A **CI**[91] may be defined as an individual item (e.g., HW component, SW module, procedure, or 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.

[90]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 SE Directive, GPG 7120.5, 4/8/2002, p.3.
[91]Ibid., p.48.

14.3 Objectives

The objective of CM is to ensure the SW and HW functional, allocated, developmental (SW), 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 MS. The CI level is where CM really begins; the process encompasses, to some degree, every item of HW and SW down to the lowest bolt, nut, and screw, or lowest SW 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.

14.4 Practices

14.4.1 Core Activities

The following are key CM assurance tasks:

- **Ensure a CM program and plan exists 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 PO use and eventually each system stakeholder will develop and use similar plans as its operational baselines accommodate newly delivered systems.

- **Ensure attributes and measurable performance parameters are defined at all needed levels of assembly.** These become benchmarks for the stakeholders and the development contractors to use as a known basis for acquisition and use of each item produced as part of system development.

- **Evaluate the identification, documentation, and verification of each CI's physical and functional characteristics or attributes to establish that an adequate description exists as a known basis for change.** CIs should be uniquely identified and verified to ensure they conform to, and perform as defined in, the configuration documentation.

- **Ensure manufactured items are correlated with their associated requirements, design, and product information.** Ensure a consistent reliable process is used to label each CI.

- **Ensure configuration information is captured 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 at CCB and assess performance, cost, and schedule impacts prior to making Class 1 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.

- **Ensure the establishment and use of a systematic change management process.** Change activity is managed and costly errors caused by ad hoc erratic change management are avoided.

14.4.2 Standards/Recommended Practices

The four basic principles of CM include: (1) identification, (2) change management, (3) status accounting, and (4) verification and auditing. For a detailed description see TOR-2006(8506)-4494, "Space Vehicle Systems Engineering Handbook," dated 30 November 2005, Chapter 23, "Configuration and Data Management."

When formalizing requirements for inclusion in a Request For Proposal (RFP), see Space and Missile Systems Center Standard SMC-S-002, "Configuration Management."

Most contractors have corporate manuals that describe their CM process. They also use commercial or customized product data management (PDM) SW to manage their corporate and program specific baseline documentation.

14.5 Key Lessons Learned

14.5.1 Configuration Management Organization Criteria

The CM organization should be organized with defined responsibilities and sufficient independence and authority to achieve the required CM objectives.

Their organization should ensure impartiality, independence, and integrity to achieve their required mission. The organizational hierarchy should be defined in a published organization chart which is maintained current. The organization should be project-related and adapted to meet the appropriate life cycle stage of the program. The relationships between activities directly involved in the CM process should be defined (e.g., CM organizational members and interfacing organizations). The relationships should be established to ensure the coordination of CM activities with other disciplines. The authority to approve configuration baselines should be fully defined. The CM system should be documented in a set of policies/procedures which are up to date and subject to document control procedures. Some method of corporate review for internal policy/procedure compliance should be in evidence and findings of deficiencies retained until corrective action (CA) is taken.

14.5.2 Configuration Management Program Planning Criteria

The specific program CM effort should be headed by a specified lead person designated by the contractor. The extent of procedural application to the specific program/project involved should be defined or tailored in a program-specific Configuration Management Plan (CMP). When available, the CMP should define applicable CM procedures to be used and who will be responsible for their performance. The CMP should also define the integration of subcontractor/vendor activities. Existing policies/procedures should be referenced within the CMP (to avoid duplication) and be available for review by the government, as required. CM milestones (e.g., design reviews and audits, documentation releases) should be identified in the respective level of program schedule for visibility and monitoring by the buyer.

14.5.3 Configuration Identification Criteria

Guidance criteria for the selection of CIs (HW and SW) should be available. The criteria should demonstrate an understanding that too many CIs increase cost and too few limit management opportunities. The main criteria for program-specific CI selection should be evident and should be related to 1) performance parameters and physical characteristics which can be separately managed to achieve overall end-use item performance, and/or 2) risk, safety, MS, logistic, or maintenance criticality. Documentation (e.g., specifications, drawings, manuals) procedures should be specified and be in compliance with program requirements. Company documentation numbering conventions should be established/identified. Identification numbering should be unique and address any supplier-unique numbering conventions expected for the program. Numbering conventions should allow for the identification of hierarchical relationships and any other unique grouping requirements. An understanding of configuration baselines and planning for the establishment of those baselines should be in evidence. Functional baselines should be established at least by the

engineering and manufacturing phase of the program. This classically yields formally released high-level performance documentation usually at a top level (e.g., system specification). Documentation should meet contractual program requirements delineated within the appropriate Contract Data Requirements List (DD Form 1423). The existence and location of HW and SW libraries/ repositories should be defined. Documentation release procedures and library/repository duplication procedures/responsibilities for SW and documentation should be clearly defined.

14.5.4 Configuration Change Management Criteria

Provisions for a formal review board (e.g., Configuration Control Board [CCB]) to review and approve controlled documentation, to include the CM Plan, CM procedures, Release Plan, specifications/drawings/manuals, and all proposed changes to them should be in evidence. Membership criteria and responsibilities should be defined. Change documentation planned for use on the program should be defined. Evaluation and approval criteria should be fully defined. The method of change implementation verification to be used should be clearly defined.

14.5.5 Configuration Status Accounting (CSA) Criteria

CSA records and management information reports which status the CM process should be in place. These records, at a minimum, should account for documentation status from its formal release for use up to its current release level (if different from the initial release level). Information tracked should include identification numbers, title, date, release status, and implementation status. Available report types and planned frequency of distribution should be identified. The reports can be computer-based or manual but they should provide, as a minimum, complete listings of baseline documents, listings of CIs and their baselines, current configuration status, and change implementation status.

14.5.6 Configuration Verification and Auditing Criteria

The contractor should be evaluated on his knowledge of FCA and PCA responsibilities and procedures defining CM personnel audit responsibilities. Audit events may be conducted on a progressive basis; however, SW and HW audit plans (if different) must be clearly differentiated. There should be a defined mechanism to track identified audit discrepancies until they have been closed by the customer. Audit milestones should be clearly defined on program master schedules.

14.6 Task Execution by Phase

Within the Mission Assurance Baseline (MAB), CM tasks are first assigned to one of the following seven phases:

1. Phase 0: Pre-Phase 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

The tasks listed in Table 14-1 ensure that spacecraft configuration baselines are well defined with a good change management, status accounting, and verification process. The assurance task products are e-mails, IOCs, or reports documenting the results of assurance tasks. CM tasks begin in pre-Phase A to ensure that the 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 through 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 HW and SW CIs and CCBs. Updating of Phases A through C baselines occurs during Phases D1 and D2 as a result of design and part changes that have been driven by CAs associated with mitigating failures that have occurred during qualification, acceptance, and integration tests at the CI, unit, subsystem, and system level. Verification of baselines occurs via FCAs and PCAs.

Table 14-1. Key Tasks by Phase

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess contract items such as SOW, CDRL/DIDs, RFP, WBS to ensure that all contractor tasks and deliverables are included, that evaluation criteria consider CM and that CM is adequately addressed by the requirements.	X						

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess contractual implementation of CM in contract (SOW, CDRL/DIDs, RFP, WBS) to ensure that all contractor tasks and deliverables are included, and that CM is adequately addressed by the requirements. Evaluate CM infrastructure.		X					
Review SRR and SDR entrance and exit criteria for CM. As appropriate, review SRR and SDR topics to ensure that CM is adequately addressed.		X					
Ensure that all CIs are identified. Review PDR entrance and exit criteria for CM. As appropriate, review PDR agenda topics to ensure that CM is adequately addressed.			X				
Assess PDA and PDR criteria for CM.			X				
Assess CM CDRLs.			X				
Review CDR and PRR entrance and exit criteria for CM. As appropriate, review CDR and PRR topics to ensure that CM is adequately addressed.				X			
Ensure that change management is implemented. Review the key CCB issues and evaluate waivers/deviations from CM procedures. Ensure that the CDR agenda addresses CM.				X			
Assess CM CDRLs.				X			

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure that the configuration control process is appropriately executed and maintained, and that CM issues are appropriated resolved. Identify CM-related risks to mission performance, reliability, suitability, and operability. Ensure that FCA/PCAs have appropriate entrance and exit criteria for CM, and the criteria are satisfied.					X		
Assess CM CDRLs.					X		
Ensure that the configuration control process is appropriately designed, used, and maintained. Review the key CM Board issues and evaluate deviations from CM procedures.						X	
Ensure that the reviews agenda address CM and CM waivers/deviations. Review Test Readiness Review (TRR), FCA/PCA, Formal Qualification Review (FQR), and Production Readiness Review (PRR) entrance and exit criteria for CM.						X	
Support IRRT CM activities.						X	
Assess CM CDRLs.						X	
As appropriate, provide CM assessments and guidance for ground segment and flight SW contract changes (upgrades, block changes), study efforts and routine operational patches.							X

For each life cycle phase, the process can be summarized by the following categories:

- **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 PO 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 PDM tools and resources for controlling all baselines. Ongoing assessment of CCB processes throughout all the team players are also addressed in SE.

- **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 (SV).

14.6.1 Core MA Processes (CMP) 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 flowdown of CM requirements to subcontractors.

During design assurance, CM assists with the assessment of CM plans, release plans, class of change, CCB procedures, baselines, HW and SW CIs (hardware configuration items [HWCIs] and computer software configuration items [CSCIs]), engineering change proposals (ECPs), Engineering Review Board (ERB), CCBs, 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 (ORA), CM assists with the management of configuration changes driven by launch and on-orbit anomalies that can change future builds.

During mission assurance (MA) reviews and audits, CM is an agenda item at SRR, PDR, CDR, Flight Readiness Review (FRR), and supports FCAs and PCAs.

14.7 Government and Contractor Enabling Processes 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, ERB/CCB procedures, CI lists, CCB minutes, ECPs, and end item data packages (EIDPs) are also needed. Table 14-2 lists enabling CM products.

Table 14-2. Enabling CM Products

Phase	Government Enabling Products	Contractor Enabling Products
Phase 0	RFP, SOW, CDRL, DIDs, WBS	
Phase A	Final Contract Criteria for SRR and SDR	Completion of Integrated Baseline Review (IBR), SRR, SDR, CM Plan, Release Plan, CCB Procedure
Phase B	Entrance/Exit Criteria for PDR	Completion of Preliminary Design Audit (PDA), PDR ERB/CCBs Completion of CDRLs
Phase C	Entrance/Exit Criteria for CDR and PRR	Completion of CDA, CDR ERB/CCBs Completion of CRLS
Phase D1	Entrance/Exit Criteria for FCA/PCAs	EIDPs ERB/CCBs Completion of CDRLS, FCAs, PCAs

Phase	Government Enabling Products	Contractor Enabling Products
Phase D2	Entrance/Exit for Criteria for System Verification Review (SVR), Manufacturing Readiness Review (MRR), Launch Readiness Review (LRR), FRR, and Independent Readiness Review Team (IRRT) IRRT CM activities.	Completion of readiness reviews ERB/CCBs Completion of CDRLs
Phase D3	Government CCBs for Ground Segment and Flight SW	Contractor ECPs to support the Ground Segment and Flight SW upgrades during operations

14.8 Practice CM Task Application Example

When assessing CM on a program, the first step is to determine the phase of interest and where in the PO WBS the CM assurance activities are managed. The appropriate CM subject matter expert (SME) then assist the PO in determining what CM assurance tasks are needed using this guide as a roadmap. To assist the PO, a standard reference set of CM tasks (Table 14-3) can be tailored to the program class (A, B, C, D). The CM assurance task products are then archived over the life cycle. This assist in the verification of accomplishment criteria associated with major milestones defined in gated processes such as the Integrated Master Plan (IMP).

Table 14-3. Reference Set of CM Tasks

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Contractual Implementation of CM	X	X					
Assess negotiated contract CM sections for completeness in regards to SOW, CDRLs, etc.							

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess CM Infrastructure	X	X					
Assess CM plan, release plan, and CCB procedures for adequacy and completeness							
Assess Configuration Identification Process	X	X	X	X			
Assess HWCIs, CSCIs, baselines, release process, etc.							
Assess CM Implementation							
Assess CM control process for subcontractors	X	X	X	X	X		
Evaluate effectiveness of ERBs and CCBs	X	X	X	X	X	X	X
Verify compliance with waiver and deviation process		X	X	X	X	X	X
Assess CSA process		X	X	X	X	X	X
Ensure configuration control activities are implemented		X	X	X	X	X	X
Verify compliance with CM plan, release plan, ERB/CCB procedures, ECP process, etc.		X	X	X	X	X	X
Verify compliance with waiver and deviation process		X	X	X	X	X	X
Audit CM process							
Assess FCA process					X		

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess PCA process						X	

14.9 References

Policy-Related

GPG 7120.5	Goddard Flight Center SE Directive, 8 April 2002

Specifications and Standards

SMC-S-002	Configuration Management, 13 June 2008
TOR-2006(8583)-1	Configuration Management, August 2005 (replaces MIL-STD-973, Configuration Management, 17 April 1992)

Handbooks

INCOSE-TP-2003-016-02, Version 2a	INCOSE SE Handbook, 1 June 2004
MIL-HDBK-61A(SE)	Configuration Management Guide, 7 February 2001
TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, Chapter 23, 30 November 2005

Deliverables

DI-CMAN-80556A	Configuration Audit Plan, 17 April 1992
DI-CMAN-80639C	Engineering Change Proposal, 13 January 1995
DI-CMAN-80640C	Request for Deviation, 30 September 2000
DI-CMAN-80641B	Request for Waiver, 13 January 1995

DI-CMAN-80642C	Notice of Revision, 30 September 2000
DI-CMAN-80858B	Contractors CM Plan, 30 September 2000
DI-CMAN-81516	As Built Configuration List, 15 July 1996

Other

Critical Process Assessment Tool (CPAT) on CM from Space and Missile Systems Center (SMC)/AXM, 14 August 1998
http://ax.losangeles.af mil/axe/axmp/cpat/

Chapter 15
Parts, Materials, and Processes

Dr. Steven R. Robertson
Parts, Materials, and Processes Department
Lawrence I. Harzstark
Electronics Engineering Subdivision
George G. Cuevas
Space Electronics Vulnerability Office
Howard Wishner
(Retired)

15.1 Introduction

The consequences of mission failure or inability to deploy the system on time because of parts, materials, and processes (PMP) issues should 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 PMP 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 PMP must also be clearly understood by the design team so that they can be applied in a manner to preserve their inherent robust capabilities.

PMP engineering has distinct MA elements that start with independently verifying that proposed contractual PMP 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 PMP controls and procedures have been developed and applied seamlessly across the program. In the implementation phase, MA focuses on ensuring that these controls and procedures are rigorously followed and that the program has indeed acquired the required robust PMP.

15.2 Definitions

PMP 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.

PMP engineering is a critical engineering discipline comprising a set of skills and knowledge used to select, apply, design, and manage PMP to manufacture an end product.

15.3 Objectives

The objective of PMP engineering is to provide a standardized set of qualified parts, materials, 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 PMP objectives achieve the required system performance through an efficient PMP program-wide policy that uses the best practices from prior or current military standards and existing supplier processes.

15.4 Practices

The PMP engineering activity plays an important role in the critical system engineering (SE) process, and as discussed previously, applicable to all phases of an acquisition. Key core practices/activities outlined in Section 15.4.1 form the basis of PMP MA, but are not limited to these practices. Products of core practices/activities are detailed in Section 15.7 and in many cases, preliminary versions can be developed in earlier phases and then finalized and maintained in the phases described.

15.4.1 Core Activities

PMP Requirements Definition. One of the primary PMP MA practices is the identification of the PMP requirements for the program as to parts selection, qualification, space quality baseline, approvals for non-standard parts, radiation, and data.

PMP Plan Reviews and Program Requirements Tailoring. A critical PMP MA task is the review/assessment of any modifications or changes the program

implements to the government flowdown requirements that are approved by the customer. Typically, the contractor prepares a PMP plan that defines exactly how the program will function, how program PMP requirements will be implemented, implementation of subcontractor requirements and management of subcontractors, screening, qualification, quality conformance inspection (QCI) and data, non-conforming items and the responsibilities and make-up of the PMP Control Board (PMPCB).

PMP Selection and Review and Approval of Drawings, Non-Standard Parts. The PMP plan defines the requirements for the review and approval of drawings including materials, non-standard parts approvals, approved parts selection lists, parts or materials waivers and deviations, procurement technical issues, and supplier selection and qualification.

The life-cycle costs of PMP as well as long-term availability are integral parts of PMP management. It is essential that PMP 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 the early program phase determines subsequent cost, schedule, and reliability of the end system. As a PMP MA process, the program approved selection and as-designed PMP lists should be independently reviewed with respect to available databases of past performance of similar PMP items. Similarly, selected suppliers' past performance should also be independently reviewed using available databases with issues being identified to the MA and program management organizations.

During production planning and PMP 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 ensure requirements are being met at both the supplier and subcontractor level and to provide a means of assessing technical and schedule performance. MA should ensure a seamless operation.

Several lists are typically generated for management of PMP programs. These lists are reviewed by the PMP MA team. These lists include the approved PMP selections lists, the as-designed PMP list and the as-built PMP list. The as-designed PMP list shall consist of the approved PMP items selected for use, and listed on the engineering drawing's parts and materials list and on the drawing notes. PMP "within, or internal to" an approved engineering drawing item shall also be listed in the as-designed lists. The as-built PMP list shall identify the PMP used in each deliverable end item. All PMP contained "within, or internal to" a deliverable item shall also be listed in the as-built list (e.g., elements internal to a hybrid).

Requirements. While it is recognized that developers' current procurement practices tend to select many 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 ensure 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 QCI were successful.

PMPCB. A PMPCB 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. The PMPCB is the central control function for parts, materials, and processes. The Board is responsible for any activity related to PMP including the subcontractor oversight functions. The PMP plan defines the overall responsibilities of the Board including its authority and delegation of functions. MA augments this activity by providing independent assessments through audits and continuing peer reviews. As a goal, PMPCB activities should appear seamless across developers and vendors, with common format and requirements being imposed on all.

Review of Screening, Qualification, QCI and Radiation Test and DPA Data. The PMP plan defines who is responsible for the review and approval of screening, qualification, QCI, radiation and Destructive Physical Analysis (DPA) data. Usually this is performed by the component engineering organization with radiation specialists reviewing the radiation data. On occasion, the data is reviewed by quality engineers.

Resolution of Nonconforming PMP and Failed PMP. The Material Review Board (MRB) is responsible for the disposition of non-conforming and failed items but shall use the expertise of the PMPCB members to provide technical assistance in the disposition recommendation. All PMP-related failures during production and test, starting at the QCI and lot DPA, are independently assessed for reach back and appropriate corrective actions (CAs). The common MA theme during these activities is based on the adage, "trust, but verify."

Program and Cross Program-Wide Issues Alert System. The program shall define the system the contractor has for identifying issues and non-conformances across the program and across all programs at the contractor to ensure problems do not go undetected and are brought to the forefront for impact. Review of this process is another MA activity.

Customer Right of Approval/Disapproval. Typically the customer has the right to approve/disapprove all actions at the PMPCB or within a specified period of time from the meeting. The approval/disapproval authority is established at the beginning of the contract and is an important MA responsibility of the PMP oversight team.

Required Skills. A wide range of skills and knowledge bases are required to support these activities. These include an in-depth understanding of applicable military standards (MIL-STDs) for various types of PMP and their associated standard testing methods, such as MIL-STD-883 test requirements for microcircuits and hybrids. 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 ensure 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 the scope of the government/contractor PMP engineering team.

15.4.2 Standards/Recommended Practices

The detailed PMP standard requirements for space programs are defined in two documents by The Aerospace Corporation (Aerospace). PMP program management requirements are defined in TOR-2006(8583)-5235, Rev. A, “Parts, Materials, and Processes Control Program for Space and Launch Vehicles.” This document establishes the requirements for the preparation, implementation, and operation of a parts, materials, and processes control program for use during the design, development, manufacture, assembly, integration, and test of space and launch vehicle (LV) systems. It is intended to be used in conjunction with TOR-2006(8583)-5236, Rev. A, “Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles.” TOR-2006(8583)-5236 establishes the minimum technical requirements for electronic parts, materials, and processes (electronic PMP) used in the design, development, and fabrication of space and launch vehicles. Both technical operating reports (TORs) are required to form a complete set of standards and practice requirements.

15.5 Key Lessons Learned

Space Quality Baseline (SQB) versus SCDs. Many contractors have not used the parts, materials, or processes defined on the SQB and generated a source control drawing (SCD) to define the requirements. In many cases, the SCD deviated from the standard PMP requirements as flowed down and incorporated in the SQB. It is believed that if an item had been selected from the SQB, it

would have required less monitoring and review than a non-SQB part and therefore would have been less costly to the program.

QCI. QCI or what is also referred to as lot acceptance test is one of three key test processes for space parts (100 percent screening and qualification are the other two). QCI is important to show that the actual flight lot still meets the design, construction, and quality requirements tested by prior qualification testing. Some issues detected later in systems test could have been discovered earlier if the lot had received a complete and proper QCI lot sample test. Evaluation of data has shown that QCI should be performed as defined in the applicable military specification (MIL-SPEC) especially on the flight lot.

Prohibited Materials (Pure Tin Escapes). Many contractors have relied on the supplier's certification of compliance that states no pure tin. This is totally insufficient as a prohibited materials prevention practice where in many cases it has been found that the parts may actually contain the prohibited material. Each lot must be evaluated for prohibited materials by non-destructive analysis techniques such as x-ray fluorescence (XRF) or energy dispersive spectroscopy (EDS) using a scanning electron microscope.

Counterfeit. Many examples of "counterfeit" parts have been observed when procuring from an independent distributor or broker and not from the original equipment manufacturer (OEM) or authorized/franchised distributor. All procurements must be made through the OEM or authorized/franchised distributor to mitigate the risks of counterfeit parts. Inspection and DPA should also be performed as part of counterfeit prevention practices.

Lack of Data Review. Based on evaluations of contractor data, it has been detected that many issues were observed in the data packages (incorrect test conditions, wrong limits used, tests not performed, data shows failures not detected, etc). It is imperative that the data be reviewed properly and thoroughly by the component engineering organization to ensure compliance.

15.6 Task Execution by Phase

Within the Mission Assurance Baseline (MAB), PMP tasks are first assigned to one of the following seven phases:

1. Phase 0: Pre-Phase 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

Key PMP tasks by phase are summarized in Table 15-1.

Table 15-1. Key Tasks By Phase

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess contract items such as SOW, CDRLs/DIDs, RFP, and WBS to ensure that contractor tasks and deliverables are included, that evaluation criteria considered PMP, and that PMP is adequately addressed by the requirements.	X						
Ensure adequacy of the PMP program policy and that it meets the derived system engineering constraints and performance needs.		X					
Ensure existence and adequacy of a cross-functional PMP management plan for efficient and uniform implementation of PMP policy.		X					
Ensure the development of an approved suppliers list and that a rating system for supplier's performance exists and is adequate.		X					
Assess contractual implementation of PMP in contract to ensure that contractor tasks and deliverables are included and PMP is adequately addressed by the requirements.		X					
Ensure establishment and adequacy of a functioning PMP control board for management of PMP on the program.		X					
Review plans for new technology insertion, ensure long lead items are identified and ensure flowdown of derived radiation hardness requirements.		X					

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Review Systems Requirements Review (SRR) and System Design Review (SDR) entrance and exit criteria for PMP and review topics to ensure the PMP is adequately addressed.		X					
Ensure that documented individual part, material, or process needs are consistent with PMP program requirements.			X				
Ensure development, maintenance, and control of a database/system documenting design requirements, design baseline, control, and use and control of life-limited and lot control items.			X				
Ensure development, maintenance, and control of approved selection, as-designed, and as-built program-compliant PMP lists and methodology for approval of new PMP.			X				
Ensure implementation of cross-program PMP issue alert system for impact review, tracking, and mitigation.			X				
Ensure development of a methodology for generation of temperature, radiation, and aging derating to meet system performance at end of life (EOL).			X				
Ensure development of part selection criteria, including the development of design manuals to ensure parts application does not exceed performance boundaries.			X				
Review and ensure an approved suppliers list.			X				

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Participate in PMPCB and review and approve PMP per program requirements.			X				
Review Preliminary Design Review (PDR) entrance and exit criteria and agenda topics to ensure PMP is adequately addressed			X				
Assess PMP CDRLs.			X				
Review and ensure PMPs have satisfactory screening, qualification, and lot qualification (a.k.a. QCI) data.				X			
Ensure demonstration and qualification of all new technology(s).				X			
Ensure the demonstration of critical manufacturing processes.				X			
Perform 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.				X			
Ensure development of a list of long lead items and methodology for ensuring “on-time” delivery.				X			
Ensure non-conforming PMP and MRB decisions are adequate and reviewed and approved by PMPCB.				X			
Ensure all analyses of failed components have reasonable root cause investigations and implementation of adequate corrective action (CA).				X			
Evaluate procured parts quality levels and specifications.				X			

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Participate in PMPCB and review and approve PMP per program requirements.				X			
Evaluate part stress analyses and radiation analyses.				X			
Verify degradation limits of critical parameters for use in worst-case design including radiation and aging degradation.				X			
Review radiation and validation of testing to ensure parts meet hardness assurance requirements.				X			
Review derating of PMP for compliance to requirements for long-term reliability.				X			
Review Critical Design Review (CDR) entrance and exit criteria, and agenda topics to ensure PMP is adequately addressed. Review key PMP issues and evaluate waivers and deviations. Ensure CDR agenda addresses PMP.				X			
Assess PMP CDRLs.				X			
Ensure there is an effective closed-loop system to feed back necessary changes derived from system-level performance results and industry data interchange.					X		
Review and monitor PMP qualification and lot acceptance test results, with emphasis on assessing any deviation from the initial requirement set and/or appropriate CAs.					X		
Ensure actual designs and application impacts on PMP are not exceeding limitations.					X		

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess new application impacts on PMP for reliability impacts and EOL adjustments.					X		
Ensure all analyses of failed components have reasonable root cause investigations and implementation of CA.					X		
Ensure new issue alerts (such as from Government Industry Day Exchange Program [GIDEP]) are properly addressed for potential impacts.					X		
During Phase D2 (fielding and checkout), PMP engineering activities and processes continue to ensure that performance expectations are being met, provide a continuing identification of technology and performance upgrade opportunities, and resolve and implement CAs/lessons learned for any system anomalies that are traceable to PMP.						X	
Ensure all reviews include addressing PMP waivers/deviations.						X	
Ensure newly issued alerts (such as from GIDEP) are properly addressed for potential impacts.						X	
As appropriate, provide PMP assessments and guidance for ground segment, study efforts, and operational anomaly resolution.							X

Phase 0

During this phase (requirements and concept definition/acquisition planning), government PMP provides support to concept studies and provides input to the Request For Proposal (RFP) released to contractors to bid on. Typically, the system program office (SPO) requests Aerospace to provide PMP inputs to the

RFP or statement of objectives (SOO). The government PMP tailors the PMP control program for SVs specified in TOR-2006(8583)-5235, Rev. A, Parts, Materials, and Processes Control Program for Space and Launch Vehicles (replaces MIL-STD-1546). In this way, the project's unique and special requirements are incorporated into a project-specific tailored PMP control plan.

During this phase, government PMP also tailors the technical PMP requirements for SVs specified in TOR-2006 (8583)-5236, Rev. A, Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles (replaces MIL-STD-1547). In this way, the project's unique and special requirements are incorporated into a project-specific tailored PMP technical requirements document (TRD).

The primary PMP objective of this phase is to ensure the PMP requirements in the RFP will result in the use of available, qualified, and reliable PMP consistent with program objectives. The government typically requires contractors to have a document detailing the contractor's PMP control program and technical requirements for PMP for SVs. The SPO requests Aerospace to evaluate a contractor-generated proposal or statement of work (SOW). During source selection, government PMP will evaluate contractors' proposals to ensure they implement PMP requirements in the RFP.

Phase A

During this phase (system definition/concept development), the government PMP verifies the contractor's PMP control program plan accomplishes the following: 1) defines all tasks and subtasks that apply to the selection, application, procurement and testing, etc. of PMP; and 2) ensures the PMP control program is consistent with operational requirements and mission needs. The PMP requirements are presented during the SRR to obtain agreement between the customer and the contractor as to precisely what PMP requirements are and how they relate to overall system and mission requirements.

Typically, the SPO requests Aerospace to evaluate the contractor's system specification. The government verifies the contractor has organized, chartered, and empowered a PMPCB to ensure consistency of PMP requirements set to required policy and directives. The government provides input at the SDR, defining top-level PMP requirements for the contract, and verifies that assurance characteristics and control features are documented as part of the initial concept baseline. The government MA team also ensures that selected characteristics and associated assurances levels fully meet system requirements and mission needs. The government verifies the prime contractor has flowed down PMP requirements to the subcontractor to the extent necessary to meet system-level requirements and ensure consistency of PMP requirements across all subcontracts. The government may also participate in subcontractor selection.

Phase B

During this phase (preliminary design), as the design and development are initialized, the PMP process is refined. The government evaluates contractor and subcontractor PMP control plans for adequacy and adherence to the tailored PMP requirements documents and verifies their PMP process is in accordance with program requirements. Government participates in PMPCBs. Government access ensures consistency of PMP requirements across all subcontracts.

In addition, during the preliminary design phase, the contractor generates data products in accordance with the requirements in the PMP control plan. For example, products will include such things as PMP characterization data, PMP selection list, preliminary parts list, and PMP approval requests (PARs). The government evaluates these data products to ensure they are of a maturity level commensurate with available engineering data and to see that they accomplish what is required by the PMP control plan. Verification of allocation and flowdown of PMP requirements to include life limiting material, aging, storage/environment, radiation effects, etc., is also accomplished during this phase. In addition, the contractor's test plans are evaluated to ensure parts tests will meet the PMPCB objectives and will not damage the parts.

It is also during this phase that the contractor's derating of PMP is reviewed for compliance to requirements for long-term reliability in accordance with program requirements. Implementation of PMPCB-approved policy for stress-derating across the program is verified. Stress deratings of parameter values are needed to achieve lower failure rates of PMP. EOL deratings are necessary to demonstrate circuits perform intended functions at EOL. Early identification of PMP derating issues allows mitigation such as replacement, life testing, analysis, etc. that can minimize additional costs and schedule delays.

A PDR is held during Phase B, at which time the preliminary design is presented. The contractor's PMP 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 to Phase C.

Phase C

PMP management is evaluated during 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. During this phase, all parts and material characterization/qualification testing should have been completed and reviewed. Radiation hardness assurance testing of flight lots should have begun. During this phase, failure analysis activity on failed PMP will occur and be reviewed for proper disposition by the government. Typical PMP MA

activities include evaluating procured parts quality levels and specifications, evaluating final part stress analyses, evaluating PMPCB operations, and evaluating final parts radiation analyses.

During this phase the contractor should generate data products for the PMP control plan tasks to the maturity level commensurate with the maturity level of available engineering data. The PMP MA activity is centered on review/assessment of activities and data products generated, which provide insight into the contractor's ability and progress toward meeting the flowed-down PMP requirements.

The PMP MA team verifies that PMP engineering monitored all subcontractors' performance to ensure that delivered products satisfy contractually flowed-down PMP requirements and allocated PMP design constraints. The team verifies the PMP processes have been properly implemented to include review of PMP selection lists, as-designed part lists, derating analyses, non-standard part approval requests, PMPCB minutes, etc. For radiation risk assessment, the team verifies the contractor's single event effects (SEE) analysis report and reviews whether the piece part SEE rate used in calculation of equipment outage rates is consistent with published (validated by parts engineering) SEE rates. The team ensures validity of piece part SEE rates used in SEE analysis and verifies the frequency of system outage (requiring ground assistance) satisfies specified system availability and dependability requirements. The PMP MA team verifies that the contractor held regularly scheduled PMPCB meetings for resolution/disposition of PMP issues and that all PMP issues were promptly resolved and effectively documented.

The team also verifies 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 PMP 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. The PMP MA team also ensures validity of piece part failure rates used in reliability analyses, based on stress derating factors mandated for the program.

The PMP MA team verifies degradation limits of critical parameters for use in worst-case design, that radiation degradation limits are derived from radiation test data, and that aging degradation deltas are derived from burn-in and life test deltas. The team ensures that degradation limits information is made available to designers in a timely fashion to allow assessment as to whether or not piece parts have the required EOL margin. Additional activities include verification of characterization data (including radiation characterization) and qualification

testing of new PMP and assurance of timely generation of radiation degradation limits for use in RLAT and worst-case design.

All PMP activities are to be successfully completed, evaluated, and approved prior to CDR. When CDR is successfully completed, Phase C can be considered completed and will advance to Phase D (build/operations).

Phase D1

During Phase D1 (fabrication and integration) PMP documents are updated and verification should be provided, indicating that the contractor maintained and updated the PMP control program plan, the program-approved parts list (PAPL), and other PMP 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 ensure thoroughness, completeness, and traceability requirements are met. This phase ensures that all noted PMP discrepancies/nonconformances and issues have been dispositioned in accordance with MRB or PMPCB procedures. This phase also verifies that the functional and product baselines have been established.

During this phase, PMP verifies that PMP 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 CA; ensures extensive characterization and, if necessary, performs independent characterization; and verifies that the PMPCB reviewed the results of the failure analysis and ruled on the validity of the cause and CA.

Phases D2 and D3

During Phase D2 (fielding and checkout) and Phase D3 (operations and disposal), PMP expertise is provided in support of on-orbit anomaly investigations.

15.6.1 Core Mission Assurance Processes Supported by PMP

During requirement analysis and validation, PMP assists with the development of PMP requirements for inclusion in the RFP, the assessment of PMP policy, requirements, and plans conducted by the prime contractor, and assessment of the flowdown of PMP requirements to subcontractors.

During design assurance, PMP assists with assessments of the implementation of PMP policy, plans, the documentation of individual part, material, or process needs consistent with PMP program requirements, and participation in PMPCB activities related to non-approved parts selection, derating criteria, and new part qualification process assessment.

During manufacturing assurance, PMP assists with audits of critical manufacturing processes, monitoring of PMP qualification, and lot acceptance test results, with emphasis on assessing any deviation from the initial requirement set and/or appropriate CAs.

During integration, test, and evaluation, PMP 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 CAs/lessons learned for any system anomalies that are traceable to PMP.

During operations readiness assurance, PMP assists with the review and analysis of launch and on-orbit anomalies.

During MA reviews and audits, PMP is an agenda item at SRR, PDR, CDR, and flight readiness review (FRR), and participates in FCAs and PCAs.

15.7 Government and Contractor Enabling Processes and Products

In addition to requiring access to the government's draft and final RFP, and negotiated contract that defines the requirements for PMP on the program, the PMP team needs access to the contractor's PMP policy that describes how the requirements will be met, implemented and managed, such as the PMP program management control plan and requirements, PMP subcontractor flow down requirements, radiation assurance control program, counterfeit control program, and prohibited materials control program. The PMP team will also need unfettered access to contractor's engineering teams, such as the PMPCB, MRB, failure analysis teams, Engineering Review Boards (ERBs), and Failure Review Boards (FRBs), at all levels of the program through the active design period, production, and testing activities. Contractor Contract Data Requirements Lists (CDRLs) for SDR, PDR, and CDR, PMP plans, PMPCB minutes, end item data packages (EIDPs), DPA reports, failure analysis reports, PMP lists including selection, as-designed and as-built lists and databases, derating stress analysis, both temperature and electrical, system reliability modeling, and model input assumptions at the piece part level are also needed. Table 15-2 contains a list of enabling PMP products.

Table 15-2. Enabling PMP Products

Phase	Government Enabling Products	Contractor Enabling Products
Phase 0	RFP, SOW, CDRL, Data Item Descriptions (DIDs), Work Breakdown Structure (WBS)	Proposal PMP Control Plan and PMP technical requirements detailing how requirements will be met
Phase A	Final contract Criteria for SRR and SDR Review and approval of PMP plans including requirements tailoring	Completion of SRR, SDR, PMP plan tailoring Radiation assurance, counterfeit and prohibited PMP plans
Phase B	Entrance/Exit criteria for PDR Attendance at Preliminary Design Audits (PDAs) Technology Readiness Assessments (TRAs) Review and approval of PMP drawings, lists, non-standard PMP requests	PMP characterization data Program approved parts list, approved PMP selection lists, preliminary parts lists, PMP approval requests Preliminary stress/derating analysis and reliability model/analysis Completion of internal TRAs for new technology insertion Completion of PDAs, PDR, and CDRLs
Phase C	Participation in and entrance/exit criteria for CDR and Manufacturing Readiness Reviews (MRRs) Review of parts lists and screening, qualification, radiation, and DPA data Review of MRB decisions and all non-conforming PMP	Completion of CDR, and CDRLs As-designed parts lists Screening, qualification, radiation, and DPA data MRB decision reports on non-conforming PMP Final stress/derating analysis and reliability model including input assumptions and exceptions for PMP

Phase	Government Enabling Products	Contractor Enabling Products
Phase D1	Participation in and entrance and exit criteria for Production Readiness Reviews (PRRs) and Test Readiness Reviews (TRRs) Review of manufacturing PMP issues Review of Bill Of Materials (BOMs) to ensure traceability to approved and as-designed parts lists	EIDPs Failure analysis reports and mitigation/CAs Deviations and waivers As-built parts lists Build/manufacturing discrepancy reports and FRB decisions
Phase D2	Participation in Phase D2 technical reviews including System Verification Review (SVR), Mission Readiness Review (MRR), Launch Readiness Review (LRR), and FRR	Completion of CDRLs for technical reviews Program impact from cross program issues
Phase D3	Review and guidance for ground segment and operational anomaly resolution possibly traced to PMP	Reports for ground segment and operational anomalies possibly traced to PMP

15.8 Practice Task Application Example

When assessing PMP on a program, the first step is to determine the phase of interest and where in the program office (PO) WBS the PMP activities are managed. The appropriate PMP subject matter expert (SME) assists the PO in determining what PMP assurance tasks are needed using this guide as a roadmap. To assist the PO, a standard reference set of PMP tasks (Table 15-3) can be tailored to the program class (A, B, C, D). The PMP task products are then archived over the life cycle of the program. This assists in the verification of accomplishment criteria associated with major milestones defined in the gated processes such as the Integrated Master Plan (IMP) to help support a successful program.

Table 15-3. Reference Set of PMP Tasks

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Parts, Materials and Processes Tasks							
Assess contractual implementation of PMP	X	X					
Assess PMP infrastructure	X	X					
Assess PMP process	X	X	X	X			
Assess PMP implementation	X	X	X	X	X	X	X
Assess PMP activities are implemented		X	X	X	X	X	X
Audit PMP Process					X	X	

15.9 References

Specifications and Standards

MIL-STD-883	Test Requirements for Ground Equipment and Associated Computer Software Supporting Vehicles, 13 November 1989
MIL-STD-1556B	Government/Industry Data Exchange Program (GIDEP) Contractor Participation Requirements, 24 February 1986
TOR-98(1412)-1, Rev. A	Electronic Parts, Materials, and Processes Control Program for Expendable Launch Vehicles, 1 January 2004

TOR-2006(8583)-5235, Rev. A	Parts, Materials, and Processes Control Program for Space and Launch Vehicles, 30 September 2008 (replaces MIL-STD-1546)
TOR-2006(8583)-5236, Rev. A	Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles, 30 September 2008 (replaces MIL-STD-1547)

Handbooks

MIL-HDBK-965	Acquisition Practices for Parts Management (for GIDEP Application Guidance Manual), 30 September 1996
TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, 31 January 2006
TOR-2006 (8546)-4591	Space Vehicle Test and Evaluation Handbook, 6 November 2006

Deliverables

The following is a list of DID documents that form the typical instructions for deliverable PMP products through CDRLs. These DIDs are older documents that should be tailored to appropriately reference the requirements of TOR-2006(8583)-5235, Rev. A, and/or TOR-2006(8583)-5236, Rev. A.

DI-CMAN-81516	As-Built Parts, Materials and Processes List, 15 July 1996
DI-MGMT-81334	Contract Work Breakdown Structure (CWBS), 1 February 2005
DI-MGMT-81453	Data Accession List (DAL), 23 January 1995
DI-MISC-80071E	Parts Approval Request, 5 August 1998
DI-MISC-80526D	Parts Management Plan, 5 August 1998
DI-MISC-81276A	As-Designed Parts, Materials and Processes List, 16 May 1986

DI-MISC-81277	Parts, Materials, and Processes Selection List, 27 July 1992
DI-QCIC-80125B	Government Industry Data Exchange Program (GIDEP) Alert/Safe-Alert Report, 5 May 2003
DI-RELI-80253	Failed Item Analysis Report, 17 October 1986
DI-RELI-80255	Failure Summary and Analysis Report, 17 October 1996

Chapter 16
Quality Assurance

Dana J. Speece
David P. Helgevold
Eric S. Richter
Product and Process Assurance Department

16.1 Introduction

Quality assurance (QA) is the engineering and management specialty discipline that implements the planned and systematic activities in a quality system so that quality requirements for a product or service will be fulfilled. QA activities support many other disciplines such as reliability engineering, configuration management (CM), parts, materials, and process (PMP) engineering, safety engineering, systems engineering (SE), manufacturing and test engineering, purchasing, and systems integration and test (I&T). One of the primary goals of QA is to ensure deliverable products and services are produced using approved and documented processes and procedures. These procedures are often based on standards such as those addressing design and workmanship.

A QA program provides an organizational framework and implements process controls that are the most conducive to ensuring 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 ensures that all quality requirements are met through control of operations, processes, procedures, testing, and inspection.

The government program office (PO) 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 to successfully execute a QA program for government programs.

16.2 Definitions

Product or service quality. The degree to which the product or service attributes, such as capability, performance, and reliability, meet the needs of the customer or mission, as specified through the requirements definition and allocation process.

Quality assurance (QA). The engineering and management specialty discipline that defines the standards to be followed to meet the product or service customer requirements. It implements planned and systematic activities in a quality system to accomplish this. QA consists of preventive actions which are focused

on processes and procedures and ideally done prior to the delivery of the product or service.

Quality control (QC). The set of observation techniques and activities used to fulfill requirements for quality. QC is focused on detecting defects once the product or service is produced. This detection is often based on review of completed documentation, physical inspection, and test. QC is a subset of QA.

Quality engineer (QE). A person trained to implement, verify, and validate the quality management system (QMS). QEs may have specialties in software (SW), metrology, supplier oversight, destructive and nondestructive testing, planning, manufacturing and testing, auditing, process control, and metrics. Prior to a product or service delivery, they are responsible for ensuring the proper checks are in place. During production they will participate in material and failure review board (MRB/FRB) activities. After production they may be responsible for the product or service acceptance.

Quality management system (QMS). A documented business system whose goal is the reduction and elimination of nonconformances to standards, specifications, and customer expectations in the most cost-effective and efficient manner. Organizations use a QMS to direct and control how quality policies are implemented and quality objectives are met.

Program office (PO) quality assurance. The quality activity associated with the organization responsible for defining and maintaining the standards of project management. PO in this context refers to a government-staffed organization and/or a separately staffed organization within The Aerospace Corporation (Aerospace).

16.3 Objectives

16.3.1 Contractor Objectives

The primary objective of a comprehensive contractor QA activity is to ensure that the delivered hardware (HW) and SW products as well as services 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. A secondary QA program objective is to ensure that the subcontractor's/vendor's plans satisfy those requirements. Supplier quality provides this function. In particular, a good QA program implemented by the contractor:

- 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 that could result in less than satisfactory performance

- Provides for timely and effective corrective action (CA)

16.3.2 Program Office Objectives

The PO QA objective is to provide oversight of all contractor activities that may have an impact on product or service quality throughout the life of the contract. In this capacity the PO may perform audits of contractors, review data (technical, cost, and schedule), participate in failure review, participate in sell-offs of HW or SW, report to the ultimate customer, and on occasion direct the contractor to perform additional activities. Because they are a separately funded entity, they often will augment contractor activities by providing specialists who assist in solving program problems. While POs have a contractual relationship with the prime and often major contractors, they typically do not have a contractual relationship with subtier suppliers and therefore have only indirect influence on these organizations.

16.4 Practices

16.4.1 Contractor Core Activities

The following are key contractor QA tasks:

- Perform initial quality planning, which encompasses the processes of reviewing, documenting, and flowing down requirements imposed by the customer, statutory, regulatory, and contractor's internal requirements. The program quality plan documents the requirements. It is developed by the contractor and submitted to the customer for approval. Once established and documented in the quality plan, the quality processes are flowed down through the contractor's internal organizations, subcontractors, and suppliers/vendors through the program quality requirements documents.

- Provide quality involvement in the design review process, which is another aspect of initial quality planning. Product designs are reviewed for producibility, inspectability, and ability to verify specific requirements are met.

- Identify the method of qualification for parts, units, and SW and in particular establish the approach for items that have not flown before in the environmental conditions of the program under review.

- 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 CM process.

- 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 on receipt, or by delegation of verification to the supplier.

- Ensure that production operations, including inspection operations, are carried out in accordance with approved data. Approved data includes drawings, parts lists, and production documents (e.g., manufacturing plans, traveler, router, work order, or planning). Changes to the approved data are documented and approved by authorized contractor quality representatives.

- Maintain the identification and traceability of the product throughout production. Identification of the configuration of the product is maintained to identify any differences between the actual configuration and the latest released configuration. Media used as an acceptance authority (e.g., stamps, electronic signatures, passwords), shall be controlled by established and documented controls.

- Ensure the conformity of the product throughout manufacturing, tests, 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 of products necessary 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.

- Maintain 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 procedures to control nonconforming material. A nonconformance resulting in a departure from contract requirements requires authorization from the customer, unless the customer has authorized specific use-as-is or repair dispositions for the product. Product dispositioned as scrapped shall be conspicuously and permanently marked or positively controlled until it becomes physically unusable. Only properly trained and certified contractor personnel including quality representatives shall be allowed to disposition nonconforming material.

- Avoid the recurrence of nonconformances by developing documented procedures to identify the root causes of nonconforming materials and/or processes and correct them through a CA process. A preventive action process should also be in place to help eliminate the cause(s) of potential nonconformances before they occur.

- Collect data that demonstrates the end item or product satisfies the requirements and conforms to specified manufacturing processes. Each end item should meet the user expectation outputs, including quality objectives and requirements of the product. End items should be built and tested with required processes and verification methods such as inspection or test. End items should be properly documented by providing evidence of product realization including acceptability assessments of products at all stages of assembly and test.

- Conduct audit activities related to manufacturing and testing of the product, including first article inspection. These include functional configuration audits (FCAs), physical configuration audits (PCAs), QMS audits, and contractor and subcontractor/supplier audits.

- 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 ensure the contractor's quality system is effective and maintained.

- Prepare and report on metrics that reflect the health of the QMS. Metrics may include status of nonconformances, failure reports, audit summaries, supplier oversight, scrap and other cost of poor quality, training, metrology, corrective and preventive actions, corrective action board (CAB) results, and results of process evaluations.

16.4.2 Program Office Core Activities

- Establish, document, and maintain a quality program for each acquisition based on contractual QA requirements (see Section 16.5). Ensure that contractors have a QMS that satisfies those requirements. 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 ensure 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.

- Review qualification of HW, SW, or facilities and request more conservative approaches when risk should be reduced.

- Review data presented in program quality reviews or side sessions given by the contractor QA organization. This activity seeks to assess the contractors' conclusions, make suggestions for further improvement, and request additional data if further detail or justification is required.

- Participate in design reviews, manufacturing reviews, or mandatory customer inspections when contractually allowed or permitted.

- Conduct separate investigations involving either component or material testing or review of existing data. For example, in the latter case, a

review of waivers might be conducted to understand how the number of waivers might be reduced on a follow-on contract.

- Review and approve or disapprove use-as-is and repair dispositions.

- If contractually required, participate in PCA, FCA, and hardware acceptance reviews (HAR). The material commonly reviewed in a HAR is called the end item data package (EIDP).

16.5 Recommended Quality Standards for Acquisition of Space Programs

Contractors should be registered to the current revision of SAE AS9100, "Quality Management Systems – Requirements for Aviation, Space and Defense Organizations." This standard was written specifically for the aerospace and space industry and is based on the more universal ISO 9001:2008, "Quality Management Systems – Requirements," standard.

Frequently, subtier suppliers and suppliers are not registered to AS9100 because the aerospace demands and expense of conformance to the standard are not justified by their business model. ISO 9001:2008 may be more appropriate as this standard simply requires a QMS is in place. If this is the case, the contractor may flow additional program-specific quality requirements to the supplier.

The registration process for AS9100 and ISO 9001:2008 is an expensive process both to receive the initial registration as well as to maintain it. Both standards require continual improvement and mandate audits by an independent third-party registrar, often on a yearly basis. As a result many smaller suppliers do not comply with either standard formally, although they may possess a QMS which satisfies many of the standards' requirements. In this case, the prime contractor or major contractor who employs these firms should exercise closer oversight by performing QMS audits and review of purchase product.

Aerospace noted that AS9100 lacked specific requirements found to be beneficial for the production of space HW. It developed TOR-2005(8583)-3859, "Quality Assurance Requirements for Space and Launch Vehicles" (2005), which provides additional requirements based on lessons learned from acquisition and execution of successful space programs. This document was converted into Space and Missile Systems Center Standard SMC-S-003, "Quality Assurance for Space and Launch Vehicles" (2008), and is recommended as a requirements document for SMC acquisitions. Additional quality requirements may be found in SMC-S-013, "Reliability for Space Systems" (2008), and SMC-S-021 Vol. 1, "Technical Reviews and Audits for Systems, Equipment, and Computer Software" (2009).

16.6 Key Lessons Learned

- The contractor's quality organization should ensure 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 certification of assemblers and inspectors for special processes such as soldering and welding.

- The quality organization determines the necessary competence for personnel performing work that has an effect 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 quality organization shall ensure buildings, workspace, process equipment, and support services needed to achieve product quality are adequate.

- Ensure design control, using a pragmatic methodology to evolve a system's design by baselining product design at various stages of maturity during development. The approach should include process planning for task sequence, mandatory steps, configuration control, review, verification, validation, responsibilities, and authority. It is critical to manage interfaces between different groups involved in the design and development to ensure effective communication and clear assignment of responsibility.

- Ensure the adequacy of the specified requirements in purchase documentation prior to transmittal to the supplier/vendor. This includes verification that the purchase is being directed to an approved supplier or vendor. Approved suppliers or vendors have been periodically reviewed and evaluated for their ability to supply products in accordance with the organization's requirements. When a contractor is organizationally part of a larger corporation, often the corporation establishes an approved suppliers list which is applied universally. Since space HW design and materials are so demanding, often suppliers approved by the corporation are not appropriate for the facility's space requirements. This situation requires special attention by the particular facility.

- The contractor's quality organization should participate in key program reviews to evaluate the effectiveness of implementing QA requirements that ensure compliance with the overall contract technical requirements. Activities supporting program reviews include system requirements reviews (SRRs), design reviews, producibility readiness reviews

(PRR), manufacturing reviews, test readiness reviews (TRRs), MRBs, FRBs, pedigree reviews, HARs, and independent readiness reviews (IRRs).

16.6.1 Quality Assurance Organization Criteria

The QA organization should include defined responsibilities and sufficient independence and authority to achieve the required QA objectives. An effective QMS and QA organization requires 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 preventive and CAs, status of follow-up actions from previous management reviews, potential changes that could affect the QMS, and recommendations for improvement.

16.7 Task Execution by Phase

Within the Mission Assurance Baseline (MAB), QA tasks are first assigned to one of the following seven Mission Assurance Guide (MAG) phases:

1. Phase 0: Pre-Phase 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

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 0 and A, QA is tasked with ensuring that quality requirements will be identified and flowed down through the contract. QA 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, QA 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 ensuring the QMS is continuing to function well. Completed HW may undergo

pedigree reviews in preparation for integration and next-level test activities. At the launch site, QA is required to ensure the safety of the HW will be maintained through launch. Once on-orbit, the QA 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. Specific QA tasks by program phase are listed in Table 16-1.

Table 16-1. Tasks by Phase

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess contract items such as the Request For Proposal (RFP) and statement of work (SOW) to ensure all contractor tasks and deliverables are included, evaluation criteria consider QA, and QA is adequately addressed by the requirements. 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.	X						
Assess contractual implementation of QA in the contract (SOW, contract data requirements lists [CDRL], data item description [DID], RFP, work breakdown structure [WBS]) to ensure all contractor tasks and deliverables are included, and QA is adequately addressed by the requirements. Evaluate QA infrastructure.		X					

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Review SRR and system design review (SDR) entrance and exit criteria for QA. As appropriate, review SRR and SDR topics to ensure QA is adequately addressed. 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 products 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.		X					
Review preliminary design review (PDR) entrance and exit criteria for QA. As appropriate, review PDR agenda topics to ensure QA is adequately addressed.			X				

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
QA is involved in evaluating the adequacy of QA requirements in the contractual requirements documents, associated contract deliverables, and PDR documentation. 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 participating in supplier site surveys, particularly those conducted with new suppliers or at new facilities.			X				
Review CDR and PRR entrance and exit criteria for QA. As appropriate, review CDR and PRR topics to ensure QA is adequately addressed.				X			

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
As the design phase 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. Finally QA participation in MRR and producibility reviews results in an understanding of the program's production readiness level and risks.				X			
During the fabrication and integration phase 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, I&T activities, FCAs and PCAs, pedigree reviews, HARs, and CABs.					X		
When HW 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.						X	
Operations and disposal phase uses QA support by exception.							X

16.8 Government and Contractor Enabling Processes and Products

In addition to requiring access to the government's draft and final RFP, and the negotiated contract, QA needs access to the contractor's QMS and QA policies, practices and guidance documentation across the prime and subcontractors. The contractor and subcontractor quality program plans and associated CDRL and subcontract data requirements list (SDRL) items are necessary products needed for review. Unit, subsystem, and system-level EIDPs are also needed to perform on overall assessment of product quality. Table 16-2 contrasts the government versus contractor enabling QA products by program phases.

Table 16-2. Enabling QA Products

Phase	Government Enabling Products	Contractor Enabling Products
Phase 0	RFP, SOW, CDRL, DIDs, WBS	
Phase A	Final Contract, Release of interface control document (ICD) Entrance/Exit Criteria for SRR and SDR	Completion of integrated baseline review (IBR), SRR, SDR, Program QA Plan, Corporate QMS policy, past QMS registration audit results
Phase B	Entrance/Exit Criteria for PDR	Completion of preliminary design audit (PDA), PDR Completion of CDRLs Make-buy decisions addressed
Phase C	Entrance/Exit Criteria for CDR, PRR, and MRR Content requirements for EIDPs, Test, and Integration requirements	Completion of critical design audit (CDA), CDR Completion of CDRLs MRRs, Producibility, and First Article Review Results
Phase D1	Entrance/Exit Criteria for MRRs, TRRs, FCA, PCAs, and HAR activities	Supplier Quality Audits results TRR Engineering Review Board (ERB)/configuration or change control board (CCB), CM records, EIDPs, FCAs, PCAs

Phase	Government Enabling Products	Contractor Enabling Products
Phase D2	Entrance/Exit Criteria for System Verification Review (SVR), Launch Readiness Review (LRR), Flight Readiness Review (FRR), and Independent Readiness Review Team (IRRT)	Launch site QA plan if applicable Completion of readiness reviews
Phase D3	On-orbital anomaly/failure reports	On-orbit anomaly resolution data Lessons learned

16.9 Practice Quality Assurance Task Application Example

When assessing QA on a program, the first step is to determine what is the phase of interest and where in the PO WBS the QA activities are managed. The appropriate QA subject matter expert (SME) then assists the PO in determining what QA tasks are needed using this guide as a roadmap. To assist the PO, a standard reference set of QA tasks (Table 16-3) can be tailored to the program class (A, B, C, or D).

Table 16-3. Reference Set of Quality Assurance Tasks

	Phase					
Task	**0**	**A**	**B**	**C**	**D1**	**D2**
Assess contractual implementation of QA requirements						
Assess negotiated contract QA requirements sections for completeness in regard to SOW, CDRLs, etc.	X	X				
Assess Quality Management System						
Assess QA plan, QA policies and procedures for adequacy and completeness	X	X				

	Phase					
Task	**0**	**A**	**B**	**C**	**D1**	**D2**
Assess QA Processes						
Assess QA procurement controls, design controls, manufacturing and test controls, and nonconforming material controls	X	X	X	X		
Assess QA Program Implementation						
Assess QA flowdown of requirements to subcontractors and suppliers	X	X	X	X	X	X
Evaluate effectiveness of inspections and test				X	X	
Evaluate effectiveness of the nonconforming material control system			X	X	X	
Evaluate the effectiveness of MRRs, TRRs, and HARs			X	X	X	
Audit QA process			X	X	X	

16.10 References

Specifications and Standards

ISO 9001:2008	Quality Management Systems – Requirements, 15 November 2008
SAE AS9100	Quality Management Systems – Requirements for Aviation, Space and Defense Organizations, 15 January 2009
SMC-S-003	Quality Assurance for Space and Launch Vehicles, 13 June 2008
SMC-S-013	Reliability Program for Space Systems, 13 June 2008

SMC-S-021, Vol 1	Vol 1: Technical Reviews and Audits for Systems, Equipment, and Computer Software, 15 September 2009

Handbooks

TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, 30 November 2005
TOR-2006(8546)-4591	Space Vehicle Test and Evaluation Handbook, 6 November 2006
TOR-2005 (8583)-3859	Quality Assurance Requirements for Space and Launch Vehicles, 1 December 2005

Chapter 17
Systems Safety Assurance

Lucio U. Tolentino
Systems Effectiveness Department
Richard C. Maynard
Independent Readiness

17.1 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.

17.2 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 damage to 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.

17.3 Objectives

A system safety risk management process is established and used to provide effective implementation of safety and occupational health policies. To ensure 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 ensure 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, is 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.

17.4 Practices

17.4.1 Core Activities

The identification and understanding of hazards and their associated risk is the basic practice 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.

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.

17.4.2 Standards/Recommended Practices

The order of precedence for system safety hazard control is:

- **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.

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).

Descriptions of 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 shortcut 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 (HW) 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.

17.5 Key Lessons Learned

Lesson Learned: Operational hazard analysis should check risk of commands

Operational hazard analysis did not detect risk of using wrong gyro sensitivity setting during on-orbit testing of satellite. One of the purposes of operational hazard analysis is to identify the risks associated with unintentional commanding. The hazard analysis should consider the fidelity of command testing and the interaction of command settings on the risk to spacecraft operation.

The satellite in question had two settings on gyro sensitivity, fine and coarse. The fine setting was in place instead of the coarse setting when an on-orbit roll

test was initiated and caused the satellite's attitude control system to saturate and go out of control. (AERO-LL-0129)[92]

Lesson Learned: Ordnance subsystem hazard analysis should consider risk of multiple ordinances in a chain not operating.

Subsystem hazard analysis did not detect the hazard of the first ordnance, which interfered with the initiation of the second ordnance. Ordnance hazard analysis should consider the risk of the dynamic response of the spacecraft from the first ordnance device interrupting the initiation of other ordnance.

A spacecraft fairing failed to open in flight because when its first ejection ordnance fired it disconnected pins to follow-on ordnance for the removal of the fairing. (AERO-LL-0089)[93]

Lesson Learned: Structural hazard analysis should consider the risk of using unvented honeycomb panels.

Structural hazard analysis did not consider the effects of low atmospheric pressure on the structural integrity of honeycomb panels.

Several satellites have been destroyed when their honeycomb structures failed. (AERO-LL-0001)[94]

17.6 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 through A. During Phases B and C, system safety is a member of the design team and supports discussions with applicable safety organizations, engineering, testing plans, handling plans, and operational plans. A large safety effort occurs during Phases B through 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 and C require a substantial system safety analysis that is captured in the initial draft of the *Missile System Prelaunch Safety Package* (MSPSP), or such documents as an Accident Risk Assessment Report (ARAR). During Phases D1 and 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 HW. Early participation and involvement in the life cycle of a system will ensure that

[92]Lesson Learned 129, TOR-2005(8617)-4204, 100 Questions for Technical Review.
[93]Lesson Learned 89, TOR-2005(8617)-4204, 100 Questions for Technical Review.
[94]Lesson Learned 1, TOR-2005(8617)-4204, 100 Questions for Technical Review.

system safety is properly addressed during system reviews, meetings with regulatory organizations, and integrating into the operational system.

System safety is a systematic approach to ensure 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 (EOL) disposal. Actions should be taken to minimize the use of hazardous materials to minimize the risks and life cycle costs associated with their use.

17.6.1 Organization of Tasks

The Mission Assurance Baseline (MAB) for system safety is organized in a hierarchy using the Mission Assurance Guide (MAG) phases discussed in Section 7.6. For each life cycle phase, the process is further organized into the following categories:

- **Program planning** includes an evaluation of the contractor's system safety plan, management plans for interaction with range safety and other regulating agencies, the initial 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 (SE)** 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.

17.6.2 Core Mission Assurance 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 flowdown of safety requirements to subcontractors.

During design assurance, system safety assists with the assessment of hazards analysis studies, the assessment of critical hazards mitigation, and the 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 the review of space vehicle fueling operations.

During mission assurance (MA) 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).

17.7 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 Systems Requirements Review (SRR) in 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 (PO's) strategy and responsibility for integrating environmental safety and occupational health (ESOH) into the SE

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 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. 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 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 Critical Design Review (CDR), an 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 SW 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 planning system disposal should be continued.

In 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 the completion status should be continued. System disposal planning should be completed. Phase D ends with system disposal.

17.8 Practice Task Application Example

When assessing system safety on a program, the first step is to determine what phase the program is in. From Table 17-1, the System Safety Manager (SSM) can evaluate the tasks that have been completed and the tasks that need to be

completed. System safety is an ongoing process throughout the life cycle of a system.

Table 17-1. Reference Set of System Safety Tasks

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess candidate architectures to support selection of most suitable technical approach	X	X					
Assess inputs to initial acquisition documents	X	X					
Assess system safety integration with design engineering		X	X				
Ensure risks are identified and reduced to acceptable level		X	X	X	X	X	X
Assess hazard analysis for adequacy and completeness	X	X	X	X			
Assess System Safety Program Plan		X	X	X	X	X	X
Assess PESHE		X	X	X	X	X	X
Assess hazard analysis and assessment			X	X	X	X	
Assess health hazard assessment process for adequacy			X	X	X	X	X
Assess operating and support hazard analysis				X	X	X	X
Assess process for tracking and mitigating hazards				X	X	X	X
Ensure system safety assesses configuration changes and deviations/waivers				X	X	X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess disposal (on-orbit and ground based) and demilitarization requirements				X	X	X	X
Assess compliance with environmental, safety, and occupational health regulations				X	X	X	X
Assess adequacy of explosive hazard classification and characteristics				X	X		
Assess explosive ordnance disposal source data for adequacy and completeness					X	X	X
Assess system safety compliance with government policy and requirements			X	X	X	X	X
Assess safety verification process for adequacy and completeness				X	X	X	X
Assess space vehicle hazard launch site procedures						X	X
Assess adequacy of MSPSP						X	
Assess environmental, safety, and occupational health requirements, processes, and activities			X	X	X	X	X
Assess post-flight analysis						X	X

17.8 References

Policy-Related

AFI 91-202 — USAF Mishap Prevention Program 1 August 1998

AFI 91-202, AFSPC Sup1 — USAF Mishap Prevention Program, 1 June 2005

AFI 91-217	Space Safety and Mishap Prevention Program, 18 February 2010
NSS Acquisition Policy, Number 03-01	Guidance for DOD Space System Acquisition Process, 12 December 2005
SMCI 63-1201	Assurance of Operational Safety, Suitability and Effectiveness for Space and Missile Systems 1 April 2004
SMCI 63-1205	Space System Safety Policy, Process, and Techniques, 20 August 2007

Specifications and Standards

AFSPCMAN 91-710	AFSPCMAN Range Safety User Requirements Manual, Volumes 1–7, 1 July 2004
MIL-STD 882C	System Safety Program Requirements, 19 January 1993

Handbooks

TOR-2006(8506)-4494	Space Vehicle Systems Engineering Handbook, 31 January 2005
TOR-2006(8546)-4591	Space Vehicle Test and Evaluation Handbook, 6 November 2006

Air Force System Safety Handbook, July 2000, Air Force Safety Agency, Kirtland AFB, New Mexico

Guide to Development of the Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE), May 2004, Space and Missile Systems Center

Deliverables

DI-SAFT-80100A	System Safety Program Plan (SSPP), 19 January 1993
DI-SAFT-80101A	System Safety Hazard Analysis Report, 19 January 1993

DI-SAFT-80102A	Safety Assessment Report (SAR), 19 January 1993
DI-SAFT-80103A	Engineering change proposal systems, 19 January 1993
DI-SAFT-80104A	Waiver or deviation system safety report, 19 January 1993
DI-SAFT-80105A	System safety program progress report, 19 January 1993
DI-SAFT-81299A	Explosive hazard classification data, 19 January 1993
DI-SAFT-81300	Mishap Risk Assessment Report, 19 January 1993

Other

AERO-LL-0001	Lesson Learned 1, TOR-2005(8617)-4204, 100 Questions for Technical Review
AERO-LL-0089	Lesson Learned 89, TOR-2005(8617)-4204, 100 Questions for Technical Review
AERO-LL-0129	Lesson Learned 129, TOR-2005(8617)-4204, 100 Questions for Technical Review

Chapter 18
Software Mission Assurance

Colleen M. Ellis
Computer Applications and Assurance Subdivision
Suellen Eslinger
Software Engineering Subdivision
Leslie J. Holloway
Software Acquisition and Process Department
David Lutton
Computers and Software Division
Karen L. Owens
Software Acquisition and Process Department

18.1 Introduction

18.1.1 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 controls spacecraft attitude, the deployment of complex mechanisms, and 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, 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 space systems has historically been fraught with major problems, including performance deficiencies, extensive software defects, and cost and schedule overruns. This chapter captures the lessons learned over many space system acquisitions and presents the best practices for the acquisition of software-intensive systems.

18.1.2 Purpose of Software Mission Assurance

Adapting the definition of mission assurance (MA) from Chapter 1, **software MA** 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, and in a timely manner, 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[95] performs many of the activities to ensure mission success, so defining the right supplier activities at contract award is critical.

Space system acquisition encompasses the entire life cycle of the system, including concept studies, concept development, preliminary design, complete design, and build and operations. Since most 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 MA within the context of the space system acquisition process.

18.1.3 Chapter Overview

The purpose of this chapter is to provide members of both government and The Aerospace Corporation (Aerospace) program offices (POs), and their Aerospace Engineering and Technology Group (ETG) support, a list from which to choose necessary software MA activities to achieve mission success.

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 software acquisition management plan (SWAMP)[96] to document all software-related acquisition tasks.

[95] See definition of "supplier" in Section 18 2.
[96] Eslinger, S., M. Gechman, D. Harralson, L. Holloway, F. Sisti, "Software Acquisition Management Plan Preparation Guide," TOR-2006(1455)-5743, Rev A, 29 December 2006.

The tasks defined in this chapter represent a complete set of software MA activities that could be performed by government and Aerospace personnel during the life cycle of the system acquisition. The government and Aerospace members of each PO would need to tailor the activities described in this chapter to the risks, requirements, and constraints of the program. The result of this tailoring process would constitute an agreement between Aerospace and the government PO for the tasks that Aerospace will perform. Potential Aerospace MA activities span the scope of all program systems and software engineering tasks—supporting the government activities and ensuring a disciplined application of software principles, processes, and standards by the supplier after contract award. This agreement could be captured in a document that is referred to as the mission assurance plan (MAP).

The MAP for software describes the MA activities and tasks to be performed, and the roles and responsibilities of the participants. The activities required to develop the plan are to understand and characterize the environment in which the software development takes place and to define the elements of the plan. Once the MAP is defined and agreed upon, Aerospace will execute according to the plan, make recommendations to the government PO, review results, and improve processes. The MAP should be consistent with the government's integrated master plan (IMP), systems engineering plan (SEP), and SWAMP.

18.2 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 PO.

Acquisition failure: Failure to meet the system's allocated cost, schedule, or technical requirements.

Contract: The legally binding agreement between the "acquirer" and the "supplier." Also, the legally binding agreement between the prime contractor supplier and a "subcontractor" or "vendor" supplier.

Contract data requirements list (CDRL): The contractually required list of the documentation (data) products to be delivered by the supplier to the acquirer.

Mission assurance (MA): 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 plan for activities to be performed by Aerospace personnel in support of a government PO system acquisition, including tasks, resources, schedules, and dependencies. As defined in this chapter, the MAP is limited to software tasks in support of software MA. It should be consistent with the software acquisition tasks defined in the software acquisition management plan. The MAP constitutes an agreement between Aerospace and the government PO for the software tasks that Aerospace will perform. It also describes the roles and responsibilities of the participants.

Mission failure: An unacceptable risk of: (1) loss of life or serious injury to life, or loss of property or serious injury to property; (2) loss, interruption, or degradation of mission capability; or (3) failure to produce a system that meets specified requirements and user expectations.

Mission success (MS)[97]: 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.

Non-functional requirements: Functional requirements define specific behavior or function of a system; non-functional requirements are used to judge the operation of a system. That is, functional requirements define what a system is supposed to *do*; non-functional requirements define how a system is supposed to *be*. Non-functional requirements are often called *qualities* of a system.[98]

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.[99]

Prime contractor: The supplier organization that has a contract directly with the government. The prime contractor may contract with "subcontractors" and

[97]In contrast, acquisition success can be defined in terms of performance, cost, and schedule.
[98]Wikipedia, 2009.
[99]CMU/SEI-2010-TR-033, CMMI® for Development, version 1.3 (CMMI®-DEV), November 2010.

"vendors" to perform part of the technical effort of the contract. This chapter refers to the prime contractor, subcontractors, and vendors as "suppliers."

Program office (PO): The government organization responsible for acquiring the system. It is made up of government, Federally Funded Research and Development Center (FFRDC), systems engineering and technical assistance (SETA), and systems engineering and integration (SE&I) personnel.

Software: Computer programs, procedures, data, and possibly documentation pertaining to the operation of a computer system.[100]

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 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 government, FFRDC, SETA, and SE&I personnel. The members of the software acquisition team do not necessarily 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 software 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: The application of a systematic, disciplined, quantifiable approach to the development and operations and support of software; that is, the application of systems engineering to software. Typical software engineering tasks include analyzing the system requirements allocated to the software, developing the software requirements, developing the software architecture, designing the software, implementing the software in the code, integrating the

[100]Defense Acquisition University, Glossary of Defense Acquisition Acronyms and Terms, Defense Acquisition University Press, 2005.

software components, and testing the software to verify that the software satisfies the specified requirements allocated to the software component of a system or subsystem. It may also include management issues such as directing program teams, scheduling, and budgeting.[101]

Software-intensive system: A system is defined to be a software-intensive system (SIS) if: (1) the system depends upon software to provide essential mission capabilities; and (2) the software poses an appreciable risk of causing a negative impact on the program, where this risk includes both acquisition failure and mission failure.[102]

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 government, 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, or in addition to, 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 that has a contract with a software team member to perform part of the required effort of the program. The prime contractor can have many subcontractors. Subcontractors can also have subcontractors. Also known as a "supplier."

Supplier: A person or organization that enters into a contract with the acquirer, or another of the software team members, to supply 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 with the government (the prime contractor) to develop and deliver products.

Sustainment: Sustainment begins with the transition of the system to maintenance, and concludes with retirement of the system.

---

[101] Ibid.
[102] SMC Software Acquisition Working Group, 2009.

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 Department of Defense Directive 5000.02, "Operation of the Defense Acquisition System." In DOD terminology, the system acquisition life cycle begins in the Materiel Solution Analysis Phase, and ends at the completion of the Operations and Support Phase. Other acquisition organizations have a system acquisition life cycle defined by their specific acquisition policies.

Validation: The process of demonstrating that a product or product component fulfills its intended use when placed in its intended environment

Verification: The process of ensuring that selected work products meet their specified requirements.

18.3 Objectives

The ultimate objective for software MA is that the software product that is part of the operational system supports the MA objectives of the system. Specifically for software, the objectives of MA are to ensure:

- The software product meets all allocated functional, interface, and performance requirements. The verification process ensures that this goal has been met. Verification here refers to all levels of testing, from software qualification test, through subsystem and system qualification test.

- The software product performs as intended in the user's operational environment. The validation process ensures that this goal has been met. Relevant stakeholders participate in the validation process.

- The software product meets the user's expectations for end-to-end operational effectiveness, operability, suitability, and supportability. This goal is verified by test (including inspection, test, demonstration, and analysis) during developmental test and evaluation, validated during operational test and evaluation, and monitored during operations for continued compliance. Users, or their surrogates, participate in the process to ensure these expectations are met.

- The software product meets quality expectations, exhibiting the required dependability, reliability, maintainability, and availability. This goal is verified by test (including inspection, test, demonstration, and analysis) during developmental test and evaluation, validated

during operational test and evaluation, and monitored during operations for continued compliance.

- The software product meets government-specified margins for computer resources (memory, processor speed, etc.) and is sufficiently extensible to accommodate future required system change and growth. This goal is verified by test (including inspection, test, demonstration, and analysis) during developmental test and evaluation, and monitored during operations for continued compliance.

- The software product is sufficiently robust to perform gracefully degraded performance in the presence of anomalous events. This goal is verified by test (including inspection, test, demonstration, and analysis) during developmental test and evaluation, and monitored during operations for continued compliance.

While these objectives are independent of acquisition life cycle phase, the specific practices and tasks to meet these objectives vary throughout the acquisition life cycle as described in Section 18.6 and in TOR-2006(8506)-5749, "Mission Assurance Tasks for Software."

18.4 Practices

18.4.1 Core Activities

This section provides an overview of the best practices for software MA, organized by space system acquisition phases. For detailed definitions of each of the tasks introduced in this section, refer to TOR-2006(8506)-5749, "Mission Assurance Tasks for Software."

Figure 18-1 illustrates the roles and responsibilities for the acquirer, supplier, and Aerospace in performing system acquisition, design, development, integration, test, transition, operation, and maintenance. Aerospace roles include acquisition support to the government on software-related 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.

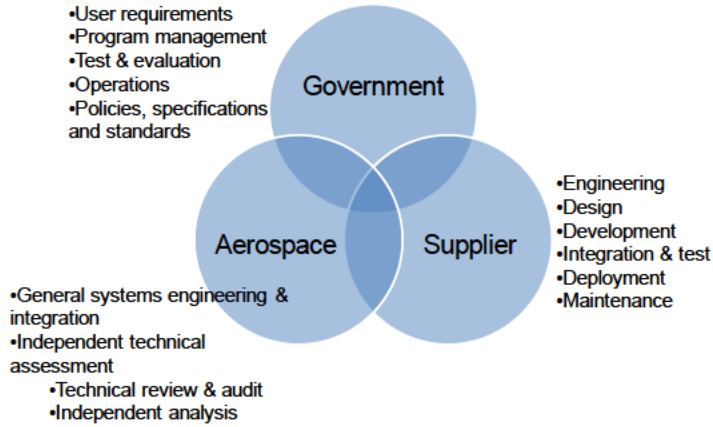


Figure 18-1. Organizational Roles and Responsibilities

18.4.1.1 Acquisition Support to the Government

Acquisition support could include any activity described in *SMC FFRDC User's Guide*. The MAP would describe those activities that enhance software quality to meet the objectives of Section 18.3. 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, or evaluating software architectures
- Reviewing or developing software cost and schedule estimates
- Assisting in the creation of the software acquisition management plan (SWAMP)[103,104]
- Assisting in the creation of the software process improvement (SWAPI) implementation plan
- Assisting in the identification of software risks for the program
- Advising on software specifications, technical standards, software deliverables, software metrics, and software reviews to be included in the RFP

[103]Eslinger, S., M. Gechman, D. Harralson, L. Holloway, F. Sisti, "Software Acquisition Management Plan Preparation Guide," TOR-2006(1455)-5743, Rev A, 29 December 2006.
[104]SMCI 63-104, "Software Acquisition Instruction," 26 May 2009

- Advising on and evaluating software elements of proposals during source selection
- Evaluating software supplier process capability, both during source selection and for contract monitoring

Similar activities would be performed post-contract award for changes due to requirements modifications or additions, or programmatic revisions.

The supplier performs many activities to ensure mission success. It is, therefore, important to include MA activities for software in the contract. Table 18-1 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 TR-2006(8550)-1, "Software Acquisition Best Practices for the Early Phases."

Table 18-1. Pre-Contract Award Activities

Activity	Mission Assurance Tasks
Establish program baseline	• Include software in system functional, non-functional, and performance requirements • Perform software-related trade studies, including space-ground requirements allocation • Determine realistic, independent baseline software effort and schedule estimates • Write a MAP for software • Write a SWAMP[105,106] • Write a SWAPI implementation plan[107]

[105]SMCI 63-104, "Software Acquisition Instruction," 26 May 2009.
[106]Eslinger, S., M. Gechman, D. Harralson, L. Holloway, F. Sisti, "Software Acquisition Management Plan Preparation Guide," TOR-2006(1455)-5743, Rev A, 29 December 2006.
[107]SMCI 63-103, "Software Acquisition Process Improvement Instruction," 28 May 2009.

Activity	Mission Assurance Tasks
Obtain contractual insight	• Require key software technical and management deliverables[108,109] • Require timely electronic access to all software products • Require software-level technical and management reviews • Require software metrics for schedule and progress, resources and cost, product size and stability, product quality, and development performance[110,111] • Require a software supplier process capability appraisal as part of the proposal and periodically after contract award[112, 113]
Obtain contractual commitment	• Mandate compliance with a robust full life cycle software development standard[114] • Require supplier commitment to the software development plan (SDP) • Require software supplier commitment to process maturity and process improvement
Select capable supplier team	• Perform a software supplier process capability appraisal as part of the source selection[115,116] • Evaluate the software architecture component of the system design • Evaluate realism of software sizing, effort, cost, and schedule in the proposal

[108]Owens, K. L. and J. M. Tagami, "Recommended Software-Related Contract Deliverables for National Security Space System Programs," TOR-2006(8506)-5738, 14 February 2008.
[109]Owens, K. L. and J. M. Tagami, "Recommended Software-Related System Engineering Contract Deliverables for National Security Space System Programs," TOR-2008(8101)-5738, 27 June 2008.
[110]Abelson, L.A., R.J. Adams, S. Eslinger, "Metrics-Based Software Acquisition Management," TOR-2004(3909)-3405, May 2004.
[111]Abelson, L., et al., "Software Measurement Standard for Space Systems," TOR-2009(8506)-6, 5 May 2011.
[112]CMU/SEI-2010-TR-033, "CMMI® for Development," Version 1.3 (CMMI®-DEV), November 2010.
[113]CMU/SEI-2011-HB-001, "Standard CMMI® Appraisal Method for Process Improvement (SCAMPI℠)," Version 1.3, Method Description Document (MDD), March 2011.
[114]Adams, R. J., et al., "Software Development Standard for Space Systems," TOR-2004(3909)-3537B, 11 March 2005.
[115]CMU/SEI-2010-TR-033, "CMMI® for Development," Version 1.3 (CMMI®-DEV), November 2010.
[116]CMU/SEI-2011-HB-001, "Standard CMMI® Appraisal Method for Process Improvement (SCAMPI℠)," Version 1.3, Method Description Document (MDD), March 2011.

Activity	Mission Assurance Tasks
Provide contract management tools	• Provide contract incentives for software quality, not just cost and schedule • Mandate periodic team software capability appraisals performed by the government • Require a system for collection, reporting, analysis, and tracking of corrective actions

18.4.1.2 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. It is important to note that the government only has a contract with the prime contractor. The prime contractor may have many contracts with their suppliers, but the government has no contractual relationship with these lower-level suppliers. It is the responsibility of the government to ensure that all contract clauses between the government and the prime contractor have been correctly flowed by the prime contractor to all their suppliers.

A new area of concern in the space systems acquisition and development environment is the increasing use of non-developmental software items (NDI). NDI software includes commercial off-the-shelf (COTS), government off-the-shelf (GOTS), re-use, and open source software. The use of NDI is intended to decrease the amount of newly developed software, and, therefore, to decrease cost and schedule. The use of NDI, however, is not without risk.

The first risk is that the contractor does not use defined criteria to select NDI software. To be appropriate for use, NDI software should closely meet the software requirements, have been developed to be reused, include needed data rights, have reasonable license fees, and be maintainable for the life of the space system. NDI software is not free; it costs to purchase the software, to install the software, to configure the software for the application, and to maintain the software for the life of the system. Obtaining the appropriate data rights to NDI software can also be costly. Whether these costs are, in fact, less than the cost of developing the software is a subject for a trade study.

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 18-2.

Table 18-2. 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 on the contract.
Fee structure and incentive plan	The fee structure (e.g., fixed price, cost plus) and incentive plan (award fee, incentive fee) determines the supplier's financial incentives. Ensure that software-specific incentives are based on quality as well as cost and schedule.
Specifications and standards	Specifications and standards include requirements that increase MA. These may include government, commercial, and other specifications and standards. For software, the recommended specifications are documented in TOR-2004(3909)-3406, "Recommended Software Standards for Space Systems," with the addition of TOR-2004(3909)-3537B, "Software Development Standard for Space Systems," and TOR-2009(8506)-6, "Software Measurement Standard for Space Systems."
Contract data requirements list (CDRL)	The CDRL identifies all data items to be delivered. These are the major products that must be reviewed by the government for technical content and quality. Recommended software CDRLs are in TOR-2006(8506)-5738, "Recommended Software-Related Contract Deliverables for National Security Space System Programs," and TOR-2008(8101)-5738, "Recommended Software-Related System Engineering Contract Deliverables for National Security Space System Programs."
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

Contract Element	Mission Assurance Implications
	contractor and any subcontractor organizations. The organizational structure provides insight into informal meetings that may be opportunities for technical review. See TR-2006(8550)-3, "The Position of Software in the Work Breakdown Structure for Space Systems," for software modifications to the standard WBS for space systems.
Technical and management reviews	The supplier's integrated management plan (IMP) should be made part of the 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 technical reviews are opportunities for reviewing the technical baseline. Management reviews provide an opportunity to review cost, schedule, and risk. The content of reviews for space systems is defined in TOR-2007(8583)-6414, Volume 1, "Technical Reviews and Audits for Systems, Equipment, and Computer Software."
Electronic environment	Many suppliers will consolidate their documentation in a single electronic repository. Ensure that all program office members (government, FFRDC, SETA, and SE&I) have access to this repository. Ensure that the government has all the software tools necessary to access the products in the repository.

18.4.1.3 Technical Review

Technical review refers to review of the work products of the suppliers who are developing the software. Government and Aerospace personnel are responsible for review of the 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 18-3 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 18-3. Plans, Procedures, Processes, and Products for Technical Review

Review Opportunities	Items to be Reviewed	Review Tasks
Plans	Software development plan(s), 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, completeness, and feasibility of the plans. Ensure that plans adequately document the selection, implementation, test, installation, and maintenance of non-developmental items (NDI).
Procedures	Software test procedures for all software items for all levels of testing, particularly software qualification testing.	Review procedure documentation for consistency with standards and associated processes and for the technical correctness and completeness of the procedures. Ensure procedures provide complete coverage of all requirements.
Processes	Project planning and oversight, software development environment, system and segment requirements definition, system and segment architecture, system and segment design, software requirements definition, software architecture, software design, software implementation and unit testing, unit integration and testing, software item	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 rigorous and systematic

Review Opportunities	Items to be Reviewed	Review Tasks
	qualification testing, software-hardware item integration and testing, system and segment integration, system and segment qualification testing, preparing for software transition to operations, preparing for software transition to maintenance, software configuration management (CM), software product evaluation, software quality assurance, software change control and 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 software team members, project process improvement.	fashion using the Software Engineering Institute's Capability Maturity Model Integration (CMMI®)[117] and the standard CMMI® appraisal method for process improvement (SCAMPI℠)[118].

[117]CMU/SEI-2010-TR-033, "CMMI® for Development," Version 1.3 (CMMI®-DEV), November 2010.
[118]CMU/SEI-2011-HB-001, "Standard CMMI® Appraisal Method for Process Improvement (SCAMPI℠)," Version 1.3, Method Description Document (MDD), March 2011.

Review Opportunities	Items to be Reviewed	Review Tasks
Products	Software engineering analysis products, operations concept products, requirements products, architecture products, design products, testing products, training products, maintenance products, operations products.	Review documentation for consistency with standards and for technical correctness and completeness of the products. Ensure that products adequately document the selection, implementation, test, installation, and maintenance of non-developmental items (NDI).
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 data and test results, follow up regression testing to closure.
Software Readiness Assessments	Software build-level products that are ready to be passed to the next phase of the software development life cycle.	Participate in a contractor or government-led readiness assessment of the software build as defined in TOR-2011(8591)-20, "Space Segment Software Readiness Assessment." Determine whether the software build-level product is sufficiently mature to proceed to the next phase of development or milestone.

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"[119], so review of processes is of particular importance in MA for software.

18.4.1.4 Independent Analyses

Independent analysis refers to work that Aerospace personnel perform independently of the supplier. Aerospace personnel perform independent analyses at the request of the government PO, or on their own initiative, to supplement supplier activity or to support or refute results of supplier activity. Table 18-4 lists some typical analyses that Aerospace personnel may be called upon to perform in support of assessing software MA.

Table 18-4. 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 supplier's software engineering organization participates in the system risk assessment process and software risk assessment is part of that process. Aerospace personnel may perform an independent assessment of the program's software-related 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 supplier's software engineering organization participates in the system requirements analysis process, and software requirements analysis is part of that process. Aerospace personnel may perform an independent analysis of the software requirements to determine if they are correct, complete, testable, and verifiable, and whether the requirements traceability is correct and complete.

[119]Paulk, Mark C., Charles V. Weber, Bill Curtis, Mary Beth Chrissis, et al., *The Capability Maturity Model for Software Guidelines for Improving the Software Process*, Addison-Wesley, 1994, p. 8.

Analysis	Description
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 personnel may perform independent modeling and analysis to validate the supplier's models. Aerospace personnel may also perform modeling and analysis on a variety of topics, independent of the contractor.
Specialty engineering	System requirements for dependability (reliability, maintainability, and availability), safety, and security apply to both software and hardware. Aerospace personnel 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 dependability, modeling, and prediction, dependability measurement, functional and software safety analyses, failure modes and effects analyses, failure review boards, trending and summarization, and root cause analyses.
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 personnel 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 personnel may perform an independent analysis of the code, particularly in mission-critical areas, to determine if it will meet allocated system requirements.

Analysis	Description
Dynamic modeling	Many system behaviors can only be revealed through the use of dynamic models. Aerospace personnel can perform dynamic modeling on the supplier's processes to make predictions about the effectiveness of the test program, the length of the test and fix cycle, and other system effectiveness assessments.
Technology readiness	Technology readiness levels measure system and component technical maturity. A low technology readiness level can stop a program from continuing. Aerospace personnel may perform an independent assessment of the technology readiness level for software.[120]
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 personnel 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 personnel participate in several types of independent readiness reviews, including launch readiness reviews, mission readiness reviews, and independent readiness review teams.
Independent program assessments	The government performs independent program assessments (IPAs) in support of every acquisition milestone.[121] Aerospace can provide software expertise for these IPAs. Informal independent review teams (IRT) are also performed between milestones to assess program status. Aerospace can provide software expertise for these ITRs as well.
Independent verification and validation	A role that Aerospace occasionally takes on is that of an independent verification and validation agent.

[120]Air Force Smart Operations -21, "Developing and Sustaining War Fighting Systems, Technology Development-1-12," Software Technology Readiness Assessment Recommendations, 30 April 2009.
[121]DODI 5000.02, Operation of the Defense Acquisition System, 8 December 2008.

18.4.1.5 Develop a Mission Assurance Plan

Once Aerospace's role in the software aspects of the acquisition program is understood, a MAP for software can be developed by the Aerospace program office. The MAP defines the tasks for acquisition support to the government, for technical review of the supplier's and 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's and supplier's program risk assessments should be used to perform the prioritization, using a risk-driven approach.[122] The acquirer's budget and risks determine the resources required.

As a second step, 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's 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.

18.4.1.6 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.[123] Based on the results of the technical review, Aerospace personnel make recommendations to the government PO about any necessary steps that the supplier should be required to perform to improve the quality of its processes or products.

18.4.1.7 Review Results and Improve Processes

Aerospace personnel ensure 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

[122]CMU/SEI-94-SR-001, "An Introduction to Team Risk Management" (Version 1.0), May 1994.
[123]*SMC FFRDC User's Guide*, 20 January 2004.

to ensure timely and economical accomplishment of software development, while maintaining software quality.

18.4.2 Software Mission Assurance Standards and Recommended Practices

The recommended software-related specifications and standards for space systems are documented in TOR-2004(3909)-3406, "Recommended Software Standards for Space Systems," which contains recommended standards for software architectures, configuration management, human systems integration, interoperability and standardization, metrics, safety, security, software life cycle processes, and test.

The primary software standard recommended for MA is the *Software Development Standard for Space Systems*[124]. This standard was developed from best practices in IEEE/EIA 12207[125] and MIL-STD-498[126] and updated to reflect modern software development techniques and to improve MA for software. This standard is recommended for all space system acquisitions.

A new standard that will be recommended for all future space system acquisitions is the Software Measurement Standard for Space Systems[127]. This standard defines the requirements for software measurement collection, analysis, and reporting across SMC space programs. This standard supports the CDRL requirement for a software metrics report.

The new standard for the content of technical reviews is TOR-2007(8583)-6414, Volume 1,"Technical Reviews and Audits for Systems, Equipment, and Computer Software," which defines the software-related entry criteria, content, and exit criteria for the system-level reviews: system requirements review (SRR), system functional review (SFR), preliminary design review (PDR), critical design review (CDR), and test readiness review (TRR), and for the software requirements and architecture review (SAR).

The standard WBS for space systems is documented in MIL-STD-883B, "Military Standard for Work Breakdown Structures for Defense Materiel Items." For software, Aerospace recommends the addition of a software organization at Level 2 of the WBS, for both the government and the supplier. This is explained

[124]Adams, R. J., et al., "Software Development Standard for Space Systems," TOR-2004(3909)-3537B, 11 March 2005.
[125]IEEE/EIA 12207.0-1996, "Software Life Cycle Processes," March 1998.
[126]MIL-STD-498, "Military Standard for Software Development and Documentation," 5 December 1994.
[127]Abelson, L., et al., "Software Measurement Standard for Space Systems," TOR-2009(8506)-6, 5 May 2011.

in more detail in TR-2006(8550)-3, “The Position of Software in the Work Breakdown Structure for Space Systems.”

Guidance for the preparation of the software acquisition management plan (SWAMP) can be found in TOR-2006(1455)-5743, Rev A, “Software Acquisition Management Plan Preparation Guide.”

The recommended software-related deliverables for MA are documented in TOR-2006(8506)-5738, “Recommended Software-Related Contract Deliverables for National Security Space System Programs,” and TOR-2008(8101)-5738, “Recommended Software-Related System Engineering Contract Deliverables for National Security Space System Programs.”

18.5 Software Mission Assurance Lessons Learned

Since the demise of acquisition reform, starting after about 2000, there have been many initiatives to revitalize systems engineering processes to increase mission success. For software, many of the lessons learned before and during acquisition reform have been captured in Aerospace reports and in courses offered at The Aerospace Institute.

Applicable reports include TOR-2004(3909)-3405, “Metrics-based Software Acquisition Management”; TR-2004(8550)-1, “Software Acquisition Best Practices: Experiences from the Space Systems Domain”; TR-2006(8550)-1, “Software Acquisition Best Practices for the Early Phases”; TOR-2006(8506)-5749, “Mission Assurance Tasks for Software”; TR-2000(8550)-1, “Software Acquisition and Software Engineering Best Practices”; TR-2005(8550)-1, “Software Acquisition Best Practices Tutorials”; and TOR-2006(3000)-5391, “Ground Software Study: Roadmap of Recommendations.”

The Aerospace Institute offers a curriculum of software acquisition courses designed for the software professional, including:

- Space Systems Software Project Management (Course No. S4430)
- Space Systems Software Acquisition Management (Course No. S4460)
- Space Systems Software Product Development (Course No. S4470)
- Capability Maturity Model® Integration for Development (CMMI®-DEV), V1.3 (Course No. S4452)
- Software Architecture and Application to Space Systems (Course No. S4440)

The Aerospace Software Acquisition Community of Practice (SACoP), located on AeroLink, provides quick access to relevant news, references, tools, training, and upcoming events, organized around the topics of modeling and simulation, policy and standards, software acquisition, software development, and software mission assurance. Many of the documents referenced in this chapter can be found on the SACoP.

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 national security space (NSS) programs[128] 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, jointly managed by the acquirer and the supplier.

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.[129,130]

[128]Kerner, J.S., et al, "Ground Software Study: Roadmap of Recommendations," TOR-2006(3000)-5391, 30 June, 2006.
[129]CMU/SEI-94-SR-001, "An Introduction to Team Risk Management" (Version 1.0), May 1994.
[130]Neitzel Jr., A. C., "Managing Risk Management," *CrossTalk*, July 1999.

18.6 Software Mission Assurance Task Execution by Phase

18.6.1 Overview

The following two sections discuss the relationships among the system acquisition life cycle, software acquisition life cycle, and the supplier's software development life cycle. They are intended to assist the reader in mapping the detailed software MA tasks to the system acquisition phases.

MA tasks for software are recommended below for all acquisition life cycle phases, using appropriate software life cycle models as illustrated in Figures 18-2 and 18-3. These recommended MA tasks are equally applicable, with appropriate tailoring, to any of the software development life cycle models and the tasks would be selected based on the risks, requirements, and constraints of the program.

18.6.2 Software Development Life Cycle Models

Modern software is developed incrementally and iteratively, using different approaches or life cycle models, depending on the risks, requirements, and constraints of the program, as well as the maturity of development processes in the supplier organization. Incremental and iterative development involves designing, building, and testing some components, followed by additional development stages that augment and correct the earlier stages until the complete product is integrated and tested. Thus, software development is carried out in asynchronous, concurrent streams. At any given time, these streams will be at different levels of maturity, with the potential need for periodic synchronization. This complex software development life cycle needs to be planned in the context of the space system acquisition life cycle phases. Figure 18-1[131] illustrates potential software development life cycle models, with requirements analysis, architecture, design, development, and testing conducted more than once, out of synchronization with the space system acquisition phases.

[131]Hantos, Peter, *Life Cycle Models for the Acquisition and Development of Software-Intensive Systems,* Systems and Software Technology Conference 2005.

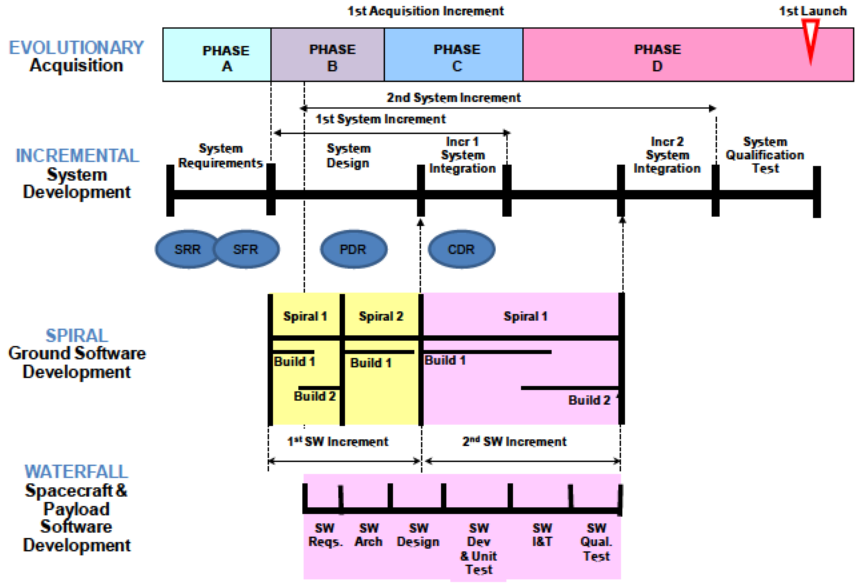


Figure 18-2. Life Cycle Model Complexity

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 development tasks with respect to the space system acquisition life cycle phases and system reviews.

The increments, spirals, and builds shown in Figure 18-2 will not all be applicable in the chosen software development life cycle of a particular program. Each increment, spiral, or build will have requirements, architecture, design, development, and test activities with associated assessment points.

- Software initiation readiness
- Software planning and process readiness
- Software readiness for system requirements review
- Software readiness for system design review
- Software architecture readiness
- Software readiness for preliminary design review
- Software readiness for critical design review
- Software build readiness for each build
- Software readiness for test readiness review
- Build turnover readiness
- Software readiness for pre-ship review

- Software readiness for mission readiness review
- Software readiness for flight readiness review
- Software readiness for transition to operations
- Software readiness for transition to maintenance

In addition, each build will have design walkthrough(s), code walkthroughs, and a qualification test. The number and timing of the tasks and reviews of the asynchronous, concurrent activities that make up the software development life cycle will depend on the risks, requirements, and constraints of the program and the magnitude of the software development effort. Refer to TOR-2011(8591)-20, "Space Segment Software Readiness Assessment"; TOR-2004(3909)-3537B, "Software Development Standard for Space Systems"; and *Life Cycle Models for the Acquisition and Development of Software-Intensive Systems*, Systems and Software Technology Conference 2005, for guidance.

18.6.3 System Acquisition Life Cycle Models

For software, 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 incremental and iterative strategy, where the supplier designs, builds, tests, and delivers multiple increments of the system.

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 events, significant accomplishments, and accomplishment criteria for the program are documented in the supplier's integrated management plan (IMP). The tasks comprising the planned events and significant 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. 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 incremental and iterative model. 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 and assessment.

Figure 18-3 shows the software life cycle periods and events for an incremental and iterative software development life cycle in relation to the system acquisition life cycle.

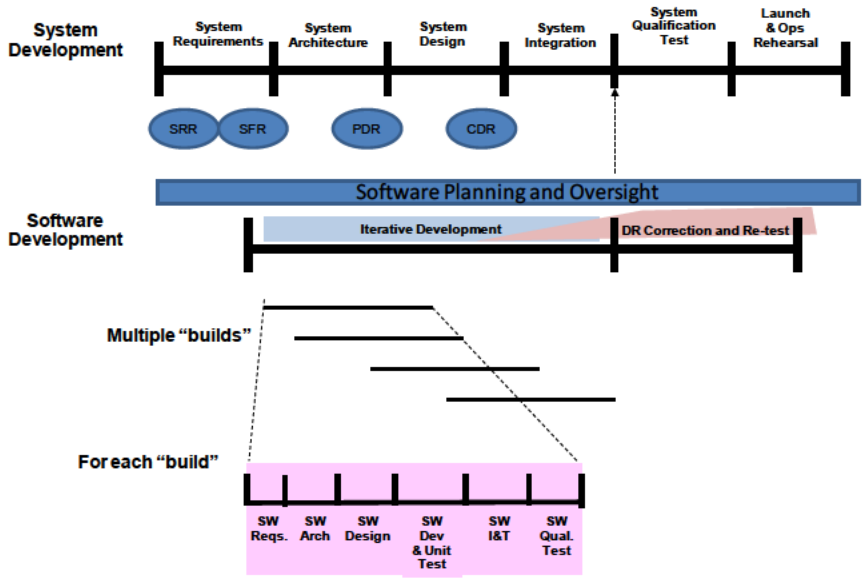


Figure 18-3. Software Life Cycle within the System Life Cycle

Software engineering staff participates in system and subsystem requirements analysis and allocation. The initial software development increment starts following SDR, unless an early software increment is planned for risk reduction. Software requirements analysis and design for early increments might complete before system PDR, and for later increments, after system CDR.

18.6.4 Execution by Acquisition Phase

In Section 18.4, the core mission assurance practices for software were defined. In this section the software mission assurance practices are mapped to the

acquisition phases. Every attempt has been made to make this material consistent with current DOD, Air Force, and SMC acquisition policies. Acquisition policy, however, is constantly changing; therefore the reader is encouraged to consult the most recent policy in conjunction with this material.

18.6.4.1 Pre-Milestone A Phase

Prior to Milestone A, the government PO works with the Joint Capabilities Integration and Development System (JCIDS) requirements process to define the capabilities needed. When the need for a materiel solution has been determined, an analysis of alternatives is performed to assess potential material solutions to meet the capability need, to identify key technologies, and to estimate life cycle costs. A technology development strategy is developed in preparation for Milestone A. Software supports this phase by reviewing the initial capabilities document (ICD), draft capability development document (CDD), system CONOPS, test and evaluation strategy (TES), and the technical requirements document (TRD) for software impact. Software also supports the development of the PO estimate that is submitted to the planning, programming, budgeting, and execution process. Software is responsible for an estimate of the software functionality, software lines of code, software development effort, software development schedule, and long-term software sustainment plan.

The acquisition PO may or may not issue one or more study contracts during this phase. If contracts are to be issued, software supports the development of the RFP, source selection, monitoring, and evaluation of the performing contractors.

During this phase, the acquisition PO begins to develop the program plans and processes that will determine how this program will be executed: the acquisition strategy, the program management plan, the systems engineering plan, the configuration management plan, the risk management plan, the SWAMP[132], and the SWAPI plan[133]. Software is responsible for the development of the SWAMP and the SWAPI. During this phase, the program office may be evaluated on the maturity of their processes, using the Air Force systems engineering assessment model (SEAM)[134], or the CMMI®-based SCAMPI℠ [135]. Software has a major role in preparing the PO for this appraisal.

During this phase the acquisition PO develops the RFP for the subsequent phase. Software supports the development of the RFP by identifying all software-

[132]SMCI 63-104, "Software Acquisition Instruction," 26 May 2009.
[133]SMCI 63-103, "Software Acquisition Process Improvement Instruction," 28 May 2009.
[134]Air Force Center for Systems Engineering, *Air Force Systems Engineering Assessment Model Management Guide*, Version 1, 1 August 2008.
[135]CMU/SEI-2011-HB-001, "Standard CMMI® Appraisal Method for Process Improvement (SCAMPI℠)," Version 1.3, *Method Description Document (MDD)*, March 2011.

related specifications, standards, and deliverables for the program. Software participates in the identification of needed data rights for development and sustainment. Software participates in the development of the requirements and evaluation criteria for the proposal. Software is responsible for performing a capability evaluation as part of source selection, so software identifies the requirements for process evaluation and process improvement for the proposal and for long-term contract monitoring.

18.6.4.2 Phase A

In this phase, the acquisition PO usually has two or more suppliers on contract, developing the system concept. Two major events will be conducted during this phase: SRR and SDR. Software participates in the review of the supplier products and processes leading up to these reviews, and in the evaluation of the reviews. An important software product at SDR is the computer system architecture, including both hardware and software; the government needs to review the architecture products to ensure a sound basis for future software development.

Current acquisition policy emphasizes competitive prototyping in this phase. For software, this may include prototyping alternative software architecture, technology demonstrations, performance studies, and prototyping of user interfaces.

In this phase the suppliers are generally required to develop a draft SDP in the SRR timeframe and a final SDP in the SDR timeframe. These SDPs describe the supplier's plans and processes for software development for the program, including all organizations developing software. These may include the prime contractor and several subcontractors from other divisions of the same company and other companies. This plan is a fundamental document for software development; coordinating software plans and processes across many diverse organizations is a major undertaking for a large program. Review of the SDP and the associated software development processes is a major responsibility of the software members of the acquisition PO.

In addition to managing the supplier during this phase, the acquisition PO is preparing for Milestone B. Software participates in the development of the products required for Milestone B: the acquisition strategy, the system performance specification, the test and evaluation master plan (TEMP), and the integrated program summary (IPS).

18.6.4.3 Phase B

This phase continues the program through system PDR. Software continues to perform contract monitoring on the suppliers and to evaluate the suppliers'

software products, processes, and process improvement. At this point the suppliers should have a software master build plan (SMBP) that describes how the software will be constructed in accordance with the software development life cycle. There should be preliminary software requirements specifications that trace to subsystem or element requirements specifications and software test plans. Key requirements should be allocated to builds.

The suppliers may be conducting prototyping to validate their software architecture and build strategy and to ensure that performance requirements can be met.

During this phase the acquisition PO develops the RFP for the subsequent phase. Software supports the development of the RFP by identifying all software-related specifications, standards, and deliverables for the program. Software participates in the identification of needed data rights for development and sustainment. Software participates in the development of the requirements and evaluation criteria for the proposal. Software is responsible for performing a capability evaluation as part of source selection, so software identifies the requirements for process evaluation and process improvement for the proposal and for long-term contract monitoring.

18.6.4.4 Phases C and D

At Milestone B, the acquisition PO selects a single supplier to execute the design and implementation phase of the program. Software performs contract monitoring on the selected supplier and continues to evaluate the supplier's software products, processes, and process improvement.

During these phases the supplier may be required to conduct an updated PDR to review the design after source selection. Later the supplier will conduct a CDR. Software participates in the review of the supplier products and processes leading up to these reviews, and in the evaluation of the reviews. In addition to the system-level reviews during this phase, the suppliers will be allocating system and subsystem requirements to software, developing the software architecture and design, and developing the software. Prototyping continues during this phase. As discussed above, there are many software processes, products, and reviews associated with the software development life cycle. There may be software build readiness assessments, as discussed in TOR-2011(8591)-20, "Space Segment Software Readiness Assessment." The software members of the acquisition PO are deeply involved with the review and evaluation of these processes, products, reviews, and assessments.

Software test is a major activity during these phases. The software team in the acquisition PO is responsible for the review and evaluation of software test plans, test procedures, test readiness reviews, test execution, and test results.

Software also supports the integration of software into subsystem and system components and the delivery and installation of the operational system.

In addition to managing the supplier during this phase, the acquisition PO is preparing for transition to sustainment. The sustainment contract is often a new procurement, which requires another RFP and source selection. Software personnel participate in the development of the RFP and in source selection for the sustainment phase.

Sustainment includes both operations and maintenance. For software, maintenance involves the identification and repair of defects, product enhancement, and technology refresh.

18.6.5 Execution Planning

As discussed in Section 18.6.2 there is a complex relationship between the system acquisition life cycle activities and the software development life cycle activities. Comparing the core activities in Tables 18-1 through 18-4 with the activities discussed in this section, it can be seen that many of the software MA activities are executed in each of the system acquisition phases with slightly different emphasis. These complex relationships mean that planning the software acquisition activities within the PO is of the utmost importance.

The plans for software acquisition are captured in the software MAP and the SWAMP. It is important to identify software acquisition activities early in the acquisition life cycle and adapt them as necessary to program changes. The references at the end of this chapter can be used to assist in planning activities and evaluating a supplier's performance. It is important to ensure that an adequate number of software engineering professionals are assigned to the program office and that the program office personnel take advantage of the software acquisition expertise throughout Aerospace.

18.7 Government and Contractor Enabling Processes and Products

Performance of software MA tasks after contract award requires: (1) timely access to products and metrics of the supplier team's software development processes, and (2) the supplier team's participation and timely response in reviews and audits that are required to perform the tasks. The means to obtain timely access to supplier data and supplier participation in reviews and audits is the SOW. The SOW is based on the WBS, and describes every task that the supplier must perform and every product the supplier must deliver. The SOW is a part of the contract.

The CDRL, which is also part of the contract, specifies the content, format, and delivery requirements for every product that the supplier must deliver. For a list of recommended software-related system-level CDRL items and software CDRL items see TOR-2006(8506)-5738, "Recommended Software-Related Contract Deliverables for National Security Space System Programs," and TOR-2008(8101)-5738, "Recommended Software-Related System Engineering Contract Deliverables for National Security Space System Programs." These documents provide the purpose and justification of each of the CDRL items, and the identification and tailoring of the data item descriptions (DIDs) used for each CDRL item, including the timing of these CDRL items with respect to major program milestones. They also provide DD1423-1 forms that can be customized to reflect specific program requirements for use on contracts. The CDRL items in these documents are recommended as contract deliverables for all space, ground, and user equipment systems for NSS programs. Putting these CDRL items on contract is one step in the systems engineering revitalization efforts to ensure mission success.

In addition to the products identified in the CDRL, there are process-related tasks that enable software MA. Highly recommended is a contract clause to enable the government to perform periodic software capability appraisals on the supplier team. This helps to ensure adherence to good software development processes. The first such appraisal can be part of the RFP and source selection process and serves to create a baseline for software process improvement. Periodic contract monitoring process appraisals, performed by the government, should be mandated in the contract. The results of these process appraisals, and subsequent process improvement, should be reflected in the supplier's award fee. Aerospace recommends that the capability appraisals be conducted in accordance with the Software Engineering Institute's Capability Maturity Model Integration® for Development (CMMI®-DEV)[136] and use the Standard CMMI® Appraisal Method for Process Improvement (SCAMPI℠)[137] for appraisals.

For support of MA, the SOW and CDRL must specify all tasks and data required on the contract, and provide timely access to all data by the government and their FFRDC, SETA, and SE&I support.

Another important enabling feature for the program is obtaining the appropriate data rights in the contract. The RFP for each phase of the program must establish the government's requirements for data rights to manage the program, to evaluate the products produced on the program, and to maintain the software for the life of the program. As discussed above, the NDI can cause significant data rights issues if they are not clarified early and documented carefully.

[136]CMU/SEI-2010-TR-033, "CMMI® for Development," version 1.3 (CMMI®-DEV), November 2010.
[137]CMU/SEI-2011-HB-001, "Standard CMMI® Appraisal Method for Process Improvement (SCAMPI℠)," Version 1.3, Method Description Document (MDD), March 2011.

18.8 Practice Task Application Example

Section 18.4 introduced the core activities for software MA, including pre-contract award activities, acquisition support to the government, technical review, and independent analyses. Many of these tasks are performed in more than one phase of the system acquisition life cycle; the details of the task will vary depending on the current acquisition life cycle phase, and must be tailored accordingly.

For example, the activity “assess the supplier’s software development plan (SDP)” would probably not be performed prior to Milestone A, because the suppliers would not yet have written their SDPs, nor have their SDPs and processes in place.

In Phase A, the suppliers are generally required to develop a draft SDP in the SRR timeframe and a final SDP in the SDR timeframe. These SDPs describe the plans and processes for software development for the program, including all organizations developing software. This may include the prime contractor and several subcontractors from other divisions of the same company and other companies. The relative maturity of the offerors’ software development plans and processes could be a criterion for source selection, and establish a baseline for subsequent process improvement.

For Phase B, the review of the offerors’ SDPs will be a major activity. At this point in the acquisition life cycle the offerors should have their software development teams identified and have plans and processes in place for the program. The offerors’ software development plans will be more mature at this point in the acquisition life cycle, and differences among the offerers’ software development plans and processes could be a discriminator in source selection.

In Phase C, the supplier’s SDP will continue to mature. It will be reviewed by the government periodically both to ensure the currency of SDPs and processes as well as to monitor compliance with the plans and processes throughout Phases C and D.

The following table is an example of the software MA tasks for assessing the supplier’s software-related development products throughout the life cycle phases.

Table 18-5. Example Tasks for Assessing Contractor Software-Related Development Products

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Contractor Software Requirements							
Verify software requirements and software interface requirements are correct, complete, consistent, feasible, verifiable, and clearly and unambiguously stated. These requirements are usually captured in Software Requirements Specifications (SRSs) and Interface Requirement Specifications (IRSs).			X	X	X	X	X
Assess Contractor Software Requirements Traceability and Allocation							
Verify that the software requirements bidirectional traceability is documented, complete, and up to date, and that all software requirements are completely and correctly traced to and from parent and child requirements. Verify that all software requirements are allocated to and trace to the appropriate software design and code element(s).			X	X	X	X	X
Assess Contractor Software Requirements Verification Matrix							
Verify that the software requirements verification matrix is complete and up to date, and that all software requirements will be completely and correctly tested or otherwise verified.			X	X	X	X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Contractor Software Architecture Description and Views							
Verify that the software architecture products are documented, up to date, complete and feasible, and support the implementation of the requirements allocated to software. Ensure that the baseline software architecture is consistent with and supports the system-level architecture. Ensure that the software architecture views, including the Physical, Logical, Developmental, Process and Behavioral (User) Views are up to date, correct, complete, consistent, feasible, clear, and unambiguous. Assess that the software architecture has been defined to the standards and level of completeness called for in the SDP.			X	X	X	X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Contractor Software Design Description							
Verify that that the software design description, including design description of the software interfaces, is documented, up to date, and that the software design description addresses all software items (including legacy, reuse, COTS, GOTS, other NDI software items) needed to meet requirements specifications. Ensure that the software design reflects the software architecture, and is complete, feasible, and will implement the requirements. Assess that the software design has been defined to the standards and level of completeness called for in the SDP.			X	X	X	X	X
Assess Contractor Database Design Description							
Verify that the database design description is documented and describes a complete and feasible design for the database, and that the database design will support the software architecture and design. Assess that the database design has been defined to the standards and level of completeness called for in the SDP. For flight software, of special concern is the database that contains the flight constants.			X	X	X	X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Contractor Use of Legacy/Reuse/COTS/GOTS/Other NDI Products							
Assess that the justification for the use of any legacy/reuse/COTS/GOTS/Other NDI software products in the software system architecture and design is documented, complete, up to date, and contains sufficient detail to support the use of said product. Verify that the documented justifications were based on a robust set of evaluation criteria.	X	X	X	X			
Assess Contractor's Software Test Procedures							
Verify quality and completeness of software test procedures for software unit testing, software integration testing, and software qualification testing. Ensure the software test procedures adequately implement their respective test plans. Ensure software unit testing and software integration testing procedures are recorded in appropriate software development folders, and that software qualification test procedures are documented in accordance with the contract.		X	X	X	X	X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess Contractor's Software Test Reports							
Verify quality and completeness of software testing reports. Ensure software unit testing and software integration testing results are recorded in appropriate software development folders, and that software qualification testing results are recorded in accordance with the contract. Verify that test results of software qualification testing records the verification status of all software requirements and all software interface requirements. Verify that software qualification test records accurately reflect actual testing (as-run test procedures, QA signatures, captured files).		X	X	X	X	X	X

18.9 References

Policy-Related

Air Force Smart Operations -21	Developing and Sustaining War Fighting Systems, Technology Development-1-12, Software Technology Readiness Assessment Recommendations, 30 April 2009
DODI 5000.01	The Defense Acquisition System, 12 May 2003
DODI 5000.02	Operation of the Defense Acquisition System, 8 December 2008
SMCI 63-103	Software Acquisition Process Improvement Instruction, 28 May 2009
SMCI 63-104	Software Acquisition Instruction, 26 May 2009

Specification and Standards

IEEE/EIA 12207.0-1996	Software Life Cycle Processes, March 1998
MIL-STD-498	Military Standard for Software Development and Documentation, 5 December 1994
MIL-STD-883B	Military Standard for Work Breakdown Structures for Defense Materiel Items, 25 March 1993
TOR-2004(3909)-3405	Metrics-based Software Acquisition Management, May 2004.
TOR-2004(3909)-3537B	Software Development Standard for Space Systems, 11 March 2005
TOR-2006(1455)-5743, Rev A	Software Acquisition Management Plan Preparation Guide, 29 December 2006
TOR-2006(8506)-5738	Recommended Software-Related Contract Deliverables for National Security Space System Programs, 14 February 2008
TOR-2007(8583)-6414, Volume 1	Technical Reviews and Audits for Systems, Equipment, and Computer Software, 30 January 2009
TOR-2008(8101)-5738	Recommended Software-Related System Engineering Contract Deliverables for National Security Space System Programs, 27 June 2008
TOR-2009(8506)-6	Software Measurement Standard for Space Systems, 5 May 2011

Handbooks

TOR-2008(8506)-9	Software Acquisition Guide for Space Systems: Pre-Phase A, 30 September 2009

Best Practices

TR-2004(8550)-1	Software Acquisition Best Practices: Experiences from the Space Systems Domain, 30 September 2004
TR-2006(8550)-1	Software Acquisition Best Practices for the Early Phases, 31 January 2006
TOR-2004(3909)-3406	Recommended Software Standards for Space Systems, 5 May 2004
TOR-2006(8506)-5749	Mission Assurance Tasks for Software, 30 April 2007
TOR-2011(8591)-20	Space Segment Software Readiness Assessment, 3 June 2011
TR-2000(8550)-1	Software Acquisition and Software Engineering Best Practices, 15 November 1999
TR-2005(8550)-1	Software Acquisition Best Practices Tutorials, 30 September 2005

Paulk, Mark C., Charles V. Weber, Bill Curtis, Mary Beth Chrissis, et al., *The Capability Maturity Model for Software: Guidelines for Improving the Software Process*, Addison-Wesley, 1994, p. 8.

Other

CMU/SEI-2010-TR-033	CMMI® for Development, version 1.3 (CMMI®-DEV), November 2010
CMU/SEI-2011-HB-001	Standard CMMI® Appraisal Method for Process Improvement (SCAMPI℠), Version 1.3, Method Description Document (MDD), March 2011
CMU/SEI-94-SR-001	An Introduction to Team Risk Management (Version 1.0), May 1994
CrossTalk	Managing Risk Management, July 1999

TOR-2006(3000)-5391 Ground Software Study: Roadmap of Recommendations, 30 June 2006

TR-2006(8550)-3 The Position of Software in the Work Breakdown Structure for Space Systems, 20 December 2006

Air Force Systems Engineering Assessment Model Management Guide, Version 1, Air Force Center for Systems Engineering, 1 August 2008.

Glossary of Defense Acquisition Acronyms and Terms, Defense Acquisition University, Defense Acquisition University Press, 2005

Life Cycle Models for the Acquisition and Development of Software-Intensive Systems, Systems and Software Technology Conference 2005.

SMC FFRDC User's Guide, 20 January 2004

Chapter 19
Information Assurance

Daniel P. Faigin
Information Assurance Technology Department
Michael R. Ware
Developmental Planning and Architectures

19.1 Introduction

The primary purpose of Information Assurance (IA) as a discipline is to ensure that appropriate consideration is given to security engineering principles throughout the acquisition, development, and management of information technology (IT) based systems and services, and their life-cycle operational and support processes, to counter cyber attacks and unauthorized use[138]. The ultimate goal is to ensure that information, systems (including their infrastructure), and network services provided are protected and uncompromised, that accurate information is securely shared with users authorized for that information, and that information and systems and services are available when they are needed. Given the ever-changing cyber threat environment and the continued exposure to insider threats, IA has become a crucial element of mission assurance (MA). MA depends on IA being adequately addressed throughout the system/services' life cycle to ensure that it functions as expected and needed in the face of threats.

Despite our best engineering efforts, large complex space systems will still have residual vulnerabilities during operation that are unknown to the mission owner and system operator. These systems will also have vulnerabilities introduced by humans who misconfigure them or misuse them during the system's life cycle. The IA MA challenge is not only to build space systems that correctly implement all of the requisite IA controls, but to also apply sound security system engineering principles as part of the overall system engineering (SE) process to mitigate some of the potential effects of "unknown" operational vulnerabilities and/or threats. System engineers should always lean towards

[138]Some customers make a distinction between "security" and "information assurance," essentially distinguishing the task of security engineering from the tasks related to assessment and authorization (also known as "certification and accreditation"). This document follows the NIST approach of a unified view of IA, where all the tasks over the lifetime of a system are viewed as significant activities towards overall life cycle risk management. In some organizations, distinct groups of IA subject matter experts (SMEs) perform the "IA" and "security" functions. As the transformational approach gains acceptance, that stovepiping (other than the required certification independence) will be less prominent, as the assessment side gains engineering visibility, the engineering side incorporates a control-based approach into the design and requirements engineering, and both are involved with the complete system life cycle from conception through acquisition and operation to ultimate disposal.

design alternatives that enhance the robustness of IA without disproportionately increasing system cost in an effort to help boost "real-world" MA.

NOTE: The Department of Defense's (DOD's) IA processes are defined in the DOD 8500 series, with the policy in DOD Directive (DODD) 8500.01, the IA controls in DOD Instruction (DODI) 8500.02, and the Assessment, Risk Acceptance and Authorization to Operate process (a process commonly called Certification and Accreditation [C&A]) in DODI 8510.01. Both the Intelligence Community (IC) and DOD are in the process of moving to a transformed process that unifies the approach taken for all U.S. government systems, including federal non-national security systems (NSS) as well as DOD and IC systems. This process will use the controls defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3[139] security controls, baselines and assignments provided in Committee on National Security Systems Instruction (CNSSI) No. 1253[140], validation approaches defined in NIST SP 800-53A Rev 1, and the risk management framework defined in NIST SP 800-37 Rev 1, combined with service and organization specific documents. DOD plans to reissue DODD 8500.01 and DODI 8500.02 in early 2012 to implement the guidance contained in CNSSI No. 1253 and reference the NIST SP 800-53 control set. DOD will also be reissuing DODI 8510.01 in mid-2012 to have the overall life cycle risk management emphasis of the NIST "risk management framework (RMF)" defined in NIST SP 800-37 Rev 1. This updated process emphasizes the life cycle nature of risk management (RM), with continuous assessment and monitoring. This chapter primarily reflects the DOD IA processes as of mid-2011, with a few anticipatory nudges towards the transformed process. It is important to note, however, that the new, transformational documents don't apply to DOD acquisitions until DOD issues/reissues directives and instructions that specifically require that these new document be used within DOD or that provide guidance on how their contents will be implemented within DOD.

19.2 Definitions

NOTE: All definitions (except as noted) are based on those in CNSSI No. 4009, IA Glossary, dated 26 April 2010. Some definitions are expanded slightly; these are indicated with †

Accreditation is the "formal declaration by a Designated Approving Authority (DAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards." The DAA is also referred to as the Authorizing

[139]"Recommended Security Controls for Federal Information Systems and Organizations," NIST SP 800-53, Rev. 3, August 2009. Revision 4 will be published in 2012.
[140]"Security Categorization and Control Selection for National Security Systems," CNSSI No. 1253, 15 March 2012.

Official (AO). Once the updated life cycle RMF is in place, "accreditation" will be called "authorization."†

Authentication is a "security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information."

Availability means "timely, reliable access to data and information services for authorized users." Note: This usage differs from the typical engineering view of "availability," which is expressed in terms of mean time between failure (MTBF) and mean time to repair (MTTR). "Availability," in the IA sense, captures the notion that information and systems are accessible and usable when they are needed even during cyber attacks. †

Certification is the **"**comprehensive evaluation of the technical and nontechnical security safeguards of an IS [information system] to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements." Once the updated life cycle RMF is in place, "certification" will be called "assessment."

Compromise is the "disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred."

Confidentiality is "assurance that information is not disclosed to unauthorized individuals, processes, or devices."

Cyber[141] is "a prefix used to describe a person, thing, or idea as part of the computer and information age. Cyber Warfare is defined as a war fighting discipline that integrates instruments of military power to achieve and sustain U.S. superiority in network communication through the integrated planning, execution, and assessment of offensive and defensive capabilities."

Information Assurance is defined to be those "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." IA ensures the correct information is provided to the correct individuals at the correct time and accurate information is shared with those authorized to access it and is available when it is needed. †

[141]National Security Agency (NSA) website (http://www.nsa.gov/about/faqs/terms_acronyms.shtml).

An **IA control**[142] is defined as "an objective IA condition of integrity, availability, or confidentiality achieved through the application of specific safeguards or through the regulation of specific activities that is expressed in a specified format (i.e., a control number, a control name, control text, and a control class). Specific management, personnel, operational, and technical controls are applied to each DOD IS to achieve an appropriate level of integrity, availability, and confidentiality in accordance with Office of Management and Budget (OMB) Circular A-130." A system's **requisite IA controls** are those IA controls required by DOD or government policy—that is, those that would be called out by the baseline appropriate for the categorization of the system—that have then been tailored based on the system's threat environment, and subsequently incorporated into the system's statement of requirements.

Integrity refers to the "quality of an IS reflecting the logical correctness and reliability of the operating system and other underlying mechanisms; the logical completeness of the hardware (HW) and software (SW) implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security model, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information." Integrity helps to ensure that information provided to an end user has not been maliciously altered. †

Nonrepudiation is "assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data."

A **Vulnerability** is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source."

19.3 Objectives

The objective of IA is to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. By doing so, IA contributes to MA by developing systems that can operate through disruptions or attacks (intended or not), ensuring that critical information systems and services are not compromised (in terms of confidentiality, integrity, or availability), and countering the threats that may be faced by the system (including computer-based ("cyber") threats as well as other external and internal threats) throughout the life cycle of the information system or service. This starts by ensuring that an appropriate IA requirement set for the anticipated threat environment is captured in the system requirements documents (SRDs) and concept of operations (CONOPS). The majority of IA

[142]DODD 8500.02, "Information Assurance (IA) Implementation," 6 February 2003, page 20.

requirements are derived from federal or national-level laws, policies, directives, and instructions that are interpreted and supplemented at the DOD or Director of National Intelligence (DNI) level and at lower organizational levels.[143] These derived IA requirements are tailored (with appropriate approvals) to address mission-unique IA requirements that are derived from the system's required mission capabilities; CONOPS; intended operational environment and users; system threat assessment report (STAR) or equivalent; and other considerations. The process continues throughout the system life cycle as IA concerns are integrated into the regular requirements feedback process, ensuring that systems are engineered, operated, and maintained to continually meet their IA requirements.

19.4 Practices

19.4.1 Core Activities

The following are key IA tasks, in no particular order:

- Ensure that an IA Strategy, IA Architecture, Program Protection Plan (PPP), IA Plan, and an IA System Security Plan and Security Assessment Report (under Defense Information Assurance Certification and Accreditation Process [DIACAP], these form the Certification and Accreditation Package) exists for each system under development. These are foundational documents that are required by law and DOD policies. They guide the planning and implementation of IA in a DOD system.[144]

- Ensure IA requirements are accurate, consistent, unambiguous, and complete. IA requirements must also be consistent with organizational policy, standards, and procedures. Properly identifying all IA requirements includes not only determining the baseline IA control set and tailoring it through the selection of additional compensating and program-specific controls, but ensuring that the additional space-specific communications security (COMSEC) and transmission security (TRANSEC) requirements have been included. Integrating the security requirements engineering with the overall SE process, and doing it early in a program's development, greatly reduces program

[143]The Defense Information Systems Agency (DISA) maintains a website (http://iase.disa.mil) that serves as a portal to IA policies, instructions, guidance, training, subject matter areas, tools, vulnerability information, and other references relevant to DOD missions.

[144]The DOD C&A process (DIACAP) is governed by DoDI 8510.01. The IC's C&A and risk management processes are governed by DNI Intelligence Community Directive (ICD) 503 and NIST FIPS 200, respectively. The U.S. Civil sector (non-national security) is governed by NIST SP 800-37, Rev. 1, and FIPS 199. Note that national security systems are in the process of moving to the NIST SP 800-37, Rev. 1/NIST SP 800-53, Rev. 3 model, as interpreted by CNSSI 1253.

risks because integrated early engineering is both cost effective and functionally more effective. Trying to add IA capabilities into a system after the system is designed or built is very difficult and expensive, and often leaves unintentional vectors for attack.

- When cryptographic mechanisms are used, establish support agreements with the AF Electronic Systems Center (ESC), Space COMSEC Directorate (HNCS) (formerly CPSG/ZJ) and the National Security Agency (NSA).[145] NSA must be involved in the selection and approval of any cryptographic devices or techniques used; the development and approval of cryptographic key specifications and management plans. ESC/HNCS acquires and distributes cryptographic equipment and provide cryptographic equipment maintenance services. ESC/HNCS handles all space cryptographic key material orders, regardless of source of cryptographic material.

- Ensure all critical system SW, firmware, and HW are trustworthy. Significant global supply chain risks exist that can result in the programs unknowingly acquiring system components that are counterfeit or that perform unwanted or malicious functions. Programs must take action to mitigate such supply chain risks especially when acquiring critical system components.

- Identify the need for any Cross Domain Solutions (CDS), and if needed, follow established CDS approval processes. A cross domain solution "provides the ability to access or transfer information between two or more security domains," for example between a Secret-level domain and one that is Top Secret. It is critical to national security that such interconnections are done using approved components and processes to mitigate the inherent security risks. This activity also includes identifying and working to resolve any barriers to mission cross domain needs, such as credential acceptance.

- Ensure that connections to external systems are thoroughly assessed from both an IA and "need to share" information perspective. Accomplishing a mission frequently requires a system of systems (SOS) to support the warfighter or end user to perform all the mission functions required and to share or access mission-relevant information. Therefore, to support MA, an end-to-end IA evaluation of all system interconnections, interactions, and accreditations (authorizations) is

[145]Depending on the agency acquiring the systems, different organizations may be involved with cryptographic acquisition. For notional purposes, this document focuses on DOD and USAF acquisitions. In particular, non-NSS and other U.S. government agencies will be more focused on the cryptographic acquisition processes, such as National Voluntary Laboratory Accreditation Program (NVLAP), provided by NIST.

necessary to evaluate risks and compliance with applicable policies. The current emphasis of the DOD is on this Enterprise view; the NIST SP 800-37/800-39 process similarly emphasizes a multi-tier Enterprise/ Mission-Business Process/Information System view.

- Ensure adequate testing and evaluation of the system to identify IA vulnerabilities and to verify the proper implementation of all requisite IA controls. IA-related testing and evaluation occurs at various points in a system's life cycle. These efforts follow rigorous test plans and enlist the aid of IA experts with special capabilities from outside the program whenever possible (e.g., NSA). Testing of the system to support its formal authorization to operate (accreditation) should be under the direction of an assessment organization (commonly called a certification authority [CA]) that is independent of the program and assigned by the system's designated approving authority (DAA)/authorizing official (AO).

- Evaluate proposed changes to system requirements and CONOPs, and assess their impact on IA-related risks. Specifically, whenever a change is contemplated, evaluate the effect of that change on end-to-end, system, and enterprise IA risks. If IA risks will increase to unacceptable levels, then the cost and schedule impact to mitigate those risks should be considered before committing to the changes.

- Ensure that the status of IA plans, technical progress, deliverables, and approvals are reviewed at each major milestone review. The DAA/AO or their representative should be present and should recommend that the program does not progress to the next acquisition phase if IA risks are considered to be excessive.

- Ensure that the IA posture of operational systems is continually assessed; maintained in proper security configurations; kept up-to-date with needed SW patches; updated to counter new, validated threats as required; regularly verified to contain the required IA mechanisms; and is supported by properly trained personnel using approved IA processes. The security of even very well-designed systems can quickly be obviated by poor operational practices. It is critical to MA that sound IA practices are followed throughout the system's life cycle (e.g., good configuration management [CM], password controls, and external connection management). Also, employing highly qualified IA personnel who can quickly respond to cyber attacks and help maintain system operations through such attacks or help to quickly restore the system afterwards is a major contributor to MA.

As IA moves into the transformational era (that is, the use of the IA control set defined in NIST SP 800-53 Revision 3), many (but not all) of these key IA processes and tasks are captured in the IA control set.

19.4.2 Standards/Recommended Practices

The IA community currently has no formal "standards" as in many other disciplines. There are a number of meta-standards—i.e., catalogs of IA controls or requirements that may be used to assemble compliance documents. The most current control catalog is NIST SP 800-53, Rev. 3; it incorporates all controls defined in DODI 8500.02 and adds a number of additional controls from federal system usage, best practice, and specialized domains. The Common Criteria for Information Technology Security Evaluation is another meta-standard that provides a catalog of functional and assurance requirements used to assess products or product categories. Many of the Common Criteria controls are also found in NIST SP 800-53, Rev. 3.

The entire U.S. government (DOD, IC, and non-national security federal sector) is in the process of transitioning to a single set of "security controls" for IA and a common process for system life cycle risk management (which encompasses the C&A process). These common security controls and risk management process are, or will be defined in the transformational versions of NIST SP 800-53, 800-53A Rev. 1, 800-30 Rev. 1, 800-37 Rev. 1, and 800-39 Rev. 1; CNSSI No. 1253; and upcoming DOD revisions to DODD 8500.01, DODI 8500.02, and DODI 8510.01. It is expected that the publication (or republication) of all documents above along with any necessary supplemental instruction or guidance will be completed by the end of 2012.

The Aerospace Corporation (Aerospace) publishes technical reports that provide information on recommended IA-related practices; for a list of relevant Aerospace reports refer to Section 19.9. It should also be noted that Chapter 7 of the Defense Acquisition Guide (DAG) contains guidance on how to address IA during system acquisitions.

19.5 Key Lessons Learned

19.5.1 Information Assurance Requirements Engineering

IA requirement engineering encompasses two primary tasks. The first of these tasks identifies applicable IA policy and ensures that the engineering and requirements development process complies with the applicable policy. The second task builds on the first by deriving specific IA requirements from applicable policy and then ensuring they are engineered into the system design, and that their implementation is validated. Both of these tasks are part of the

first two steps of the NIST SP 800-37, Rev. 1, Risk Management Framework: Categorizing the Information System and Selection of the Security Controls.

Before actual development begins, the program office (PO) works with the information owner and end users to determine what information is contained in the system; how this information is anticipated to flow through the system; the projected timeline of data flow; and the availability, integrity, and confidentiality needs of that information. This process starts during system concept development. IA SMEs must be involved during the creation of documents such as the capability development document (CDD); the CONOPS; the determination of key performance parameters (KPPs); and the identification of initial capabilities for the initial capabilities document (ICD). The IA impacts are expressed in the system categorization, which in the DOD is currently the mission assurance category (MAC) and confidentiality level (CL) of the system.[146] The IA SMEs provide oversight during this process to ensure that an accurate determination is made regarding the MAC and CL.

Based on the system categorization (which captures the availability, integrity, and confidentiality needs), the PO in consultation with the IA SMEs determine the baseline set of IA controls. These controls should be considered during the analysis of alternatives process to ensure that the controls selected are cost-appropriate for the value of the protected information and do not have an unacceptable impact on mission performance; the trades between mission performance and system security should be coordinated with the authorizing official to ensure the security posture of the enterprise is preserved. The selected IA controls serve as a starting baseline. Mission-unique threats then should be considered to determine additional required IA controls; these mission-unique controls must also address the specific IA requirements for space systems (captured in Committee on National Security Systems Policy [CNSSP] No. 12 and DODD 8581.01) to provide the basic IA framework for the system. Note that some IA controls will be not applicable as the technologies or services they cover are not used by the system under development. IA controls dictated by policy will not be eliminated from the baseline control set just on the basis that the system has no current threat requiring those IA controls. When a required IA baseline control cannot be implemented because of technical or other justifiable

[146]Non-national security systems capture the availability, integrity, and confidentiality needs by determining an impact level (representing worst-case impact) for confidentiality, integrity, and availability, and then using the high-watermark of the impact, using the approach defined in NIST FIPS 199. In the past, IC systems use the notion of Protection Level (PL) defined in DCID 6/3. In the transformational era, national security systems will use the categorization approach defined in CNSSI No. 1253, where there is a distinct impact level of low/moderate/high in each of confidentiality, integrity, and availability. Based on the confidentiality, integrity, and availability impact levels, a baseline set of controls will be selected. At that point, one or more applicable overlays may be applied that add or subtract controls; for space systems, common overlays will be the tactical overlay (for the ground or terminal segment) and the space overlay. The subsequent baseline will then be tailored or supplemented based on specific mission or organizational needs.

reasons, compensating IA controls will be selected and implemented to reduce risks. The resulting set of applicable IA requirements serves to guide the ultimate requirements that are put on contract. Throughout this process, the IA SMEs help to define the IA requirement set and provide objective assessments of the requirements and how they are to be applied.

The IA controls in a system are designed to specifically protect the mission information within the system (protection of the critical items (such as internal algorithms) and critical resources. Identification of these critical items and ensuring they are appropriately protected is the goal of the Program Protection Planning process. Protection of controlled unclassified information and classified information is governed by many DOD and national directives and policies—these directives lead to many of the areas in which IA SME involvement is critical (e.g., requirements development, cryptographic devices, cross domain solutions, threat analysis, and security testing). With respect to the protection of mission information, the IA SMEs work with the information owner to validate the identification of this type of information and ensure its correct classification, and to ensure that the information owner's requirements for protection are captured in the IA controls.

As development of the system commences and the third step of the NIST SP 800-37, Rev. 1, Risk Management Framework (Implement Security Controls) commences, the MA effort turns to assessment of the implementation of IA controls. The IA SMEs work in various integrated process teams (IPTs) and working groups to ensure that correct and effective implementation approaches are chosen that satisfy the requirements of the IA controls and provide appropriate protection. If the cost of implementation and sustainment of the control does not reduce IA risk sufficiently to justify the expense (when balanced against the value of the asset or information), then that IA control may not be appropriate. The IA control trade-off studies should also take into account the impact of IA mechanisms on information flows; system timing parameters; and system functions to achieve the level of MA needed. The IA SMEs should help document the rationale for including, excluding, or modifying IA controls to provide the rationale for the security architecture.

IA SMEs work to keep the program informed of upcoming changes in the IA control set which are dictated by policy changes and evolving threats faced by DOD. On the implementation side, the IA-SMEs confirm that the system-level IA controls are appropriately decomposed into lower-level design specifications to ensure proper implementation in SW, firmware, and HW. The IA SMEs ensure that IA controls have been adequately covered by mission-unique HW, firmware, and SW, and that commercial off-the-shelf (COTS) components have been appropriately and correctly integrated into the system to meet IA requirements.

It is important to remember that IA engineering is part of, and addressed through, the "SE" process. A system without an adequate level of IA (as determined by the system's Authorizing Official and policy/law) will not be capable of meeting its mission requirements any more than if one of the other system engineer specialties were inadequately addressed (e.g., controls or power).

19.5.2 Risk Management/Certification and Accreditation

The last step before a system is turned over and becomes operational is determination of the risk of operating a particular system or service, and acceptance of that risk by the authorizing official. This assessment and authorization process, called C&A under DIACAP, corresponds to Step 4 (Assess) and Step 5 (Authorize) of the NIST SP 800-37, Rev. 1, Risk Management Framework. Assessment (certification) refers to an independent, comprehensive evaluation and validation of the system to establish the degree to which it complies with assigned IA controls based on standardized procedures. For those IA controls that are found to be missing or improperly implemented, the Assessment/Certifying Authority that oversees the system's assessment provides an independent assessment of IA risks by placing each finding or deficiency related to control non-compliance into one of the following three categories:

Category I	Vulnerabilities that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges. An approval to operate will not be granted while Category I weaknesses are present.
Category II	Vulnerabilities that provide information that have a potential to lead to unauthorized system access or activity. Category II vulnerabilities that can be satisfactorily mitigated will not prevent an approval to operate from being granted.
Category III	Vulnerabilities that may impact IA posture, but are not required to be mitigated or corrected for an approval to operate to be granted.

The certifying authority provides the findings of the assessment process along with recommendations to the DAA/AO to support the authorization (accreditation) decision. Depending on the level of residual IA risks in the system and the system's test needs, the DAA/AO will issue one of the following authorizations: (1) Authorization to Operate (ATO)—this is full approval to operate the system; (2) Interim Authorization to Operate (IATO)—this is an approval to operate for a limited period with conditions (e.g., while work

commences to mitigate the excessive IA risks; (3) Interim Authorization to Test (IATT)—this is an approval to operate with non-live data for a limited period for testing purposes; or (4) Denial of Authorization to Operate (DATO)—this is the DAA/AO's judgment when IA risks are so excessive that the risks of operating outweigh the benefits of deploying the system.

Involvement of the IA SMEs is a critical part of the A&A/C&A process supporting both the PO and certification team:

- **Program Office**. IA SMEs support the PO reviews of the A&A/C&A artifacts prepared by the contractor and PO to ensure accuracy and correct assessment of risk. The IA SMEs also ensure that proper verification and validation of controls has been performed (both in terms of compliance with the control validation procedures as well as technical soundness of the validation approach in the system context). The IA SMEs also ensure that the system is actually configured the way it is represented in the documentation and that this configuration is technically sound and appropriate given the mission.

- **Assessment/Certification Team**. Independent IA SMEs[147] from outside the PO support the authorizing official/accrediting authority and assessment/certification team. They review packages received and provide recommendations to the authorizing official/accrediting authority. They also ensure that the approach taken to validate the controls was appropriate, and that the descriptions of the system in the packages are internally and externally consistent and realistic. These tasks are of particular importance for they provides cross-program visibility, thus allowing A&A/C&A lessons learned to flow among and between programs increasing the future potential for mission success.

19.5.3 Threat Analysis

Threat analysis[148] is an essential process that supports MA. Two major documents that drive space system threat requirements are (1) the Capstone threat and (2) the STAR documents. The Capstone is a high-level generic document and the STAR is a system-specific threat document; these documents are generated by the Defense Intelligence Agency (DIA) for large or special

[147]Using different IA SMEs is desirable to ensure independence of the assessment/certification team's review and to eliminate any appearance of inappropriate influence from the PO. While there may be support to the assessment/certification team from IA-SMEs supporting POs, they should not be the lead or primary members.

[148]Note that there are multiple perspectives to threat analysis. One focuses on new and potential threats, and how this might affect the overall system architectures and what controls need to be implemented to mitigate risk. The other focuses on system operations, detecting new specific instances of known threat vectors, such as new malware attacks.

interest acquisitions specified in DODI 5000.02. Both documents identify threats that must be countered. These threats can be countered by proper design of the space system and by operational processes (i.e., CONOPS or tactics, techniques, and procedures (TT&P). IA SMEs must ensure that specific system threats are considered when identifying requisite IA controls, including mission-unique IA controls, for a system. The system specific threats will dictate the generation of additional IA controls necessary for MA and these mission-specific IA controls will be in addition to the baseline controls required by policy for a system. For systems that are not large enough to qualify to have a STAR generated by DIA, IA SMEs must team with the system's mission user representatives, intelligence agency representatives, and PO personnel to develop the equivalent of the STAR by analyzing the Capstone threat document, STARs for similar programs, and other pertinent threat information sources.

19.5.4 Cryptographic Devices

Cryptographic devices and mechanisms are vital to ensuring the confidentiality and integrity of both system information and mission data as well as assisting in non-repudiation and system availability capabilities. Missteps in the acquisition of these devices and mechanisms can create significant schedule delays and cost overruns. The **most important thing** that a PO can do to minimize the risk of cryptographic-related delays or overruns is to ensure that NSA/Information Assurance Directorate (IAD)[149] and ESC/HNCS[150] are aware of and involved with new space system acquisitions from concept development forward, regardless of who is providing the cryptographic devices.

DODD 8581.01 requires the use of cryptography for encrypting and authenticating telemetry, tracking, and commands (TT&C) to space platforms and for encrypting all data generated onboard the space platform that is transmitted to external receivers. Only NSA/IAD certified and/or approved products are permitted to be used to secure classified communications. Any spacecraft that needs TT&C cryptographic capabilities will need space cryptographic flight and ground HW as well as program-specific keying material. It is the responsibility of the PO to acquire cryptographic devices and related material needed for their space system. Cryptographic requirements are coordinated by the PO and the satellite integrator with ESC/HNCS and NSA/IAD. DODD 8581.01 also dictates other cryptographic requirements for space systems used by DOD that contribute to MA.

[149]NSA is the National Manager for Information Security Systems. Among other things, the NSA/IAD is responsible approving the use of each cryptographic device to be used in a specific system for the protection of national security information. NSA/IAD is also responsible for the evaluation and certification of these cryptographic devices and reviewing and approving how they are actually implemented into the system.

[150]ESC, HNCS provides acquisition, engineering, technical, maintenance, and logistic support for U.S. government communications security (COMSEC) equipment used to in DOD and IC space systems.

Cryptographic device acquisition starts in parallel with concept development and requirements definition. Every space program is required to convey their cryptographic needs through the requirements process. PO IA SMEs work with ESC/HNCS and NSA/IAD to define the cryptographic requirements early. The requirements must address cryptographic capabilities needed; system needs and requirements (size, weight, and power (SWaP) radiation hardening, etc; equipment availability; need dates; threats; CONOPS; and the intended operational environment. This process involves the program documenting their HW and key material requirements using ESC/HNCS Equipment and Key Material order forms.

Ongoing communications are critical to the procurement of the cryptographic equipment. The IA SMEs should ensure that ESC/HNCS and NSA/IAD are included in PO and contractor IA working groups to provide the timely exchange of schedule and technical requirements status. IA SMEs will also be working with ESC/HNCS personnel in general forum sessions, and Space COMSEC Requirement Reviews (SCRRs) to review requirements and resolve outstanding issues.

It is also important to note that the specific cryptographic devices and techniques used to protect each and every national security system “must be approved by NSA.” POs should get NSA Cryptographic Algorithm Configuration Management Board approval of their selection of cryptographic algorithms and cryptographic-related design plans early in the system’s preliminary design phase to avoid costly redesigns. At the same time the program should coordinate with ESC/HNCS for the acquisition of the appropriate crypto for the system or advise them that the program is acquiring their crypto through a User Partnership Agreement (UPA) or independent Commercial COMSEC Evaluation Program (CCEP) effort.

Given adequate time ESC/HNCS will fund for the acquisition of the crypto and will provide it to the program at no cost. A number of options are available to POs to manage this process and acquire the necessary cryptographic equipment. In decades past, NSA developed most new space cryptographic devices and the Air Force (AF) funded the NSA-managed production. The cryptographic devices were then provided to the POs as government-furnished equipment (GFE) via ESC/HNCS. Today, there are various options for developing new cryptographic devices or for acquiring cryptographic devices that are already in production.

If a program has IA requirements that dictate the development of new cryptographic devices, its IA SMEs must work with NSA/IAD and ESC/HNCS to determine which of the following approaches will best meet its needs:

1. The preferred approach would be that the PO has Air Force Network Integration Center (AFNIC) and ESC/HNCS develop the cryptographic devices with NSA approval and support without using funding from the PO. This involves having the PO coordinate with ESC/HNCS to have them include the procurement of the cryptographic devices in the Program Objectives Memorandum (POM). Once the devices are produced and certified, ESC/HNCS provides the equipment to the program as GFE.

2. If the PO has needs that dictate that they develop their own cryptographic devices, it can request permission from NSA to do so. If NSA determines that the program's needs and approach are sound, NSA will enter into a UPA under the User Partnership Program (UPP) with the PO for the development of the cryptographic device. In this case, NSA is only responsible for the security aspects of the cryptographic product. NSA will provide cryptographic design guidance and will evaluate and certify the end devices. It is up to the PO to manage the development and production, and arrange for life-cycle support for the devices needed. Note: Equipment developed under a UPA is developed and certified only for that program.

3. In those cases where new development funding is not readily available within either the PO or ESC/HNCS the PO can make new cryptographic needs known to industry. If there is a strong enough business case to do so, a commercial COMSEC vendor may decide to develop the needed, new cryptographic devices and do so with their own funding and at their own risk. The vendor would initiate this development only after it was approved by NSA under the CCEP. The CCEP is similar to the UPP except in this case the vendor (instead of a PO) requests NSA to approve the development effort and to provide cryptographic technical guidance and perform the evaluation and certification. The vendor produces the equipment for sale to ESC/HNCS or directly to the PO after the NSA cryptographic certification is completed. Note: When using CCEP cryptographic devices, transponders, Common Data Links (CDL), or other devices using cryptography, it is important to inform NSA/IAD and ESC/HNCS to process key orders and coordinate among various agencies for support.

4. The PO can request that NSA contract for the development of new cryptographic devices using PO funding and work with ESC/HNCS to ensure life-cycle support for the device. Over the past decade or two, this approach has largely given way to UPAs and CCEPs.

All new cryptographic devices for national security applications must be developed in accordance with NSA specifications contained in NSA's Technical Security Requirements Document (TSRD) and Information Assurance System Requirements Document (IASRD) that are tailored for the specific cryptographic development. Documentation needed by NSA to support cryptographic certification is contained in Agreed Data Requirements List (ADRL) which is part of the TSRD. The PO must ensure that the ADRL items are added to the Contract Data Requirements List (CDRL) for their acquisition.

In some cases where only controlled, unclassified information is being protected, NSA may authorize the development and certification of cryptographic devices under NIST specifications. However, it should not be assumed that this will always be the case; therefore, it is critical to obtain NSA approval in advance of any design or acquisition decisions.

A PO has several options that for acquiring cryptographic devices that are already in production; they are as follows:

1. Buy existing cryptographic devices directly from a CCEP vendor. Note: These devices are usually proprietary; ESC/HNCS and NSA/IAD may not have access to the detailed equipment design and specifications. Therefore, the program will need to work directly with the CCEP vendor to obtain this information. NSA/IAD must pre-approve the sale and use of the CCEP devices for the program and intended system.

2. Provide technical requirements and/or capabilities documents along with in-place dates to ESC/HNCS. ESC/HNCS system engineers will review and recommend solutions in cooperation with logistics and program managers. Typically, requirements need to be identified 2 years in advance of in-place need dates to allow for the ESC/HNCS POM process, procurement contract, and manufacturing lead times. ESC/HNCS will work with the programs to ensure HW delivery. Note that programs may need to provide funds for procurement of Space COMSEC products if ESC/HNCS is unable to fund for the required products.

3. Coordinate with ESC/HNCS for use of equipment from the Space COMSEC Utility Program (CUP). The Space CUP, managed by ESC/HNCS, is a new contingency process intended to meet the cryptographic needs of quick reaction programs such as those under the Operationally Responsive Space (ORS) effort. These quick-reaction programs may have tasking to launch within a few weeks or months from the initial tasking, which would not allow time for the normal acquisition of the Aerospace Vehicle Equipment (AVE) cryptography.

The ORS Office and ESC/HNCS have begun an effort to acquire a small number of space cryptographic devices to hold at the depot for use by these quick reaction programs. Acquisition organizations (such as Space and Missile Systems Center [SMC] and the Space Development-and Test Wing) identify satellite programs needing Rapid Response (providing authorization for the program to proceed). The Rapid Response requirements are identified and ESC/HNCS issues the equipment from the Space CUP shelf stock and along with cryptographic key material to meet validated requirements. Using the CUP requires timely coordination between the parties involved to identify and supply the equipment. Note: Programs may need to provide the funds for procurement of Space COMSEC products if ESC/HNCS is unable to fund for the required products. The program typically will have to order replacement equipment through the normal ESC/HNCS processes.

Each option to develop new cryptographic devices or to acquire existing cryptographic devices has positives and negatives associated with them. PO IA SMEs should work closely with ESC/HNCS and NSA from the very beginning to ensure that the program selects the best options for the program considering all factors. Some of these factors include taking into account cryptographic capabilities needed; system needs; equipment availability; need dates; retirement dates for cryptographic devices; funding available; threats; CONOPs; and the intended operational environment.

The development of new cryptographic devices and the associated cryptographic certification process are “long-lead” items. Success begins and is heavily dependent on complete and accurate system descriptions and CONOPs since this drives the requirements to which the cryptographic devices are developed. IA SMEs serve to facilitate the process, ensuring that the correct documents are provided and that their content is complete and correct, which can provide significant time savings. Note that any changes to the system design or CONOPS may precipitate changes to the cryptographic device design that can greatly extend an all ready long-lead process.

Another aspect of cryptographic device acquisition is cryptographic device testing. Cryptographic certification testing will be done at the contractor’s facility, if the cryptographic device is developed by the space prime or sub-prime contractor instead of being an NSA-developed item. In such cases, the IA SMEs will provide necessary assistance to the certification testing team.

19.5.5 Key Management

Closely coordinated with the cryptographic device development and/or acquisition is the development of the system key management plans (SKMP) to

support their integration and operation within a given space system. The PO and system development contractors in coordination with ESC/HNCS and NSA are responsible for the SKMP. This plan supports the operation of their system as described in the CONOPS, while taking into account all stakeholders involved with the generation, distribution, and management of the program's cryptographic key material. This activity is a critical schedule task. The program should ensure that the key order is placed and validated with ESC/HNCS no later than 120 days before it is required at all COMSEC account locations. The actual generation of the keys occurs at an NSA key production facility.

There is much governance in this area, and IA SMEs work to ensure that the SKMP is developed in accordance with the published policy, but it is the ultimate responsibility of the PO and system developers to create a "workable" and NSA-approvable SKMP. IA SMEs also ensure that the documented approach taken with respect to key management is compatible with the overall system architecture, CONOPS, and key management infrastructure (KMI).

19.5.6 Cross-Domain Solutions

Another long-lead item in system acquisition are CDSs, which mitigate connectivity across different security domains with assured controlled flows of information. Cross-domain requirements are defined in the latest version of CJCSI 6211.02C, and specific cross-domain requirements for AF space systems are defined in AFSPCI 33-202.

The Unified Cross Domain Management Office (UCDMO) (http://www.ucdmo.gov), established in 2006, maintains a list of standard CDS devices approved for use. Programs are required to provide specifications of their CDS needs, and the Cross-Domain Review Board (of which the UCDMO is a member) will attempt to select an already certified device to satisfy a program's CDS needs. If one is not available, the Cross-Domain Review Board will determine if a custom solution must be processed. IA SMEs work to ensure that the cross domain needs are correctly, completely, and adequately represented and assessed, and that the appropriate and current process is being followed. This can significantly smooth the cross domain acquisition task.

The specific cross domain requirements of a program are captured in the cross-domain appendix (CDA), which is the heart of the cross-domain process. This document provides a description of the data that is flowing between the domains and the channels it flows on, sanitization and release requirements, throughput requirements, data labels, and other characteristics. Participation of the IA SMEs in the CDA development process is critical to ensure that the flow's needs are accurately and completely represented. The Cross-Domain Review Board uses the CDA to identify and minimize the risk of operation of a CDS, and to recommend a standard vetted cross-domain device that they believe meets the

program's needs. If no such standard device is available, the UCDMO works with the program to develop and certify such a device. The overall process vets the CDS's operational need and residual risk through a series of government working groups and ensures that only UCDMO-authorized CDSs are deployed.

Numerous groups participate in the CDS process. To streamline a program's interface to the process, combatant commands, services, and agencies each have a cross-domain solution office (CDSO). Staffed with CDS representatives, the office provides a single CDS process point of contact for a program. The CDSO can provide status on how a program's CDS is proceeding in the process, guidance on the process itself, and can field technical and product-related questions. As soon as a program identifies a potential CDS requirement, it should contact its CDSO.

19.5.7 Program Protection

A critical aspect of MS is protection of those critical program aspects (either information or components) that, if compromised in terms of confidentiality, integrity, or availability, could result in significant degradation in mission effectiveness or MS; shortening of the expected combat-effective life of the system; reduction of technological advantage; significant alteration of program direction; or enabling an adversary to defeat, counter, copy, or reverse engineer the technology or capability. Such assets are called Critical Program Items (CPIs), and represent not the mission data the system operates on, but rather items such as unique algorithms, custom SW and firmware implementations, and custom or unique HW production facilities. CPIs might also reflect unique architecture approaches or system components. DODI 5200.39, "Critical Program Information (CPI) Protection within the Department of Defense," requires that these items be identified in a PPP. IA SMEs play a critical role in the development of this plan, providing independent assessment of the criticality of the proposed CPIs. This is significant as each CPI introduces costs aspects for its protection.

Program protection also addresses the issue of global supply chain risks, exploring the risks inherent of using commercial vendors, many of whom source components from providers of unknown trustworthiness. IA SMEs can provide independent review of supply chain risks and recommend risk mitigation measures. IA SMEs can protect vendor and component provider's proprietary information that may be examined in the risk mitigation process. Program protection also requires demonstration that system security engineering has been integrated into the overall system engineering process.

Program protection looks at all aspects of protection in a program's life cycle. This includes protection during development by the contractor and how the contractor protects critical information. It also includes ensuring that adequate

protection mechanisms are in place during operation and sustainment of the system. Note that program protection is much broader than just IT mechanisms: it also includes physical and procedural mechanisms.

Program protection provides one way to adapt to changing threats. Updated threat assessments should result in updates to the PPP, which may identify cases where additional requirements are necessary to provide the information, system, or services. These additional requirements would then be fed back into the requirements engineering process for future updates.

19.5.8 Anti-Tamper

AT is defined as "the SE activities intended to prevent and/or delay exploitation of critical technologies in U.S. systems. These activities involve the entire life cycle of systems acquisition including research, design, development, testing, implementation, and validation of AT measures. Properly employed, AT measures add longevity to a critical technology by deterring efforts to reverse-engineer, exploit, or develop countermeasures against a system or system component." The specific AT approach to be taken is very system and device dependent and can vary widely. AT is used to protect cryptographic components as well as other system components. IA SMEs assist with helping to define the requirements for AT; identify and involve offices and experts that specialize in AT; help assess AT design alternatives; and assess the resulting design for adequacy.

Note that AT is a critical part of PPP. One of the required aspects of a PPP is an AT Plan.

19.5.9 Emanations Security

EMSEC is defined as "protection resulting from measures taken to deny unauthorized individuals information derived from intercept and analysis of compromising emanations from crypto-equipment or an IS." IA SMEs help ensure that the system design is adequate to meet the published guidelines for EMSEC.[151]

19.5.10 Security Testing

Security testing, in a broad sense, is a verification of the mechanisms that ensure that a system can deliver the correct information to the correct individuals at the correct time. This includes verification of the IA controls that ensure confidentiality, integrity, and availability; it also includes verification of specific system security requirements related to confidentiality, integrity, and

[151]DODD C-5200.19, "Control of Compromising Emanations (U)," 16 May 1995.

availability. IA controls have specific validation procedures that must be followed to state that their implementation is compliant.[152] The best approach to security testing is to ensure that these validation procedures are integrated into the test procedures (TPs) used to validate all other requirements contained in the system/subsystem specification (SSS). IA SMEs play a critical role in assessing the adequacy of the testing measures against these validation procedures. They can also provide an independent assessment of IA risk caused by IA control non-compliance; this assessment provides significant information to the certification team. Test plans and procedures need to be written in the early development phases, and testing planned for the component, unit, and system levels. IA functional testing must be integrated into testing activities.

Another part of security testing is the vulnerability and penetration testing performed by government organizations. This testing often finds unpatched and misconfigured systems; if not performed in a timely manner, the findings can result in significant schedule delays. IA SMEs can reduce these delays by providing an independent vulnerability assessment before government testing, thus permitting the contractor to reduce the vulnerability footprint, and to provide an independent pre-assessment of the vulnerability findings. IA SMEs can also assess the adequacy of vulnerability remediation approaches, thus ensuring that the contractor truly understood the vulnerability; has implemented an adequate solution to remediate the vulnerability; and has examined the design to ensure there are no other similar vulnerabilities.

Lastly, controls are not just assessed as a chunk at the end of each authorization/accreditation cycle—they are considered on a continuous basis as part of continuous assessment. This testing and monitoring represents Step 6 of the NIST SP 800-37, Rev. 1, Risk Management Framework, monitoring the security controls. IA SMEs are involved in this monitoring through determination of the controls affected by system changes and assessing the adequacy of the monitoring of those controls.

19.5.11 Sustainment and Integrated Logistics Support

Constantly evolving threats and new vulnerability findings require systems to be updated with security patches and upgrades that mitigate vulnerabilities. The Air Force Integrated Network Operations and Security Center (INOSC) regularly issues notices of mandatory patches to systems to address discovered security vulnerabilities. Although these can easily be applied to pure COTS systems, their application in SOS or large networks of COTS products is complicated,

[152]For the controls defined in DODI 8500.02, the validation procedures are defined at the DIACAP Knowledge Service website. For NIST SP 800-53, Rev. 3, high-level validation procedures are defined in the companion document, NIST SP 800-53A, Rev. 1. NIST is also defining system specific validation cases. The DOD plans to have any DOD specific validation procedures that are required on the DIACAP Knowledge Service website.

requiring assessment and regression testing to both validate compliance and confirm any mission impact is acceptable. Issues that come into play include that different parts of an SOS may operate on different versions of the COTS SW (complicating patching) because of different schedules for block changes (because of external scheduling factors). Such systems may also have to deal with program-unique patches. Implementing concurrent IA changes to several operational sites introduces additional cost, schedule impacts, and risk. IA SMEs provide independent assessment of a program patching strategy, ensuring that system assets are patched as quickly as possible, but in a manner that does not detrimentally affect MA. IA SMEs can also provide independent review of security patch announcements to determine applicability to a program's assets.

For systems still in the development phase, the application of security patches to COTS components of these systems can increase program cost and schedule. Development contracts should be written to specifically address how to handle security patches and upgrades, and to account for the inevitable impacts that they will have.

Another important aspect of sustainment and ILS concerns the acquisition of HW and SW for production and maintenance purposes throughout the system's life cycle. It is important to understand and mitigate global supply chain risks that threaten MA with counterfeit or maliciously altered technology. IA SMEs can help in identifying and assessing program risks and in identifying and validating viable solutions to mitigate those risks.

19.5.12 Cost Estimation for Information Assurance

The field of cost estimation with respect to security impacts is a young one, and techniques are still under development for vetted quantitative approaches. IA SMEs can provide experience and judgment regarding the qualitative impacts to the overall budgeting process as well as recommending reliable costing models that might fit a particular program. In many ways, the most important contribution an IA SME can make is ensuring that the program specifically budgets a reasonable amount for IA-related activities (as required by DODD 8581.01) and that it also budgets for overall SW and design assurance. IA SMEs also have the responsibility to ensure that the budget for IA is not seen as an *extra* cost, but as in integral and necessary cost for the program. It is important to remember when doing this that the organization that pays the cost of building IA into a system is not the organization that pays the cost when the information or availability of the operational system is compromised on the battlefield.

Often, IA is thought of only in terms of the technological and procedural controls it adds to a system. These are important aspects of cost estimation; however, the IA SMEs must ensure that full, life-cycle consideration is given to

all IA-related costs. These costs include analyzing different IA products and technologies; assessing IA acquisition costs; maintaining IA controls (including security updates and patches); supporting IA-related sections of requirement documents, ICD and CONOPS through development and testing; coordinating with IA authorities; physical security; performing IA security reviews; and re-certifications; upgrading IA-related functions in information and network systems, HW and SW; and disposing of protected information and classified equipment. Procedural controls must include the costs of ongoing user education. Some of the costs above are just increments to the typical life-cycle HW and SW operations and maintenance (O&M) costs; others (such as those related to IA-specific devices such as cryptographic devices and boundary protection devices) are specific to IA. In general, it is hard to factor out which costs are attributable to only IA versus those needed for any well-designed system.

Integral to IA is *assurance*. Assurance is not just related to the IA controls: increased assurance (in the general sense) provides confidence that critical system functions (including IA controls) operate as expected over the system lifetime. IA SMEs should ensure that the costs in this area are also adequately considered. These costs include additional documentation, additional training, additional peer review, additional testing, and similar activities. The difficulty comes in quantifying how much additional work is required based on a specified Evaluation Assurance Level or rating.[153] It should be noted that most of these activities fall under the traditional domains addressed by software assurance. IA SMEs must ensure that they are applied to both IA controls as well as to mission-critical, system functions. There are a few IA specific activities such as C&A and cryptographic acquisition that are clearly IA costs.

19.6 Task Execution by Phase

Within the Mission Assurance Baseline (MAB), IA tasks are first assigned to one of the following seven phases:

[153]Such as might be found in the Common Criteria for Information Technology Security Evaluation.

1. Phase 0: Pre-Phase 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

Table 19-1 tasks ensure IA programmatic and technical requirements are adequately addressed throughout the life cycle of the system. The assurance task products can be emails, IOCs, or reports documenting the results of assurance tasks. IA tasks begin in pre-Phase A to ensure that the Request For Proposal (RFP) adequately addresses needed IA activities in the statement of work (SOW), CDRL, data item descriptions (DIDs), and specifications. The primary focus of IA during Phases A through C is to ensure baselines are properly established; CDRLs are completed fully and accurately; and IA is adequately addressed at system requirements reviews (SRR), system design reviews (SDR), preliminary data reviews (PDR), and critical design reviews (CDR) at the system, subsystem, and unit levels with oversight and participation by the DAA/AO and NSA representatives as appropriate. Updating of Phases A through C baselines occurs during Phases D1 and D2 as a result of design changes that were precipitated by corrective actions (CAs) associated with mitigating failures that have occurred during qualification, acceptance, and integration testing at the configured item (CI), unit, subsystem, and system level, or because of changes in threats or CONOPS.

Table 19-1. Key Tasks by Phase

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure potential IA requirements and issues are considered as part of initial planning, studies, and contracts. Categorize the information system and determine the preliminary set of IA controls that will be applicable.	X						

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Assess contractual implementation of IA controls in contract (SOW, CDRL/DIDs, RFP, WBS) to ensure all contractor tasks and deliverables are included, and CM is adequately addressed by the requirements. Evaluate IA infrastructure and implementation to assess IA control implementation. Review SRR and SDR entrance and exit criteria for IA. As appropriate, review SRR and SDR topics to ensure IA is adequately addressed.		X					
Ensure all IA-related CIs are identified. Review PDR entrance and exit criteria for IA. As appropriate, review PDR agenda topics to ensure IA is adequately addressed and IA controls appear to be implemented correctly.			X				
Assess preliminary design audit (PDA) and PDR criteria for IA.			X				
Assess IA-related CDRLs.			X				
Review CDR and PRR entrance and exit criteria for IA. As appropriate, review CDR and PRR topics to ensure IA is adequately addressed and IA controls appear to be implemented correctly.				X			
Evaluate waivers/deviations from IA procedures.				X			
Ensure the CDR agenda addresses IA.				X			
Assess IA-related CDRLs.				X			

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure IA-related CM issues are appropriately resolved through the configuration control process. Identify IA-related risks to mission performance, reliability, suitability, and operability. Ensure functional configuration audit (FCA)/PCAs have appropriate entrance and exit criteria for CM, and the criteria are satisfied.					X		
Assess IA-related CDRLs. Start assessment of IA control implementation and ensure authorization processes are followed.					X		
Review key CM Board issues and evaluate deviations from IA procedures.						X	
Ensure the review agendas address IA and IA waivers/deviations. Review Test Readiness Review (TRR), FCA/PCA, Formal Qualification Review (FQR), and Production Readiness Review (PRR) entrance and exit criteria for CM.						X	
Support independent readiness review team (IRRT) IA activities.						X	
Assess IA-related CDRLs. Continue the control assessment and authorization process.						X	
As appropriate, provide IA assessments and guidance for ground segment and flight SW contract changes (upgrades, block changes), study efforts, and routine operational patches.							X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Ensure security patches and updates are implemented and secure configurations are maintained.							X
Oversee the monitoring of IA control compliance.							X
Ensure operations and maintenance personnel are up to date on IA-related training.							X

For each life cycle phase, the process can be summarized by the following categories:

- **Program planning** includes an evaluation of the contractor's IA plans and staffing to ensure IA is fully integrated with their SE process; and also to ensure they understand the deliverables and extensive interaction needed between themselves, their subcontractors, the system PO technical team, and NSA if any cryptographic devices are being developed.

- **Systems engineering** includes a those tasks to ensure that all IA-related requirements are fully understood in context of the system's intended operational and threat environment; and to ensure the proper allocation and translation of IA requirements to lower-level subsystems and components to achieve the best balance of IA throughout the system considering system constraints and other system functions.

- **Space systems IA** tasks are required to evaluate whether the contractor's IA process at lower levels successfully flow up possible impact of lower-level configuration changes to the space vehicle (SV).

19.6.1 Core Mission Assurance Processes Supported by Information Assurance

During requirement analysis and validation, IA SMEs assist with the development of IA-related requirements for inclusion in the RFP; review of contractor proposals to address IA-related requirements; and assessment of the flowdown of IA requirements to subcontractors.

During design assurance, IA SMEs assist with the assessment of IA-related design plans and their implementation to ensure they are complete and consistent with top-level IA requirements and policies.

During manufacturing assurance, IA SMEs assist with a review of manufacturing plans, processes, and operations to ensure the integrity of critical system parts and components as well as overall system integrity, and to protect against the exfiltration or malicious alteration of national security information of cryptographic components.

During integration test and evaluation, IA-SMEs assist with the review of IA-related test plans; cryptographic device and cryptographic key testing; EMSEC testing; IA certification; and system vulnerability testing.

During operations readiness assurance (ORA), IA assists with the assessment of the operational readiness planning and reviews of the system with respect to IA-related tasks and deliverables; residual system vulnerabilities or IA-related risks; operational IA training; the status of cryptographic devices and cryptographic key needed for operations; and the system's IA A&A/C&A status.

During MA reviews and audits, IA is an agenda item at SRR, PDR, CDR, and flight readiness review (FRR).

19.7 Government and Contractor Enabling Processes and Products

In addition to requiring access to the government's draft and final RFP, and the negotiated contract, the IA team needs access to the contractor's IA plans, guidance documentation, and change documentation across the prime and subcontractors. The IA team will also need unfettered access to the contractors' engineering team at all levels of the program through the active design period, testing, and certification activities. This is even more critical if the contractor is developing new cryptographic devices. Contractor CDRLs for SDR, PDR, CDR, engineering change proposals (ECPs), and end item data packages (EIDPs) are also needed.

Table 19-2. Enabling IA Products

Phase	Government Enabling Products	Contractor Enabling Products
Phase 0	RFP, SOW, CDRL, DIDs, work breakdown structure (WBS)	
Phase A	Final Contract Criteria for SRR and SDR	Completion of IBR, SRR, SDR, IA Plan, Release Plan
Phase B	Entrance/Exit Criteria for PDR	Completion of PDA, PDR Completion of CDRLs
Phase C	Entrance/Exit Criteria for CDR and PRR	Completion of CDA, CDR Completion of CDRLS
Phase D1	Entrance/Exit Criteria for FCA/PCAs	Completion of CDRLS
Phase D2	Entrance/Exit Criteria for System Verification Review (SVR), Manufacturing Readiness Review (MRR), Launch Readiness Review (LRR), FRR, and IRRT	Completion of readiness reviews Completion of CDRLS
Phase D3	Information Assurance Vulnerability Alerts (IAVA)	Contractor ECPs to support upgrades during operations

19.8 Information Assurance Practices Task Application Example

When assessing IA on a program, the first step is to determine what program phase is of interest and where in the PO WBS the IA assurance activities are managed. The appropriate IA SME then assists the PO in determining what IA assurance tasks are needed using this guide as a roadmap. To assist the PO, a standard reference set of IA tasks (Table 19-3) can be tailored to the program class (A, B, C, D). The IA assurance task products are then archived over the life cycle. This assists in the verification of accomplishment criteria associated with major milestones defined in gated processes such as the Integrated Master Plan (IMP).

Table 19-3. Reference Set of IA Tasks

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Review and Verify IA Requirements							
Verify that IA was adequately addressed during concept development efforts	X						
Review STAR or its equivalent for system and assess if the system's IA controls adequately address those threats.			X	X	X	X	X
Review and verify that CDD and capabilities production document (CPD) adequately address IA requirements.		X	X	X			
Verify that information stored, processed, or transmitted by the system was identified, together with the information owner requirements for protection of that information.	X	X					
Assess IA impacts of external and internal interfaces (in particular, looking for potential cross domain interfaces and interfaces that introduce vulnerability risks), to help define boundary protection requirements.		X	X	X	X	X	X
Verify that the determination of the confidentiality, integrity, and availability impact levels (in DODI 8500.02 terms, the MAC and CL) of the system (or equivalent transformational categorization) has been properly made.		X					

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify that all cryptographic functions were identified that are needed for protecting the system and information (during processing, transmission, or storage) based on system requirements, the mission, and IA policies. If any cryptographic devices are needed from ESC/HNCS, ensure coordination with ESC/HNCS and ensure the RFP identifies these devices as government off-the-shelf (GOTS) products where appropriate.		X	X				
Verify that AT and TRANSEC requirements were identified and are appropriate. Verify their incorporation into system requirements and SOWs as appropriate.		X	X				
Verify that IA-related system requirements are adequately traced to ICDs and architecture products (e.g., DODAF products).		X	X				
Verify the participation of operational command(s) in defining IA-related requirements for the mission and system.		X	X	X	X	X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify that the PO is following applicable U.S. policies, instructions, and guidelines in developing and deploying the system. Potentially applicable IA policies include (but are not limited to) DOD 8500-series; DODD 5200.39; DNI ICD 503,CNSSI No. 1253; NIST SP 800-53, Rev. 3, and 800-37, Rev. 1; NIST FIPS 199 and 140-2; and Service or Agency-level implementing instructions for above.	X	X	X	X	X	X	X
Verify that any changes in CONOPs, mission capabilities, system requirements, intended users or operational environment fully consider IA implications (security risks, cost, schedule, etc.) and are approved by the DAA/AO as appropriate.		X	X	X	X	X	X
Verify IA Technology Readiness							
Review IA technologies being considered or needed for developing and fielding the system and confirm their respective technology readiness levels are sufficient to support the program's schedule.		X	X				
Review and Assess Contract-Related IA Activities							
Assess contract RFP(s) for adequacy of addressing IA in system requirements, CDRL/DIDs, and WBS.	X	X	X	X	X	X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify that deliverables, reviews, and communications needed by NSA with the cryptographic device developer(s) under any UPA are reflected in the PO's contract(s).		X	X				
Review and verify contract proposals comply with IA requirements and adequacy of IA staffing proposed.	X	X	X	X	X	X	X
Verify that NSA-approved products used throughout acquisition and operations are protected as required by policy and the product's certification package (e.g., the Security Production Assurance document).			X	X	X	X	X
Ensure the IA activities dictated by policy that developing contractor must comply with are incorporated into the SOW.		X	X				
Ensure the IA documentation dictated by policy that the developing contractor must produce is incorporated into the SOW and contractual deliverables.		X	X				
Review and provide recommendations on RFPs for adequacy of CDRLs specific to IA (e.g., IA Plan) or with IA aspects (e.g., test plan, SW development plan), compliance documents, assessment criteria, and the SOW.		X	X				
Evaluate the contractor's SW assurance plans, activities, and products and verify that they meet contract requirements to meet IA needs.			X	X	X	X	

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify DAA/AO review and approval of the PO's implementation of IA policy in program technical requirements and development contractors' SOWs. Verify other stakeholders included as appropriate.		X	X	X			
For engineering milestones, verify the development of IA pass/fail criteria and determine compliance.		X	X	X			
Review and verify adequacy of contractor system design and process documentation to be incorporated in the C&A information package.			X	X	X	X	
Assess the Technical Requirements Document (TRD) with respect to IA requirements.			X	X			
For each UPA cryptographic device to undergo certification, verify the establishment and mutual understanding of cryptographic device certification requirements in the TSRD with the developing contractor. If ESC/HNCS products are to be used, ensure coordination with ESC/HNCS and that the RFP identifies these GOTS products.		X	X				
Verify NSA/ESC/HNCS Involvement							
Verify that NSA and ESC/HNCS are invited to participate in concept development studies and early system architectural efforts.	X	X					

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify adequacy of Memorandum of Agreement (MOA) between the PO and NSA and/or ESC/HNCS that delineates NSA services needed, funding needed for NSA support, deliverables, milestones, work schedule, reviews, and single points of contacts.	X	X	X	X			
Verify that the PO contacted NSA and ESC/HNCS to identify any GOTS cryptographic devices that meet program needs.		X	X				
Verify that the PO contacted NSA to identify any cryptographic devices to be developed by the PO, and if so, verify that a UPA was initiated.		X	X				
For any GOTS cryptographic units needed, verify that the PO contacted ESC/HNCS to ensure program funding to acquire the cryptographic device and can deliver the cryptographic device when needed or if PO funding is needed.		X	X				
Verify that the PO contacted NSA for assistance with the identification and approval of both cryptographic algorithms and implementation assurances appropriate to meet the system's cryptographic functional and performance needs for its intended user set and operational environment.		X	X				

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify IA/System Engineering Integration							
Verify that all system and segment trade studies identified and fully conveyed IA implications (security risks, cost, schedule, etc.) of potential options.	X	X	X	X	X	X	X
Review system architecture documentation (e.g., DoDAF views) verify incorporation of IA aspects of information flows, component functions, etc.		X	X	X			
Verify integration of IA into system acquisition processes and documentation (includes the Configuration Management Plan, Software Development Plan, Risk Management Plan, System Engineering and Management Plan, and Test Evaluation and Management).		X	X	X	X	X	
Verify proper interpretation and integration of IA requirements within non-IA fields of expertise, including Military Construction (MILCON) (e.g., EMSEC), SW, HW, and networking.			X	X	X	X	X
Verify Mandated Processes (e.g., C&A, Program Protection, Clinger-Cohen) Followed Per Schedule							
Confirm initiation of the mandated DODI 8510.01 process by verifying registration of system with DOD component and assembling the assessment team.		X	X				

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Review and verify DIACAP Implementation Plan (DIP) for completeness across segments within the accreditation boundary.			X	X	X	X	
Verify coordination of schedules and approach captured in the DIP with stakeholders as appropriate (e.g., User Segment DAA/AOs, DAA/AOs of external, interfacing ISs).		X	X	X	X	X	
Verify that the PPP was written and boarded in Phase A.		X	X				
Verify adequate funding and awareness training to protect CPI throughout the system's life cycle as described in the PPP.			X	X	X	X	X
Verify that documentation needed (e.g., IA strategy) for Clinger-Cohen Act is properly completed and submitted.		X	X	X	X		

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify CDS Processes Followed							
Verify that needs and requirements for any CDS have been formally identified. Verify that the PO has contacted and is working with Service CDS Office (single point of contact [POC] for Defense Information Systems Network [DISN] DAAs, Defense IA/Security Accreditation Working Group [DSAWG], Cross-Domain Technical Advisory Board [CDTAB], and DISA SIPRNet Connection Approval Office [SCAO]); has notified the Program Manager, DAA/AO, Certifying Authority, and user representative; and is beginning the CDA.		X	X				
Verify system changes are coordinated with the CDS office.				X	X	X	X
For SIPR/NIPRNet connections, verify appropriate connection approval office approvals (e.g., SCAO) have been coordinated.				X	X	X	
Review the Plan of Actions and Milestones (POA&M) for completeness.		X	X	X	X	X	X
Verify that UCDMO-applicable bodies assess risk and coordinate ATC.			X	X	X	X	X
If a new CDS product is being developed, confirm Pre-Operational Security Control Assessment (previously called Certification Test and Evaluation [CT&E]) testing of CDS and updating of CDA with results.			X	X			

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify mitigation of Pre-Operational Security Control Assessment (previously called CT&E) findings, development of Security Test and Evaluation (ST&E) plans, and updates to the CDA.			X	X	X		
Ensure actions required by POA&M (e.g., vulnerability mitigations, clarification of documentation) are executed on schedule.							X
Verify the coordination of the Cross-Domain Solutions Advisory Panel (CDSAP) and Community Jury review of initial CDA and ticket request and verify PO receipt of ticket number and recommended CDS.			X				
Verify Trustworthiness of Critical Components							
Verify that DOD Trusted Foundries or classified facilities were used to produce mission-critical integrated circuits (ICs), and if not possible, verify adequate steps taken to ensure the trustworthiness of ICs procured.			X	X	X		
Assess Software Development Plan to ensure that it incorporates measures that address SW quality and reduce the likelihood of IA vulnerabilities.			X	X			
Assess software security test planning.	X	X	X	X	X		

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Evaluate the Software Configuration Management Plan to ensure it requires detailed assessment of changes with respect to IA risks.		X	X	X	X	X	X
Verify Approvals and Certifications							
Verify that the PO has obtained NSA approval for all cryptographic devices and technology used in system and also NSTISSP-11 certification where required.		X	X	X			
Verify that all cryptographic devices used are certified in accordance with instructions from NSA.			X	X	X		
Verify the IA accreditations (authorizations) of all external systems to which connected.			X	X	X		
Assess Adequacy of Cryptographic Key Processes, Plans, and Documentation							
Verify that the PO coordinated with ESC/HNCS and NSA during development, review, and validation of the system Key Management Architecture.		X	X				
Verify that the PO coordinated with ESC/HNCS to solicit NSA assistance in Key Specifications development (as needed) and worked with ESC/HNCS to ensure key production meets program schedule.			X	X	X	X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify the development and NSA approval of a Level 1 SKMP for each new cryptographic product used in the system. Ensure there has been appropriate ESC/HNCS coordination with key management and distribution.			X				
Verify the development and NSA approval of a Level 2 SKMP for each new cryptographic product used in the system. Ensure there has been appropriate ESC/HNCS coordination with key management and distribution.			X				
Verify the development and NSA approval of a Level 3 SKMP for each new cryptographic product used in the system. Ensure there has been appropriate ESC/HNCS coordination with key management and distribution.				X			
Verify the development and NSA approval of the SKMP. Ensure there has been appropriate ESC/HNCS coordination with key management and distribution.				X			
Assess IA-Related Risks							
Verify that DAA/AO (or their representative), user reps, NSA, and ESC/HNCS all participate in major design reviews and program milestone reviews to help assess IA-related risks.		X	X	X	X		

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify that the risks associated with using cryptography or IA technology/devices that must be developed or modified to support program needs are fully understood by PO.		X	X	X			
Verify the adequacy of progress of cryptographic and IA device certifications (by NSA, Common Criteria Test Lab [CCTL], Cryptographic Module Validation Program [CMVP], etc.) through product milestones and review boards such as the NSA Technical Review Boards. Assess expediency of processes for resolving disagreements and documentation inadequacies that may cause delays in certification schedule.			X	X	X		
Verify coordination of annual risk assessments involving PO personnel spanning domains of expertise to identify new, reassess/remove existing, update descriptions of, and prioritize CPI described in the PPP. Reviews should be no less frequent than each key decision point (KDP).		X	X	X	X	X	X
Confirm that any CDS tickets are proceeding at an appropriate pace through the UCDMO process.			X	X	X		
Assess Adequacy of IA Resources							
Verify that IA was adequately addressed during the development of any system cost, schedule, or manpower estimates; and that adequate IA resources are programmed.		X	X	X	X	X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify adequacy of contractor's schedule and manpower plans for cryptographic device development, production, and operational support; verify PO and NSA review and approval of documentation needed for NSA certification of program-developed cryptographic devices.		X	X	X			
Verify Adequate IA Testing							
Review and assess the completeness of Requirement Validation Plans for IA requirements against governing IA policy and guidance.			X	X			
Assess the accuracy and completeness of validation and test reports for IA requirements.			X	X	X	X	
Verify coordination of installation of CDS, ST&E, and independent testing, and update CDA with ST&E findings.				X	X		
Verify IA-related functions are included during the ST&E of the system as configured for operations.					X	X	
Verify Adequate Operational IA Processes							
Confirm that there are plans and resources for ensuring operators are adequately trained with respect to IA.				X	X	X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Review and assess for adequacy all documentation for operational processes relevant to IA. Documentation includes (but is not limited to) the Configuration Management Plan, Disaster Recovery Plan, Continuity of Operations Plan, user/administrator manuals, and SW and HW manuals.						X	X
During system operations, verify the accuracy of IA-related system documentation (e.g., network topology, HW baseline, design/implementation changes), currency of COTS products (e.g., implement IAVAs), and the execution of processes (e.g., CM).							X
Confirm that contingency planning has been adequately addressed and is coordinated with the operational command.			X	X	X	X	X
Verify Adequacy of IA Risk Management Processes							
Assess the potential loss or impact from threats that the system cannot currently defend against and verify that the cost of any additional IA controls needed are warranted, and if so, that they are implemented in the system.		X	X	X	X	X	X
Verify that IA risks are identified and tracked through a sound risk management process by the PO.		X	X	X	X	X	X

	Phase						
Task	**0**	**A**	**B**	**C**	**D1**	**D2**	**D3**
Verify IA Lessons Learned Documented							
Verify capture and documenting of IA lessons learned throughout the program life cycle and maintain lessons learned in an appropriate database.		X	X	X	X	X	X

19.9 References

Policy-Related

AFSPCI 33-202 "Information Assurance," 15 January 2009

CJCSI 6211.02C "Defense Information System Network (DISN): Policy and Responsibilities," 9 July 2008

CJCSI 6510.01E "Information Assurance (IA) and Computer Network Defense (CND)," 15 August 2007

CNSSI No. 1253 "Security Categorization and Control Selection for National Security Systems," 15 March 2012

CNSSI No. 4009 "National Information Assurance Glossary," 26 April 2010

CNSSP No. 12 "National Information Assurance Policy for Space Systems Used to Support National Security Missions," 20 March 2007

DAG, version 1.5 "Defense Acquisition Guide," Version 1.5, November 2004

DNI ICD 503 "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," effective 15 September 2008

DODD 8500.01E	"Information Assurance (IA)," 24 October 2002, certified current as of 23 April 2007
DODD 8581.01	"Information Assurance (IA) Policy for Space Systems Used by the Department of Defense," 21 June 2005
DODD C-5200.19	"Control of Compromising Emanations (U)," 16 May 1995
DODI 5000.02	"Operation of the Defense Acquisition System," 8 December 2008
DODI 5200.39	"Critical Program Information (CPI) Protection within the Department of Defense," 16 July 2008
DODI 8500.02	"Information Assurance (IA) Implementation," 6 February 2003
DODI 8510.01	"DoD Information Assurance Certification and Accreditation Process (DIACAP)," 28 November 2007
DODI 8570.01	"Information Assurance Training, Certification, and Workforce Management," 15 August 2004
NTISSIP 11	"National Information Assurance Acquisition Policy," July 2003

Specifications and Standards

NIST FIPS 140-2	"Security Requirements for Cryptographic Modules," 25 May 2001
NIST FIPS 199	"Standards for Security Categorization of Federal Information and Information Systems," February 2004
NIST FIPS 200	"Minimum Security Requirements for Federal Information and Information Systems," March 2006

NIST SP 800-30, Rev. 1	"Guide for Conducting Risk Assessments" (Projected: October 2011)[154]
NIST SP 800-37, Rev. 1	"Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," February 22, 2010
NIST SP 800-39, Rev. 1	"Integrated Enterprise-wide Risk Management: Organization, Mission, and Information Systems View," March 2011
NIST SP 800-53, Rev. 3	"Recommended Security Controls for Federal Information Systems and Organizations," August 2009
NIST SP 800-53A, Rev. 1	"Guide for Assessing the Security Controls in Federal Information Systems," June 2010

Handbooks

TOR-2007(8583)-6699	"Information Assurance Handbook for DOD Space Systems: Space System Acquisition Policy," 8 June 2007
TOR-2007(8583)-6702	"Information Assurance Handbook for DOD Space Systems: Guidance on Application of DOD 8500.01/8500.02 IA Controls," 31 August 2007[155]
TOR-2007(8583)-6703	"Information Assurance Handbook for DOD Space Systems: National Security Agency (NSA) Cryptography," 15 June 2007
TOR-2007(8583)-6704	"Information Assurance Handbook for DOD Space Systems: Certification and Accreditation," 8 June 2007

[154]The NIST SP documents listed represent the "transformational" documents; that is, those documents that reflect the unified risk management approach that will be used by the non-NSS Federal Government, the DOD, and the IC. For those documents not yet published, NIST has the previous non-transformational versions available. The current FISMA Implementation Schedule is available at http://csrc.nist.gov/groups/SMA/fisma/schedule.html.

[155]An equivalent version of this document that addresses the NIST SP 800-53, Rev. 3, is in the publication process.

TOR-2007(8583)-6705	"Information Assurance Handbook for DOD Space Systems: Cross Domain Solutions," 15 September 2007
TOR-2007(8583)-6707	"Information Assurance Handbook for DOD Space Systems: Use of Common Criteria in Acquisitions," 15 June 2007

Deliverables

Crypto development-related documents needed for NSA crypto certification purposes are contained in NSA's ADRL. Other documents should support overall system information assurance C&A will be specified as part of the CDRL for the system acquisition contract.

UCDMO	Unified Cross Domain Management Office, http://www.ucdmo.gov

Other

DCID 6/3

Appendix A1
Definitions/Glossary

Accountability is defined as the obligation or willingness to accept responsibility to account for one's actions through acceptance of specific mission assurance (MA) activities and execution of those responsibilities. In the context of MA, Aerospace accepts and documents accountability for a defined set of activities over the acquisition life cycle to ensure a higher probability of mission success.

Acquirer is the organization responsible for managing the contract that procures the system and 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 evaluated by a government program office/ engineering development team before they are released for mission operations. For the purposes of this guide, activation includes space vehicle activation on orbit, launch vehicle activation after successful completion of launch base processing when judged ready to perform flight operations, and ground system activation after deployment (e.g., the crews are proficient and ready for mission operation).

Assembly consists of structurally integrated and interconnecting hardware, forming a part or module or system. Assemblies cross subsystem boundaries. Examples include solid rocket motor sections, or a bus panel on which several electronic units belonging to different subsystems are mounted, or a ground station equipment rack that demodulates, decrypts, processes, and routes downlinked data for distribution.

Audits are independent inspections of each configuration item 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.

Core mission assurance processes (CMP) implement MA objectives and goals and are usually time and acquisition phase dependent as they are closely coupled with system engineering processes over the life cycle of 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 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.

Hazard is a real or potential condition that directly or through induced effect causes 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-Federally Funded Research and Development Center (FFRDC)/systems

engineering and technical assistance (SETA) team, where Aerospace performs that FFRDC role for national security space (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.

integrated Mission Assurance Tool (iMAT) is the corporately supported asset for tracking and reporting of MA accountabilities and assessments. (Hosts the Mission Assurance Baseline [MAB].)

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 assurance is 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.

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 proven scientific, engineering, quality, and program management principles toward the goal of achieving mission success.

Mission Assurance Baseline (MAB) the corporate, configuration-controlled set of tasks performed to increase confidence toward the goal of achieving mission success for a satellite system and associated ground systems. The set represents activities for all space vehicle (and ground system) mission types across all acquisition and mission phases. This set is based on mission success guidance found in specifications and standards, policy, and other guidance, ETG

expertise, program office experience, industry best practices, and lessons learned.

Mission assurance disciplines are engineering specialty domains that are principally applied in support of MA processes and are implementable across entire program-spans and are associated with the use of a unique, standard set of technical tools/procedures.

Mission assurance execution is a definite phase-sequential order that governs the intended execution of a set of core MA processes. The majority of the tasks under a specific process tend to be concentrated in a particular program phase, 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.

Mission assurance baseline "framework" is the hierarchical structure around which MAB tasks are organized, so that tasks of interest can be easily located. (Sometimes referred to as a tree or folder system to file MAB tasks.)

Mission assurance phases emphasize that MA is an active process throughout a system's life cycle from concept definition to disposal. The phases as defined present unique MA tasks specific to each phase over the life cycle of the system.

Mission Assurance Plan (MAP) is a program office-produced document that provides a structured and consistent communication of program office support within the program office, customer set, and senior management as well as serves as guidance to the personnel in the program office.

Mission Assurance Policy is a policy established by the U.S. Government for applications to NSS systems. These are the Space and Missile Systems Center (SMC)-sponsored "Assurance of Operational Safety, Suitability, and Effectiveness (OSS&E) for Space and Missile Systems" policy and National Reconnaissance Office (NRO)-sponsored "Mission Assurance Implementation" policy.

Mission assurance processes are program-phase dependent and executable via combinations of technical means and procedures.

Mission assurance reviews offer formal and informal opportunities to share detailed technical information characterizing system performance, issues, and risk horizontally across program management and engineering disciplines and vertically from the lowest-level engineer to the highest-level manager to ensure they all have the same information.

Mission assurance task is a specific activity performed by a responsible engineer. The MAB contains a "super-set" of tasks that includes all the MA core processes and supporting disciplines, as well as tasks derived from specifications, standards, lessons learned, and best practices.

Mission assurance task plan is a program office-tailored set of MAB tasks believed to be practically executable within the scope and constraints to meet the specific needs of that program. The MA task plan may be an appendix to the MAP.

Mission assurance verification is focused primarily on assessing MA tasks applied to the program in accordance with the total risk tolerance of the program, considering the constraints for cost and schedule, and ensuring formal reviews validate and document risk-mitigation tactics.

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 risk is the possibility of an adverse outcome in the execution of a specific mission for which a space system acquisition has responsibility. Mission risk focuses on technical risk impact to mission success.

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. MS is typically evaluated after operational turnover and according to program-specific timelines and criteria, such as key performance parameters. MS assessments include operational assessments and user community feedback. In contrast, acquisition success can be defined in terms of performance, cost, and schedule.

Operations assurance is the verification of operations procedures, following their definition, to ensure consistency with overall system integrity and safety goals; and the validation that the operational execution of the procedures meets the intent and preserves actual system integrity and safety.

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 MS in terms of directly attributable positive consequences.

Producibility is a design accomplishment that enables manufacturing to repeatedly 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, inspection, test, and acceptance of hardware without sacrificing desired function, performance, or quality.

Program risk Is the possibility of an adverse outcome in an acquisition activity for which a space program has responsibility. Program risks may be reported as cost, schedule, or technical.

Quality of a product is the degree to which a product's 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 and certified, and are available to support the operation.

Responsible engineer is assigned accountability to specific MA tasks; responsible for risk assessment of the task completion through reporting final assessment status with supporting evidence.

Responsible manager plans MA task assessment effort, assigns tasks to responsible engineers, reviews assessments, and reports assessment status and summary risk.

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 (SOW) is the complete list and description of tasks to be performed and products to be delivered by the supplier; specified in the contract.

Subject matter expert (SME) or “domain expert” is a person who is an expert with special knowledge or skills in a particular area or discipline

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.

Supporting MA discipline (SMD) is an engineering discipline that is executed, in its whole or, more frequently, in partial terms, to support MA core 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 of systems is a collection of task-oriented or dedicated systems that pool their resources and capabilities together to create a new, more complex system that offers more functionality and performance than simply the sum of the constituent systems.

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 flightlike units (e.g., qualification unit) to investigate problems/anomalies in latter stages of development.

Validation is an MA activity that provides confidence, through independent analysis or test, that the technical means and processes accomplish their intended purpose, in this case to meet user needs. Requirements validation occurs during the front end of the systems acquisition life cycle. At the system level, validation occurs before the as-built system is transitioned into mission operations.

Verification (of requirements) 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.

Appendix A2
Acronym List

A&A	Assess and authorize
ACAT	Acquisition category
ACO	Administrative contracting office
ADRL	Agreed data requirements list
AEHF	Advanced extremely high frequency
AF	Air Force
AFI	Air Force Instruction
AFNIC	Air Force Network Integration Center
AFPD	Air Force Policy Directive
AFMCI	Air Force Material Command Instruction
AFPEO	Air Force Program Executive Office
AFSC HQ	Air Force Space Command Headquarters
AFSPCI	Air Force Space Command Instruction
AGE	Aerospace ground equipment
AI&T	Assembly, integration, and test
AIAA	American Institute of Aeronautics and Astronautics
ALC	Administrative contracting office
ALT	Accelerated life testing
AMD	Angular momentum desaturation
ANSI	American National Standards Institute
AO	Authorizing official
AOA	Analysis of alternatives
APB	Acquisition program baseline
ARAR	Accident Risk Assessment Report
ASC/ENSM	Aeronautical Systems Center/Engineering Directorate (Air Force Material Command [AFMC])
ASTM	American Society for Testing and Materials
AT	Anti-tamper
ATC	Authority to connect
ATO	Authorization to operate
AVE	Aerospace vehicle equipment
BAR	Broad area review
BIST	Baseline integrated system test
BOL	Beginning-of-life
BOM	Bill of material
C&A	Certification and accreditation
CA	Certification/certifying authority
CA	Corrective action
CAB	Corrective action board
CAD	Computer-aided design
CCB	Change control board
CCEP	Commercial COMSEC Evaluation Program

CCTL	Common criteria test lab
CDA	Critical design audit
CDA	Cross domain appendix
CDC	Concept design center
CDD	Capabilities development document
CDL	Common data link
CDR	Critical Design Review
CDRL	Contract deliverable requirements list
CDS	Cross domain solutions
CDSAP	Cross-Domain Solutions Assessment Panel
CDSO	Cross Domain Solution Office
CDTAB	Cross-Domain Technical Advisory Board
CE	Chief engineer
CI	Configuration item
CIL	Critical items list
CL	Confidentiality level
CLS	Contractor logistic support
CM	Configuration management
CMAN	Command (Air Force Space Command AFSPCMAN)
CMMI	Capability Maturity Model Integration
CMP	Configuration management plan
CMP	Core MA process
CMVP	Cryptographic Module Validation Program
CNSS	Committee for National Security Systems
CNSSP	Committee on National Security Systems Policy
CO	Contracting officer
COE	Common operating environment
COLA	Collision avoidance
COMSEC	Communications security
CONOPS	Concept of operations
COPV	Composite overwrapped pressure vessel
COTR	Contracting office technical representative
COTS	Commercial off-the-shelf
CPAT	Critical process assessment tool
CPD	Capabilities production document
CPI	Cost performance index
CPI	Critical program information
CPI	Critical program items
CSA	Configuration status accounting
CSAT	Constellation Sustainment Assessment Team
CSCI	Computer software configuration item
CT&E	Certification test and evaluation
CUP	COMSEC Utility Program
CWBS	Contract work breakdown structure
DAA	Designated approving authority

DAG	Defense Acquisition Guide
DAL	Data accession list
DATO	Denial of authorization to operate
DCMA	Defense Contract Management Agency
DFMA	Design for manufacturing and assembly
DI	Data item
DIA	Defense Intelligence Agency
DIACAP	Defense Information Assurance Certification and Accreditation
DID	Data item description
DIP	DIACAP Implementation Plan
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DITL	Day in the life
DMS	Data management system
DOD	Department of Defense
DODI	Department of Defense Instruction
DOORS	Dynamic Object Oriented Requirements System
DPA	Destructive physical analysis
DSAWG	Defense IA/Security Accreditation Working Group
DSCC	Defense Supply Center Columbus
DSOR	Depot source of repair
DT&E	Development, test, and evaluation
DTC	Design-to-cost
E2E	End to end
ECP	Engineering change proposal
EDS	Energy dispersive spectroscopy
EEE	Electronic/electrical/electromagnetic
EIA	Electronics Industries Alliance
EIDP	End-item data package
EM	Engineering model
EMC	Electromagnetic compatibility
EMCS	Electromagnetic Compatibility Society (IEEE)
EMI	Electromagnetic interference
EMRR	Executive mission readiness report
EMSEC	Emanations security
EOC	Evidence of completion
EOL	End-of-life
ERB	Engineering Review Board
ESC	Electronic Systems Center
ESD	Event-sequence diagram
ESOH	Environmental safety and occupational health
ESS	Environmental stress screening
ET	Event tree
ETG	Engineering and Technology Group

ETTI	Environmental Test Thoroughness Index
EUTA	Engineering unit test assembly
EVM	Earned value management
FAR	Federal Acquisition Regulation
FAT	Factory acceptance test
FCA	Functional configuration audit
FDIR	Failure detection, isolation, and recovery
FET	Field effect transistor
FFRDC	Federally Funded Research and Development Center
FISMA	Federal Information Security Management Act
FIST	Final integrated systems test
FMEA	Failure modes and effects analysis
FMECA	Failure mode, effects, and criticality analysis
FOR	Flight Operations Review
FPGA	Field-programmable gate array
FQR	Formal Qualification Review
FRACAS	Failure reporting analysis and corrective action system
FRB	Failure Review Board
FRR	Flight Readiness Review
FTA	Fault tree analysis
GAP	General Availability Program
GFE	Government-furnished equipment
GIDEP	Government Industry Data Exchange Program
GN&C	Guidance, navigation, and control
GOTS	Government off-the-shelf
GSE	Ground support equipment
GSE&I	General system engineering and integration
GST	Ground system test
GUI	Graphic user interface
HAR	Hardware Acceptance Review
HBT	Heterojunction bipolar transistors
HDBK	Handbook
HIS	Human systems integration
HNSC	Space COMSEC Directorate (formerly CPSG/ZJ)
HW	Hardware
HWCI	Hardware configuration item
I&T	Integration and test
IA	Information assurance
IAD	Information Assurance Directorate
IASRD	Information Assurance System Requirements Document
IATO	Interim authorization to operate
IATT	Interim authorization to test
IAVA	Information assurance vulnerability alerts
IAW	In accordance with
IBR	Integrated Baseline Review

IC	Integrated circuit
IC	Intelligence community
ICD	Initial capabilities document
ICD	Intelligence Community Directive
ICD	Interface control document
ICE	Independent cost estimate
ICS	Interim contract support
IEEE	Institute of Electrical and Electronics Engineers
IGCE	Independent government cost estimate
ILSS	Integrated Logistics Support System
iMAT	Integrated Mission Assurance Tool
IMP	Integrated management plan
IMS	Integrated master schedule
INOSC	Integrated network operations and security center
INCOSE	International Council on Systems Engineering
IOC	Initial operations capability
IPA	Independent program assessment
IPPD	Integrated product and processes development
IPS	Independent program summary
IPSC	Institute for the Protection and Security of the Citizen
IPT	Integrated product team
IPT	Integrated process team
IRR	Independent Readiness Review
IRRT	Independent Readiness Review Team
IRS	Interface Requirements Specification
IRT	Independent Review Team
ISBN	International Standard Book Number
ISO	International Organization for Standards
ISO/IEC	ISO/International Electrotechnical Commission
IST	Integrated system test
IT	Information technology
IT&E	Integration, test, and evaluation
ITA	Independent technical assessment
JAPC	Joint Audit Planning Committee
JCIDS	Joint Capabilities Integration and Development System
KDP	Key decision point
KMI	Key management infrastructure
KPP	Key performance parameter
LCC	Life cycle cost
LCCE	Life cycle cost estimate
LEO	Low Earth orbit
LLIL	Limited life items list
LRR	Launch Readiness Review
LV	Launch vehicle
M&P	Materials and parts

M&P	Materials and process
M&S	Modeling and simulation
MA	Mission assurance
MAB	Mission Assurance Baseline
MAC	Mission assurance category
MAG	Mission Assurance Guide
MAP	Mission assurance plan
MCO	Mars climate orbiter
MDAP	Major Defense Authority
MDI	Mars orbit insertion
MDG	Manufacturing Development Guide
MGS	Mars global surveyor
MIB	Mishap Investigation Board
MIL-SPEC	Military specification
MIL-STD	Military standard
MILCON	Military construction
MLD	Master logic diagrams
MLE	Mean life estimate
MMD	Mean mission duration
MMP	Manufacturing Management Plan
MOA	Memorandum of Agreement
MOI	Mars orbit insertion
MPL	Mars Polar Lander
MRB	Material Review Board
MRR	Manufacturing Readiness Review
MRR	Mission Readiness Review
MRR	Mission Review Board
MS	Mission success
MS	Milestone
MSPSP	Missile System Prelaunch Safety Package
MTBF	Mean time between failure
MTTF	Mean time to failure
MTTR	Mean time to repair
MTS	Member technical staff
NAMT	NASA Audit Management Team
NASA	National Aeronautics Space Administration
NAVAIR	Naval Air
NDI	Non-development item
NEPA	National Environmental Policy Act
NIPRNet	Unclassified but Sensitive Internet Protocol Router Network
NIST	National Institutes of Standards and Technology
NSA	National Security Agency
NSS	National Security Space
NSS	National Space Systems
NVLAP	National Voluntary Laboratory Accreditation Program

O&M	Operations and maintenance
O&SHA	Operating and support hazard analysis
OCD	Operational concept description
OCI	Organizational conflict of interest
OD	Operational demonstrations
OEM	Original equipment manufacturer
OMB	Office of Management and Budget
ORA	Operational readiness assurance
ORA	Operations readiness assessment
ORS	Operationally Responsive Space
OSS&E	Operational safety, suitability, and effectiveness
OT&E	Operational test and evaluation
PAPL	Program-approved parts list
PAR	Parts, materials, and processes approval request
PCA	Physical configuration audit
PDA	Preliminary design audit
PDM	Product data management
PDR	Preliminary Design Review
PESHE	Programmatic environment, safety, and occupational health evaluation
PHA	Preliminary hazard analysis
PHL	Preliminary hazard list
PHS&T	Packaging, handling, storage, and transportation
PI	Program integrator
PL	Payload
PL	Protection level
PM	Program manager
PMO	Program management office
PMP	Parts, materials, and processes
PMP	Program management plan
PMPCB	Parts, Materials, and Processes Control Board
PO	Program office
POA&M	Plan of actions and milestones
POC	Point of contact
PoF	Probability of failure
POM	Program objectives memorandum
PPBS	Planning, programming, and budgeting system
PPP	Program protection plan
PRA	Probalistic risk assessment
PRD	Program requirements document
PRR	Producibility Readiness Review
PRR	Production Readiness Review
PSR	Pre-Ship Review
QA	Quality assurance
QCI	Quality conformance inspection

QML	Qualified manufacturing line
QMS	Quality management system
QPL	Qualified parts list
R&D	Research and development
R&M	Reliability and maintainability
RAD	Requirements allocation document
RBD	Reliability block diagram
RDT&E	Research, development, test, and evaluation
RF	Radio frequency
RFP	Request for proposal
RM	Risk management
RMA	Reliability, maintainability, and availability
RMA	Risk management analysis
RMF	Risk management framework
RMP	Risk management plan
SAR	Safety Assessment Report
SAR	Software Requirements and Architecture Review
SAS	Supplier assessment system
SC	Spacecraft
SCA	Satellite Control Authority
SCAO	SIPRNet Connection Approval Office
SCD	Source control drawing
SCRR	Space COMSEC Requirement Review
SDR	System Design Review
SDRL	Subcontract data requirements list
SE	Systems engineering
SEE	Single-event effect
SEIT	System engineering and integration test
SEMP	Systems Engineering Master Plan
SEP	Systems Engineering Plan
SETA	Systems engineering and technical assistance
SFR	System Functional Review
SHA	System hazard analysis
SI	Software item
SIPRNet	Secret Internet Protocol Router Network
SIS	Software Interfaces Specification
SKMP	System key management plan
SLOC	Source lines of code
SM	Single manager
SMC	Space and Missile Systems Center
SMCI	Space and Missile Systems Center Instruction
SMD	Supporting MA discipline
SME	Subject matter expert
SOO	Statement of objectives
SORAP	Source of repair assignment process

SOS	System-of-systems
SOW	Statement of work
SP	Special publication
SPI	Schedule performance index
SPO	System program office
SQB	Space quality baseline
SRCA	Safety requirements/criteria analysis
SRD	Systems requirements document
SRR	System Requirements Review
SS	System specification
SSDD	System/Subsystem Design Description
SSHA	Subsystem hazard analysis
SSM	System safety manager
SSPP	System Safety Program Plan
SSS	System/subsystem specification
STAR	System Threat Assessment Report
ST&E	Security test and evaluation
STE	Special test equipment
SV	Space vehicle
SV	System view
SVR	System Verification Review
SW	Software
SWAMP	Software Acquisition Management Plan
SWaP	Size, weight, and power
T&E	Test and evaluation
TEMP	Test and Evaluation Master Plan
TER	Test Exit Review
TLYF	Test like you fly
TOR	Technical operating report
TP	Test procedure
TPM	Technical performance measures
TRA	Technology Readiness Assessment
TRANSEC	Transmission security
TRD	Technical requirement document
TRL	Technology readiness level
TRR	Test Readiness Review
TSRD	Technical security requirements document
TT&C	Telemetry, tracking, and command
TT&P	Tactics, techniques, and procedures
TWT	Traveling wave tube
U.S.	United States
UARC	University affiliated research center
UCDMO	Unified Cross Domain Management Office
UIS	User interface specification
UPA	User partnership agreement

UPP	User Partnership Program
USAF	United States Air Force
UTC	Universal time coordinated
UUT	Unit under test
UVF	Unverified failure
VCRM	Verification cross-reference matrix
VTC	Videoconference
VWG	Verification working group
WCAA	Worst-case circuit analysis
WIRE	Wide-field Infrared explorer
WBS	Work breakdown structure
WG	Working group
XRF	X-ray fluorescence

Appendix A3
Space System Development Analyses

The following is a list of analyses that should be considered in satellite development. The following Aerospace subject matter experts contributed to this list: Kevin Bell, Nai-Yi Cheng, Mark Mueller, Brian Lenertz, John Welch, Selma Goldstein, David Thomas, Kenneth Luey, and Ron Duphily. Reed James of Lockheed-Martin provided information in the area of space environments and Walter Dennis' chapter on acquisition strategy considerations in the *Space Vehicle Systems Engineering Handbook* provided additional insight across the board. Suggestions for additions are welcome.

Software

- Processor usage
- Memory usage
- Bus usage
- Complexity analysis
- Code analysis
- Test coverage
- Software reliability
- Security analysis
- Reuse
- Tools
- Problem and correction report
- Root cause
- Timing
- Failure tree
- Methodology

Hardware in general

- Worst-case circuit analysis
- Worst-case component analysis
- Fault analysis
- Reliability analysis
- Temperature
- Thermal expansion
- Evaluation of qualification testing
- Evaluation of acceptance testing
- Tolerance
- Weight

Fault management
- Subsystem functional fault coverage
- Bottom-up fault coverage
- Response time
- Notification
- In-view/out-of-view coverage
- Fault processor coverage

Command and data handling
- Bus loading
- Timing
- Signal margin
- Command and telemetry port margin
- Telemetry bandwidth margin

Power
- Energy balance
- Bus stability
- Fusing, steady-state and transient
- Impedance stability
- Solar array sizing
- Solar array phasing
- Battery sizing

Guidance and control
- Stability
- Actuator sizing
- Pointing accuracy
- Alignment
- Calibration
- Phasing

Structures and mechanisms
- Force/torque margins, static and dynamic
- Stress analysis
- Design load cycle
- Thermal distortion
- Clearances, on launch vehicle and on orbit
- Deployment
- Test and Transportation clearances
- Separation
- Tolerance buildup
- Venting

Antennas
- Phasing
- Pointing accuracy
- Deployability
- Surface tolerance
- Efficiency
- Steering speed
- Beamwidth considerations like coverage and off-axis loss
- Mechanical robustness
- Gimbal limit effects at different satellite nodes and different mission phases

Communications/telemetry tracking and control
- Link budgets in various mission phases and environments
- Jamming immunity
- Node selection
- Interference potential
- Polarization
- Multipaction
- Multipath
- Ranging error drift
- Carrier, subcarrier stability
- Data transmission and factors such as rate, coding, modulation, bandwidth, and format

Thermal
- Thermal predictions, vehicle and subassembly, ground and flight, over entire life
- Margin predictions
- Heater power
- Growth capability
- Heat pipe sizing
- Radiator sizing

Propulsion
- Line priming/surge analysis
- Waterhammer potential
- Propellant budget
- Propellant residuals
- Flow/performance modeling
- Pressure blowdown
- Contamination and filter sizing
- Propellant remaining estimation algorithm

- Thruster performance models
- Valve force margin
- Propellant tank slosh analysis
- Propellant tank expulsion efficiency and operation in mission environment
- Phasing

Explosive ordinance
- Lot acceptability analysis
- Explosive force

Cables and connectors
- Impedance
- Load carrying
- Mechanical robustness

Non-optical payload
- Power
- Signal to noise
- Dynamic range
- Channel fidelity
- Field of view
- Pointing accuracy

Electro-optical sensors
- Optical design and baseline performance
- Tolerance
- Stray light
- As-built analysis
- End-to-end performance analysis
- Field of view
- Pointing accuracy

Mass properties
- Mass
- Center of gravity, weight distribution
- Moment of inertia
- Stiffness
- Margin

Contamination
- Satellite sources and effects contamination analysis

Test Like You Fly
- Exceptions

Space environments
- Total dose
- System generated electromagnetic pulse
- Single event upset
- Single event effects
- Photocurrent burnout
- Event recovery
- Atomic oxygen
- Electrostatic discharge
- Ultraviolet effects
- Micrometeoroids

Launch loads
- Coupled loads
- Model fidelity

Dynamic environments
- Vibration
- Acoustic
- Shock

Electromagnetic compatibility
- Emissions
- Susceptibility

Safety
- Hazard analysis
- Missile system prelaunch safety package
- Collision avoidance

Reliability
- Reliability predictions
- Failure modes and effects (and criticality)

System engineering
- Requirement allocation
- Requirement decomposition
- Requirement traceability
- Trade studies
- Cost

Schedule
Risk posture
Interface compatibility
Functional allocation
Feasibility