AEROSPACE REPORT NO.
TOR-2011(8591)-21

Mission Assurance Guidelines for A-D Mission Risk Classes

June 3, 2011

Gail Johnson-Roth
Acquisition Risk and Reliability Engineering Department
Mission Assurance Subdivision

Prepared for:

Space and Missile Systems Center
Air Force Space Command
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

Contract No. FA8802-09-C-0001

Authorized by: Engineering and Technology Group

Developed in conjunction with Government and Industry contributions as part of the U.S. Space Programs Mission Assurance Improvement workshop.

AEROSPACE REPORT NO.
TOR-2011(8591)-21

Mission Assurance Guidelines for A-D Mission Risk Classes

June 3, 2011

Gail Johnson-Roth
Acquisition Risk and Reliability Engineering Department
Mission Assurance Subdivision

Prepared for:

Space and Missile Systems Center
Air Force Space Command
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

Contract No. FA8802-09-C-0001

Authorized by: Engineering and Technology Group

Developed in conjunction with Government and Industry contributions as part of the U.S. Space Programs Mission Assurance Improvement workshop.

AEROSPACE REPORT NO.
TOR-2011(8591)-21

Mission Assurance Guidelines for A-D Mission Risk Classes

June 3, 2011

Gail Johnson-Roth
Acquisition Risk and Reliability Engineering Department
Mission Assurance Subdivision

Prepared for:

Space and Missile Systems Center
Air Force Space Command
483 N. Aviation Blvd.
El Segundo, CA 90245-2808

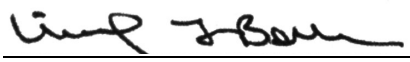
Contract No. FA8802-09-C-0001

Authorized by: Engineering and Technology Group

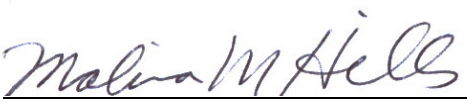
Developed in conjunction with Government and Industry contributions as part of the U.S. Space Programs Mission Assurance Improvement workshop.

Mission Assurance Guidelines for A-D Mission Risk Classes

Approved by:



Michael L. Bolla, Principal Director
Mission Assurance Subdivision
System Engineering Division
Engineering and Technology Group



Malina M. Hills, General Manager
MILSATCOM Division
Space Programs Operations
Space Systems Group

Acknowledgements

This document has been produced as a collaborative effort of the Mission Assurance Improvement Workshop. The forum was organized to enhance Mission Assurance processes and supporting disciplines through collaboration between industry and government across the US Space Program community utilizing an issues-based approach. The approach is to engage the appropriate subject matter experts to share best practices across the community in order to produce valuable Mission Assurance guidance documentation.

The document was created by multiple authors throughout the government and the aerospace industry. We thank the following contributing authors for making this collaborative effort possible:

Dr. Rudy Emrick (Orbital Sciences Corporation)
Matthew Fahl (Harris)
Linda Halle (The Aerospace Corporation)
Edward Hume (Johns Hopkins University Applied Physics Laboratory)
Jean-Claude Inauen (Northrop Grumman Aerospace Systems)
David Kalian (The Boeing Company)
Maj David Laird (National Reconnaissance Office)
Jay A Landis (Space and Missiles System Center)
Pat Martin (NASA, HQ)
Dave Michel (Raytheon Space and Airborne Systems)
Eli Minson (General Dynamics)
Mark Oja (ATK)
Andy Penner (Lockheed Martin Corporation)
Brian Shaw (The Aerospace Corporation)

A special thank-you for co-leading this team and efforts to ensure completeness and quality of this document goes to:

Dave Pinkley (co-lead) – Ball Aerospace
Gail Johnson-Roth (co-lead) – The Aerospace Corporation

The Topic Team would like to acknowledge the contributions and feedback from the following organizations:

The Aerospace Corporation
Ball Aerospace & Technologies Corporation
The Boeing Company
General Dynamics
Johns Hopkins University Applied Physics Laboratory
Lockheed Martin Corporation
Northrop Grumman Aerospace Systems
Orbital Sciences Corporation
Raytheon Space and Airborne Systems
Space and Missile Systems Center

The authors deeply appreciate the contributions of the subject matter experts who reviewed the document:

Chris Burno (Ball Aerospace & Technologies Corporation)
James Haug (Raytheon Space and Airborne Systems)
Malina Hills (The Aerospace Corporation)
Brian Hudson (United Launch Alliance)
Scott Lichty (Lockheed Martin Corporation)
Kendall Nii (Orbital Sciences Corporation)
Frank Rotter (The Boeing Company)
Pete Portanova (The Aerospace Corporation)
Tom Stout (Northrop Grumman Aerospace Systems)

Executive Summary

The "Mission Assurance Guidelines for A-D Mission Risk Classes" document is a team product from the 2010-2011 Mission Assurance Workshop (MAIW) program. The goal of the team, which consisted of government and industry partners, was to develop guidelines to define characteristic profiles for mission assurance processes for a given space vehicle risk Class (A, B, C, or D) to serve as a recommended technical baseline suitable to meet program needs based on programmatic constraints and mission needs. This document leverages the 2010 MAIW product, "Mission Assurance Program Framework," that defined 16 processes supporting mission success that were universally consistent across all organizations, and considered the essential set necessary to provide effective mission assurance for U.S. space programs.

Contractors are required to respond to acquisitions specifying different mission risk classes without sufficient guidance on the characteristics and requirements for those different classes. The early life cycle establishment of risk tolerance level provides the basis for government and contractors to effectively communicate during the development and implementation of appropriate acquisition strategies and relevant requirements. This document provides mission risk class profiles A through D for the U.S. space programs considering factors such as criticality to a specific government agency's strategic plan, national significance, availability of alternative opportunities, success criteria, investment, mission life, and other factors. Mission risk class profiles are based on NPR 8705.4, NASA risk classifications, and DOD-HDBK-343, requirements for one-of-a-kind space equipment. The mission risk Class A profile represents **minimum practical risk** where all potential avenues are pursued to reduce the program risk exposure for critical national systems. The mission risk Class B profile is **low risk** with minor compromises in the application of mission assurance standards to balance programmatic tradeoffs between minimum risk and lower cost for operational and demonstration systems. The mission risk Class C profile represents **moderate risk** and shifts the risk burden from the government to the contractors' best practices for exploratory or experimental missions. The mission risk Class D represents the **highest risk** profile, typically for one year or less experimental missions and more fully shifts development to contractor best practices with minimal government oversight.

This guideline defines characteristic profiles for mission assurance processes with a set of typical process practices aligned with the definitions for a given mission risk class profile (A, B, C or D) that reflects stated mission risk tolerance commensurate with program constraints and mission objectives. The guidelines provided in this document will serve as input to requirements documents assessed against a specific acquisition's cost-technical drivers, and quantified risks and mitigation strategies to define the program risk baseline and requirements to meet stated mission objectives.

Contents

Figures

Tables

1. Introduction

1.1 Background

The "Mission Assurance Guidelines for A-D Mission Risk Classes" document was established to define typical practices to ensure mission success across the mission risk classes (A, B, C or D). Mission risk class profiles are associated with technical and quality issues that impact mission success. Execution risk associated with acquisition program cost and schedule is only indirectly addressed in this document. This document examines each of the mission risk classes followed by a critical assessment of the common mission assurance processes that are recommended as an essential set necessary to provide effective mission assurance for U.S. space vehicle programs.

The definition of mission assurance (MA) adopted by these guidelines is defined as part of the Mission Assurance Strategic Intent TOR-2011(8591)-9, Third United States Program Mission Assurance Summit Overview, December 2, 2010, which contains the Mission Assurance Strategic Intent approved by National Aeronautics and Space Administration (NASA), National Reconnaissance Office (NRO), Missile Defense Agency (MDA), Space and Missile Systems Center (SMC). 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**".

This document leverages the 16 processes defined by the 2010 Mission Assurance Improvement Workshop (MAIW) product, "Mission Assurance Program Framework," TOR-2010(8591)-18, for their support in achieving mission success. The appendices of this document provide tables and summaries of typical process execution for the 16 MA framework processes supporting mission success. The material presented should not be a standalone reference but as a starting point for developing the program's risk strategy given mission needs and programmatic constraints. The 16 processes included both core (key drivers to mission success, independent of organizational construct); and supporting (verification process/activities executed within the performing discipline to verify work product or process integrity prior to completion). The core and supporting processes together formed the set of MA activities that the U.S. space enterprise judged to be essential to provide effective mission assurance for U. S. space programs and optimize the probability of mission success.

Risk strategy development requires that the development architecture be critically evaluated from a risk balance perspective to understand risks inherent in the level of uncertainty associated with those risks. Class D mission class is the only risk profile in which unknown risk is acceptable. It is limited to low cost projects during the initial phase of technology development and demonstrations since the cost of failure in space is normally prohibitive. These missions may be mitigated later through re-flight opportunities.

An overview of a risk balance methodology is provided in Chapter 4, and process application guidelines for risk classifications are discussed in depth in Appendix D, which establishes an example risk-balancing framework. Prior to this application discussion, Chapter 2 and Chapter 3 establish the foundation for the guidelines by defining and categorizing the 16 processes for mission success, and examining the core characteristics of the four mission risk classes.

The mission risk classes A through D establish a hierarchy for the U.S. space program considering factors such as criticality to a specific government agencies strategic plan, national significance, availability of alterative opportunities, success criteria, investment, mission life, and other factors.

NPR 8705.4 “Risk Classification for NASA Payloads” and DOD-HDBK-343 “Design, construction, and testing requirements for one-of-a-kind space equipment” have been leveraged to define basic risk mission classes and success criteria. In addition, this document is a companion document to the Aerospace Technical Operating Report (TOR-2011(8591)-5), Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles. The intended audience for the Aerospace document is government program offices and the contractor community to provide guidance during acquisition planning for National Security Space (NSS) systems. The acquisition-planning document is a top-down government-driven examination of compliance document tailoring. This guideline is a bottom-up examination of typical mission success process execution across the same mission classes. Both documents were reviewed to ensure no conflicting guidance.

Note that a given acquisition may have multiple mission risk classes assigned for different mission elements. For instance the primary payload, spacecraft bus and secondary payloads may have different risk profiles depending on the role they play in the overall mission.

1.2 Existing Mission Class Guidelines

Reference documents that provide guidelines for management of risks across mission classes are summarized in Table 1. They establish a four-tiered space mission risk profile classification approach where technical and program management attributes are established for the range of U.S. space missions spanning high priority/minimum practical risk (e.g., high national priority) to low priority/high risk (e.g., minimum acquisition cost) tolerance.

This classification system was created to correlate mission attributes to allowable risk tolerance, and facilitate a common understanding of many elements of the planned development and mission assurance processes. NASA flows down the risk classification for the majority of their acquisitions and assigns risk class to specific mission category such as flagship, discovery, and explorer missions. There is currently a parallel effort within NSS for specification and standard revitalization that provides prescriptive guidance for assuring mission success for Class A, missions.

Table 1. Existing Risk Classification Guidelines

Document	Scope
TOR-2011(8591) – 5, Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles, 13 September 2010	Establishes mission class tailoring of compliance documents and provides specific tailoring guidance to those documents in order to better map requirements to the spectrum of NSS acquisitions. Defines four mission risk classes consistent with this document
DOD-HBDK-343, Design, Construction, and Testing Requirements for One of a Kind Space Equipment, 1 February 1986	Technical and program requirements for the design, construction, and testing of various classes of space equipment. Defines four payload classes A-D. Requirements are a composite of those that have been found to be cost effective for one of a kind space programs.
NASA NPR 8705.4, Risk Classification for NASA Payloads, 14 June 2004 (revalidated 9 July 2008)	Establishes baseline criteria that define the risk classification level for NASA payloads and nonhuman-rated launch systems or carrier vehicles, the design and test philosophy and the common assurance practices applicable to each level. Utilizes the same Class A-D approach described in DoD-HDBK-343.

2. Mission Success Processes

The list of 16 processes is taken from the 2010 MAIW topic "Mission Assurance Program Framework," captured in TOR-2010(8591)-18. The MA Framework guideline provides an industry and government matrix of processes that support achieving mission success.

The 16 processes shown below are organized into the three categories identified in Table 2. The appendices follow the same category structure with one appendix for each process. The processes are defined in more depth in each appendix chapter.

Table 2. MA Framework Mission Success Processes

Category	Process
1. Program Execution	(1) Design Assurance (2) Requirement Analysis and Validation (3) Parts, Materials and Processes (4) Environmental Compatibility (5) Reliability Engineering (6) System Safety (7) Configuration/Change Management (8) Integration, Test and Evaluation
2. Risk, Oversight and Assurance	(9) Risk Assessment and Management (10) Independent Reviews (11) Hardware Quality Assurance (12) Software Assurance (13) Supplier Quality Assurance
3. Triage, Information and Lessons Learned	(14) Failure Review Board (15) Corrective/Preventative Action Board (16) Alerts, Information Bulletins

Each of these three categories serves an essential role in the assurance of mission success. The process roles can be characterized as:

- Category 1 Program Execution processes include inline processes performed throughout program execution as integral elements of the design and development process responsible for building in consistency, completeness, quality, reliability, safety, and verifying requirements and validating the implementation.
- Category 2 Risk, Oversight, and Assurance processes include insight/oversight parallel processes for identification of potential risks to mission success based on both gated assessment processes. Note in the application of these processes oversight vs. insight is defined as follows:

  - Oversight is defined as the act of overseeing a program to actuarially characterize risk. Oversight implies certain separateness between customer and contractor and more of a regulatory control superintendence type of relationship.
  - Insight is defined as cooperative engagement with the contractor in the characterization and mitigation of risk. It implies relying more on the contractor's command media where the contractor as the developer is responsible for identifying and mitigating

developmental risk. The insight is more focused on acute observation and deduction based on contractor-communicated mission risk.

- Category 3 Triage, Information and Lessons Learned processes represent anomaly investigation, product and process corrective action, and information sharing processes assuring product reliability and continual process improvement.

3. Mission Risk Class Profile Key Characteristics

This chapter examines A through D mission risk class key characteristics. The mission class profiles lay out a structural approach for defining a hierarchy of risk combinations for the US space systems enterprise. Characteristic categories in Table 3 examine key programmatic and mission indicators with corresponding mission class considerations. The table is followed by summary characteristics of each class. Note that none of these characteristics is absolute. It portrays representative characteristics exhibited by the risk class profiles.

Table 3. Mission Risk Class Profiles

Characteristic	Class A	Class B	Class C	Class D
Risk Acceptance	Minimum Practical	Low Risk	Moderate Risk	Higher Risk
National Significance	Extremely Critical	Critical	Less Critical	Not Critical
Payload type	Operational	Operational or Demo Op	Exploratory or Experimental	Experimental
Acquisition costs	Highest Lifecycle Cost (LCC)	High LCC	Medium LCC	Lowest, LCC
Complexity	Very high – High	High – Medium	Medium – Low	Low - Medium
Mission Life	>7 years	≤7 years	≤4 years	< 1 yrs
Cost	High	High to Medium	Medium - Low	Low
Launch Constraints	Critical	Medium	Few	Few - None
Alternatives	None	Few	Some	Significant
Mission Success	All practical measures	Stringent/minor compromises	Reduced mission assurance standards	Few mission assurance standards
Typical Contract Type	Cost Plus Award Fee (CPAF)*	CPAF-Firm Fixed Price (FFP)	Cost Plus (CP)-FFP	FFP

* Note that CPAF for Class A is for first of fleet, not once a production program is in-place.

Class A missions are extremely critical operational systems where all practical measures are taken to ensure mission success. They have the highest cost, are of high complexity, and the longest mission life with tight launch constraints. Contract types for these systems are typically cost plus because of the substantial development risk and resultant oversight activities.

Class A missions are achieved by strict implementation of mission assurance processes devised through proven best practices to achieve mission success over the desired life of the system. All practical measures, to include full incorporation of all specifications/standards contract requirements with little to no tailoring, are taken to achieve mission success for Class A missions. Class A missions are long life, nominally greater than 10 years and represent large national investments for critical applications.

NASA Class A missions are represented by flagship missions such as the Hubble Space Telescope Cassini, and the Jupiter Icy Moon Orbiter (JIMO). NSS Class A missions include the Global Positioning System satellite and military communication satellite systems to include Milstar.

Class B missions are defined as critical operational, exploration, and technical demonstrators in which only minor compromises are taken in stringent processes for mission success to achieve a low risk profile. The criteria for minor compromises include allowing controlled single point failures, proto-flight hardware, Level/Grade 2 EEE parts, reduced circuit analysis, etc. Class B missions have high costs, are of high to medium complexity, long mission life, with moderate launch constraints. Contract types for these systems are cost plus if there is any significant technology development, i.e., lower technology readiness level hardware and can be potentially firm fixed price given well-defined requirements.

Class B space vehicles are priority missions whose minor compromises to MA are due to programmatic tradeoffs between minimum risk and lower costs. The majority of specification and standard requirements are flowed down, but minor tailoring is allowed based on achieving a low risk tolerance to mission success. Contactor equivalent processes for Class B missions are sought where possible to ensure the risk profile is maintained without unnecessarily driving cost.

NSS Class B missions may become or have the potential to become operational. An example of an NSS Class B mission is the Advanced Research and Global Observation Satellite (ARGOS). NASA Class B programs include Discovery, Mars Exploration Rover (MER), Mars Reconnaissance Orbiter (MRO) and ISS payloads.

Class C missions are defined as lower national significance, exploratory or experimental missions, with a reduced set of MA standards applied resulting in a moderate risk profile. They have moderate to low cost, are of moderate to low complexity with reduced mission scope, shorter mission life, few launch constraints, and some alternatives available. Contract types for these systems are typically a combination of cost plus for new development such as instruments, and fixed price for the spacecraft bus.

Class C space vehicles are not critical to national goals. The missions have a shorter life span of 1-5 years with assurance standards based on contractor best practices.

An NSS example of the upper end of a Class C space vehicle is the Communications/Navigation Outages Forecasting System (CNOFS) that was sponsored by the Space Test Program with the payload suite being provided by the Air Force Research Laboratory. NASA Class C missions include Explorer payloads including Medium-Class Explorer and Small Explorer and International Space Station complex sub-rack payloads.

Class D missions are defined as having low national criticality. They tend to be experimental type missions with minimum MA standards/requirements put on contract and a higher risk profile. They have the lowest costs, are of low mission complexity, typically only one year or less mission life, with minimum launch constraints and opportunities for alternatives to achieve mission objectives. Contract types for these systems tend to be firm fixed price sponsoring best effort with minimum government oversight.

Class D space vehicles' focus is on keeping acquisition cost low. Mission failure would have little to no impact on national goals. They are research-oriented missions providing a proof of concept within a limited budget and mission scope. MA standards are contractor based (best practices) with a higher risk tolerance.

An example of a Class D is the MidStar space vehicle developed by the Naval Academy. Another example is CubeSats that are (4 inch cubes), semi-standard satellites that are typically produced and modified by universities and university-corporate partnerships. For NASA Class D missions include technology demonstrators, simple International Space Station payloads.

4. Process Application Guidelines for Risk Classifications

The recommended audience for these guidelines includes both U.S. space system contactors and their government agency acquisition counterparts. The guideline provides a framework, characteristic profiles, in order to foster critical evaluation of the risk strategy for a given acquisition to establish the program baseline. These characteristic profiles define typical process practices aligned with the definitions of risk classifications. The practices stated - for a given process - at a given mission risk class, are not meant to be used rigidly. They are intended to identify typical execution but must be further evaluated in the context of the needs of the specific acquisition. Once a program baseline is agreed to and documented by the contract, changes to that baseline must be approved by the government, contractor, and associated suppliers.

This guideline introduces the concept of risk balance, which supports the critical evaluation process. The objective of this risk balance discussion is to lay the groundwork for managing the application of a data-driven risk-based acquisition. The concept of risk balance in the context of minimizing the risk to mission success is illustrated in Figure 1. The figure identifies the four mission risk classes from Class A minimum practical risk to Class D higher risk. The column graph vertical axis represents the total risk exposure. The total risk exposure for Class A typically is greater due to factors such as mission length for NSS national missions. The column graph horizontal axis represents the level of mission assurance activities performed. Class A programs do everything possible to eliminate risk. The MA activity for program risk mitigation is large with the residual risk left after mitigation as low as practical. Class B programs still have significant MA activities for program risk mitigation with only minor reduction in assurance activities over the lifecycle. Accepted residual risk is larger than for Class A programs but typically risk uncertainty is understood. Class C has less MA activities for risk mitigation and considerable more residual risk, for instance Class C missions are typically single string. Class D has the smallest number of MA activities for risk mitigation and the largest residual risk. The focus of Class D missions is typically experimental.

The bar chart on the right in Figure 1 shows the increase of predicted mission success (Ps) with mission assurance investment. These class relationships can be instructive in formulating the appropriate risk balance with programmatic constraints. The graph shows as greater MA resources are applied there is a significant valued added benefit to MA investment especially for the Class D and C missions as noted by the increase in Ps for those missions. These classes typically will have sufficient self-governance to achieve a reasonable Ps. For Class B, which has minor compromises in stringent MA practices, there is value added benefit as your random failure probability is low leading to a high probability of success. For Class A, a higher probability mission success is desired striving to achieve minimum practical risk; for missions of high national importance/criticality, failure is not an option. The random failure probability is only slightly better than Class B but the residual risk is reduced to a level where infant mortality and/or design-precipitated failures have a very low likelihood. Note that this graph is representative of improvement in mission success with investment. It is not an absolute and the mission classes can vary and overlap when a specific risk strategy is chosen.

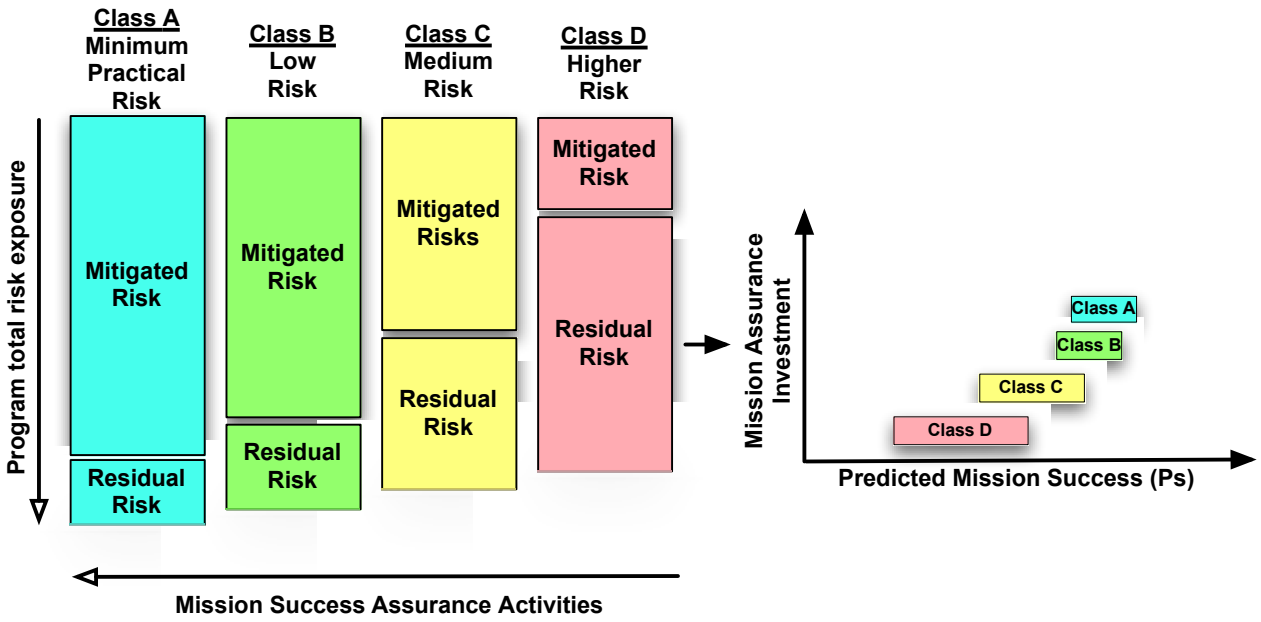


Figure 1. Risk balancing approach overview.

Class A missions tend to be the most expensive and require the most time to execute, characterized as first of fleet long-life national assets and flagship missions. These missions tend to be very complex with multiple payloads and capabilities. On the other extreme Class D missions are the least expensive and may just be a payload sharing a ride. Risk acceptance is higher, not all risk is well understood due to the application of minimum assurance standards and processes, and the fact that the mission itself may be a risk mitigation effort to prove out a new technology. The intent of this guideline is to balance accepted risk against mission, cost, and schedule constraints while providing the highest level of mission success achievable within those constraints. Note that while the Class C and D risk profiles embody the most risk to mission success the probability of mission success must still be relatively high because a failure in space is seldom cost effective. Appendix D examines risk balance in greater detail providing a methodology for performing a risk balance critical evaluation in the development of the programs risk strategy.

4.1 Process Execution Perspectives

Supporting the critical evaluation process, the typical process execution practices given in the appendixes can be examined from four execution perspectives:

1. Process Application Level
2. Process Rigor
3. Process Oversight
4. Process Relationships

Each perspective is reviewed below:

Process Application Level. Product assembly level at which a process is applied to ensure compliance of a given requirement and/or support graceful degradation of mission performance.

Example includes failure modes and effects analysis (FMEA) or fault tree analysis (FTA) (inductive and deductive analysis respectively), which can be applied at multiple levels in a

design to ensure no single point failures (SPFs), redundancy integrity, fault isolation, or identifying contributing paths to a fault event. This will vary across the mission classes to protect redundancy in a Class A or B system, to limit fault propagation in a Class C system, enabling graceful degradation, and to ensure that an experimental payload in a Class D system cannot undermine the integrity of other payloads or the entire mission.

Process rigor. Method and depth of process used to identify and reduce risk by eliminating or reducing risk to a residual level that is acceptable for a given mission risk class.

Examples:

1. Hardware quality assurance inspection of patent defects (e.g., solder joints for ensuring workmanship). All solder joints for Class A missions must be inspected including hidden joints using techniques such as 3D X-ray techniques, whereas for Class B systems process capability can be used to validate solder integrity.
2. Worst Case Circuit Analysis (WCCA) identification of end of life margins. For Class A all circuits must be analyzed. For Class B the most susceptible circuits to part parameter variations are analyzed. For Class C and D there may be little margin required and test may be used as a substitute for the analysis.

Process oversight. Process oversight by independent management and subject matter experts evaluating both process application and product fulfillment of requirements and mission needs.

Examples include government and contractor independent assessments performed at contractual milestones or on-demand due to non-conformance issues. The oversight can range from insight obtained through review and approval of contractual documents to both structured and tabletop reviews, to boards convened to resolve major issues.

Process relationships. Degree of overlap of the mission success processes in preventing a fault, either internally or externally introduced, during the development process or in operation, from preventing or degrading mission success.

Examples

1. Extensive screening of EEE parts in Mission Class A and B systems provides assurance that the mission will not experience infant mortalities. However, rigorous system level testing at the assembly level (proto-qual or proto-flight) can be used in Class C and D systems to precipitate some latent defects that will bound the risk for short duration missions with reduce costs and part procurement times.
2. System safety requires interlocks to assure inhibit design requirements are met in all Class A and B missions but procedural controls can achieve the same risk avoidance, albeit at potentially higher risks for Class C and D risk profiles.
3. Risk mitigation burn-down plans for Class A and B mission classes assure residual risk is acceptable for a given profile in line with development. Independent reviews can capture risks and recommend risk burn-downs, albeit with the latency of the reviews in the designs, and still providing a level of assurance of mission success.
4. Material Review Board actions capture and fix local hardware anomalies for all the mission risk classes, but the Class C and D risk profiles may not execute the more rigorous Failure Review Board process increasing the probability of failure recurrence since the Material Review Board focus is primarily on proximate cause versus the Failure Review Board investigation of true root cause and contributing factors.

4.2 Guideline Usage in Formulation of Program Risk Strategy

Given a critical evaluation of the Appendix processes and reviewing their execution perspective the following are potential ways in which these guidelines can be used to support the programs risk strategy.

1. To engender a thought process for establishing an optimal acquisition risk strategy that balances program constraints with the needed characteristics for mission success. Critical evaluation must consider programmatic constraints and mission needs in the context of required performance, robustness, implementation, and operational risks.

2. Support communication between the customers and contractors to set the initial risk tolerance and risk profile expectations. These guidelines serve as an initial set of typical process execution that facilitate alignment between customer and contractor expectations for development.

3. Comparison of the contractual requirements and contractor command media to the mission class guidelines, and take action to address gaps that may exist.

4. Support the critical evaluation required for dialing up or down the risk of a given risk tolerance profile. The MA processes are established for how they are typically executed in a given mission risk class. However, as established in risk balance, the processes are not executed in a vacuum and must be viewed in a system context on achieving an optimal risk posture given programmatic constraints.

5. Provide a foundation for contractors to cost a given mission risk class. The risk profile cases are fleshed out according to the 16 core and supporting processes for ensuring mission success. The typical execution profiles in a given risk class can be used to guide the bottom-up costing for a given risk profile.

5. Risk Class Process Summary

This section provides a summary of the detailed risk class matrices captured in the first three appendixes that identify mission Class A through D typical process execution. The summary table below captures one row for each of the 16 processes. The appendixes process matrices examine each process in detail including the constituent elements of each process.

The typical process execution captured across the A to D mission risk class profiles provide the basis for initiating a critical evaluation for establishing the program's risk strategy as introduced in section 4. Performing a critical evaluation for a given acquisition requires detailed programmatic, funding, and mission requirements discussions between the acquisition agency and the contractor(s). The objective of the evaluation is to achieve the optimal development architecture given programmatic constraints and mission needs. Appendix D, Risk Balance Critical Evaluation Methodology" identifies key drivers for this evaluation. Drivers include class of mission, mission specific requirements, mission environments, funding strategy and other mission and programmatic objectives. Both the programmatic baseline and its funding strategy must be in alignment with an achievable development baseline that effectively manages risks to mission success including performance, robustness, implementation, and operations risks. Appendix D identifies a methodology for management of risk uncertainty in the development baseline and achieving an optimal risk balance.

Table 4. MA Process Mission Class Summary.

MA Process	Class A	Class B	Class C	Class D
Design Assurance	• **Contractor**: Full design assurance practices, Test driven verification • **Independent Assessment**: Test-Like-You-Fly (TLYF) exceptions, Manufacturing Flow, Millions of Instructions per Second (MIPS) • **Government**: Full review and approval of all processes and products	• **Contractor**: Full design assurance practices • **Independent Assessment**: TLYF exceptions, Manufacturing Flow, MIPS • **Government**: Review and concurrence on process and products, Audit • **Delta**: Reduction in deliveries and formal approval	• **Delta**: Best Practices based, Funding type programmatic control • **Contractor**: Design assurance practices • **Independent Assessment**: Internal TLYF, MIPs • **Government:** Review and concurrence, Audit	• **Delta**: Developer discretion programmatic control • **Contractor**: Essential design assurance practices to mission • **Government:** Periodic review and approval
Requirements Analysis and Validation	• **Contractor**: Validation of Concept of Operations (CONOPS), user scenarios, system readiness, compliance; Subcontractor approval • **Independent Assessment**: for quality, traceability, mission effectiveness, cost/schedule, mission analysis, verification and validation (V&V) of models and simulations • **Government**: Approval (unit level)	• **Delta**: Reduction in deliveries and formal approval • **Contractor**: Class A plus Assume more of oversight responsibility • **Independent Assessment**: Class A Elements • **Government**: Approval (Unit)	• **Delta**: Best practices based, Funding type programmatic oversight • **Contractor**: Mission validation, V&V • **Independent Assessment**: traceability, effectiveness • **Government:** Approval (System)	• **Delta**: Developer discretion programmatic oversight • **Contractor**: Critical requirements flow down • **Government:** Approval (System)
Parts, Materials and Processes	• **Part Quality**: Level 1 • **PMPCB**: Customer voting membership • **Radiation**: RDM 2X lot specific, 4X non lot data, SEE <75Mev/ng/ sqcm, slant ray analysis • **Radiation Testing**: <margin • **Material**: Heritage envelope or test qualification • **Material approval**: Formal	• **Part Quality**: Level 2 • **PMPCB**: Customer voting negotiated • **Radiation**: Radiation design margin (RDM) 2X lot specific, 4X non lot data, SEE <75Mev/ng/sqcm • **Radiation Testing**: <margin • **Material**: Heritage envelope or test qualification • **Material approval**: Formal	• **Part Quality**: Level 3 • **PMPCB**: No customer voting • **Radiation**: RDM 2X, SEE <37 Mev/ng/sqcm • **Radiation Testing**: Based on data evaluation • **Material**: Heritage envelope or test/analysis qualification • **Material approval**: Informal	• **Part Quality**: Per parts management plan • **PMPCB**: Less formal • **Radiation**: Scoped to critical design • **Radiation Testing**: Scoped to critical design • **Material**: Parts, Materials and Processes Control Board (PMPCB) acceptance • **Material approval**: Informal

MA Process	Class A	Class B	Class C	Class D
Environmental Compatibility	• Environmental compatibility analysis of orbit, mission life, launch factors, mission scenarios • Mission requirements decomposed into individual program plans • Requirement compliance satisfied through testing • No waivers on key performance parameters • Greatest design margins (qual levels)	• Environmental compatibility analysis same as Class A • Mission requirements decomposed same as Class A • Physical testing balanced with analysis, modeling and simulation • Waivers allowed on less critical requirements • Reduced design margins (protoqual levels)	• Environmental compatibility Vetted for impact to other systems and payloads • Mission requirements decomposed based on contractor best practices • Physical testing only used to satisfy mission critical requirements • Waivers acceptable with justified risk impact to mission success • Reduced design margins (protoqual levels)	• Environmental compatibility driven by primary payloads • Mission requirements decomposed based on prior experience • Testing driven for major requirements or driven by primary payload • Waivers acceptable as per Class C for defined requirements • Minimal design margins
Reliability Engineering	• **Monitoring/Control**: Comprehensive policy, procedures, monitoring and control processes • **System Reliability**: System models hardware and software, performance trending, mission reliability • **Design Analysis**: Failure Modes and Effects Analysis (FMEA) flight/ground, mechanism Fault Tree Analysis (FTAs), and full worst case analysis (WCA) • **Testing/Screening**: Subassembly/ part level qualification and assembly level environmental stress screening (ESS) on volume units • **Anomaly Management**: First power application reporting, formal closed loop system	• **Monitoring/Control**: Policy, procedures, monitoring and control processes with reduced margin requirements • **System Reliability**: Minimum SPFs allowed, key parameter trending • **Design Analysis**: Failure Modes and Effects Analysis (FMEA) redundancy boundary, mechanism Fault Tree Analysis (FTAs), and reduce worst case analysis (WCA) for susceptible circuits • **Testing**: Subassy/part level qualification and assembly level environmental stress screening (ESS) on volume units • **Anomaly Management**: Negotiated first power application reporting, formal closed loop system	• **Monitoring/Control**: Monitoring for product spec compliance • **System Reliability**: Single string/selective redundancy, parts count analysis, trending limited • **Design Analysis**: Functional Failure Modes and Effects Analysis (FMEA) redundancy boundary, critical mechanism Fault Tree Analysis (FTAs), and reduce worst case analysis (WCA) for high risk designs • **Testing**: Reduced margins, critical mission reliability driven • **Anomaly Management**: Acceptance reporting, formal closed loop system	• **Monitoring/Control**: Monitoring required for personnel safety • **System Reliability**: Single string baseline, analysis limited • **Design Analysis**: S/C payload Failure Modes and Effects Analysis (FMEA) redundancy boundary, safety critical mechanism Fault Tree Analysis (FTAs), and recommended worst case analysis (WCA) not required • **Testing**: Qualification to safety critical items only • **Anomaly Management**: Internal capture in nonconformance system

MA Process	Class A	Class B	Class C	Class D
System Safety	• **Safety Analysis**: Preliminary hazards assessment (PHA), subsystem hazard analysis (SSHA), system hazard analysis (SHA), software system analysis (SSA), operating and support hazard analysis (OSHA), on-orbit hazard analysis, debris • **Safety Risk Assessment**: Hazard likelihood/severity • **Mishap Reporting**: Formal mishap investigation and reporting	• **Safety Analysis**: PHA, SSHA, OSHA • **Safety Risk Assessment**: Same as Class A • **Mishap Reporting**: Same as Class A	• **Safety Analysis**: PHA, OSHA • **Safety Risk Assessment**: Same as Class A • **Mishap Reporting**: Same as Class A	• **Safety Analysis**: PHA, OSHA • **Safety Risk Assessment**: Same as Class A • **Mishap Reporting**: Same as Class A
Configuration/ Change Management	• Formal configuration management (CM) plans, processes and boards integrated throughout the supplier chain with government approval for baseline/change control and configuration audits	• Same as Class A. Government review at sub/supplier levels may be limited	• CM plan not a deliverable; rely on contractor best practices • Formal configuration management is usually initiated once subsystems are integrated • Software CM is initiated earlier	• Not required; applied at the discretion of the developer using best practices
Integration, Test and Evaluation	• **Integration**: Full standard compliance, interface checkout, full copper path evaluation, high fidelity simulator checkout, in-process screening • **Testing – Requirements Compliance and Validation**: Qualification/proto-qualification, full software validation, operability including redundancy checkout, System test including interfaces, launch support test • **TLYF:** All exceptions documented and approved by the customer • **Evaluation**: Maximum customer engagement	• **Integration**: Full standard compliance, interface checkout, full copper path evaluation, Suitable fidelity simulator checkout, In-process Screening • **Testing – Requirements Compliance and Validation**: Proto-qualification with delta cycles, margins, duration, full software validation, operability including redundancy checkout, System test including interfaces, launch support test • **TLYF:** All exceptions documented and approved by the customer • **Evaluation**: Customer review and approval at system/subsystem level	• **Integration**: Standard compliance with tailoring, interface internal checkout, final integration evaluation, GSE validated simulator checkout, reduced in-process screening • **Testing – Requirements Compliance and Validation**: Proto-qualification new hardware/acceptance heritage with delta cycles, margins, duration, software best practices validation, operability, partial system test including interfaces, launch support test • **Evaluation**: Customer review and approval at system level	• **Integration**: Follows best practices, final integration evaluation, GSE certified simulator checkout • **Testing – Requirements Compliance and Validation**: Safety and compatibility testing, software best practices validation, operability. Verification not validation • **Evaluation**: Customer approval of program plan and review at key milestones

MA Process	Class A	Class B	Class C	Class D
Risk Assessment and Management	• Formal joint risk management plan with multiple RMBs • Active management of residual risk • RMB chaired by contractor with customer active participation • Customer approval of programmatic and technical risks mitigation plans	• Joint risk management planning with contractor lead • Residual Risk kept within risk profile • RMB chaired by contractor with customer participation • Customer monitoring of risk mitigation plans	• Contractor risk management planning with customer concurrence • Residual Risk kept within risk profile • RMB internal to contractor • Customer monitoring mission compliance, not margins	• Contractor risk management planning with customer concurrence • Residual risk kept within risk profile • RMB internal to contractor • Customer monitoring mission compliance, not margins
Independent Reviews	• Numerous programmatic and technical reviews • SMEs from customer community and contractor • Full standards compliance for entry and exit criteria • All issues tracked to closure	• Small reduction in programmatic and technical reviews • SMEs from customer community and contractor • Standards compliance for negotiated entry and exit criteria • All issues tracked to closure	• Limited programmatic and technical reviews • SMEs from customer community and contractor • General Standards for compliance review conduction • All issues tracked to closure • Review only for moderate to high risk items	• Few key milestone reviews • Internal review based on contractor standards • Best practice standards • All issues tracked to closure • Review only for high risk items
Hardware Quality Assurance	• Full ISO 9001:2000 and AS9100C compliance • Minimum tailoring • Full set of HQA processes to ensure program meets contract and assures mission success.	• Same as Class A program with the exception that there is less customer oversight in areas such as design review and purchasing documents.	• Greatly reduced customer involvement • Relax processes in purchasing, traceability, verification, and environmental controls • Less frequent audits • First article inspection focused on key design features versus 100% verification	• Greater HQA tailoring focused only on key controls and inspection • Audits not typically performed • Nonconformance handling and product preservation potentially done by program resources other than HQA • No first article inspection

MA Process	Class A	Class B	Class C	Class D
Software Assurance	• Full software/firmware SQA process • Independent assessment by customer and contractor SMEs • Detailed artifact capture/closeout • Statistical Reliability Growth • Software Safety Program • SCCB management • Test witnessing	• Same SQA process as Class A • Independent assessment by contractor with customer audit • Core artifact capture/closeout • Statistical Reliability Growth • Significant hazard Software Safety • SCCB management • Test monitoring	• Contractor SQA process • Heritage reuse model • Critical artifact capture/closeout • Process focused Reliability growth • Major hazard Software Safety • SCCB support • Selective test monitoring	• Contractor SQA process recommended • In-line reviews • Major artifacts • Process focused Reliability growth • Personnel/Interface Hazard Software Safety • SCCB support • Test auditing
Supplier Quality Assurance	• AS9100 certification at contractor, Tier 1 and Tier 2 • Full flow down of customer requirements • Formal verification of supplier certification and process/activity artifacts • Quality Standards customer driven	• AS9100 certification at contractor and major suppliers with intent verification at lower levels • Tailored flow down of customer requirements • Formal verification of supplier certification and process/activity artifacts with tailoring in QMS continuous improvement programs, and documentation process • Quality Standards combined customer/contractor driven	• AS9100 certification at contractor and major suppliers desirable with self-report allowable • Reliance on supplier best practices • Contractual QA based on minimum product standards • Quality Standards best practice driven	• Contractor meets the intent of AS9100 certification at contractor and verification of QA process at supplier for safety-critical elements • Reliance on PI best judgment of acceptable levels of QA • Only key QA practices required
Failure Review Board	• Strive for root cause, seek to eliminate defects in all sibling hardware and verify effective preventive measures • Formal FRB meetings with customer as voting member • FRB control of investigation • Artifacts well documented • Unverified failure commonly results in worst case change out	• Strive for root cause, seek to eliminate defects in all sibling hardware and verify effective preventive measures • Formal FRB meetings with customer but not as voting member • FRB delegation of investigation to cognizant engineer or supplier but closely monitored • Artifacts well documented • Unverified failure thorough evaluation with worst case change out or contingency planning	• Strive for root cause but with a reduced level of control and rigor • FRB meetings based on contractor best practices with results provided to the customer • FRB investigation led by cognizant engineer and suppliers • Less formal presentation of results • Unverified failure processed per contractor policy with eye to cost	• Focus is on actions to return the hardware to service • Failure investigation team may be limited to cognizant engineer and QA (could include supplier) • Less formal results captured in non-conformance system • Unverified failure monitored

MA Process	Class A	Class B	Class C	Class D
Corrective/ Preventative Action Board	• Likely to have a program specific C/PAB especially for multiple vehicle programs • Same processes as for wide area C/PABs • Programs generate data to support actions to investigate and correct problems • Routine reporting to customer	• Rare to have program unique C/PAB • Programs support wider area C/PABs at company level • Programs generate data used to identify systemic issues or take actions directed by C/PAB • Customer reporting of actions impacting program	• No program unique C/PAB • Programs support wider area C/PABs at company level • Programs generate data used to identify systemic issues or take actions directed by C/PAB • Customer reporting of actions impacting program	• No program unique C/PAB • Programs support wider area C/PABs at company level • Programs generate data used to identify systemic issues or take actions directed by C/PAB • Customer reporting of actions impacting program • Process may be ad hoc for academic and research communities
Alerts, Information Bulletins	• Alerts/Bulletins assessed as potential risks and mitigate to program risk posture • Review of as-design/built, in-line screens, impacts • Supplier same rigor • Regular customer status	• Alerts/Bulletins assessed as potential risks and mitigate to program risk posture • Review similar to Class A but dictated by company policy • Low risk use-as-is • Supplier reporting on impact • Customer status on impact	• Alerts/Bulletins assessed as potential risks and mitigate to program risk posture • Review same as Class B • Moderate risk use-as-is • Supplier responsibility or contractor performs • Only compliance reporting	• Alerts/Bulletins assessed as potential risks and mitigate to program risk posture • Review same as Class B • Moderate risk use-as-is • Contractor performs • Only compliance reporting

6. Appendix Risk Class Matrices Layout

This section outlines the format of appendixes containing detailed mission risk class matrices. The process matrices are organized into three appendixes with mission class typical process execution corresponding to the class definitions. Each process area examines its applications for each of the mission risk class profiles, some effectiveness tips for the application, and references that are specific to the creation of the particular appendix. Each risk class matrix is laid out according to:

Title

Contributing team members

A,B,C-1. **Introduction.** Provides information about what the matrix covers (or does not cover). Explanation of any special nuances associated with the reading of the matrix.

A,B,C-2. **Definitions.** Definitions are provided to define how specific terms are used within the process risk class matrixes.

A,B,C-3. **Matrix.** Process detailed by mission risk class

A,B,C-4. **Matrix Summary.** Summary that essentially describes what was presented in the matrix as major characteristics for the risk class types. This summary provides the rationale for the matrix process assignments to ensure the matrix will remain clear and unambiguous especially after a period of time.

A,B,C-5. **Effectiveness Tips.** Effectiveness tips of lessons learned, rules, or heuristics in application of the matrix.

A,B,C-6. **References.** References list of the references used to create the matrix

7. Future Work Recommendations

Future work proposed is based on findings from the development of Mission Risk Class Matrices and from review comments that were out of the scope for this document. Each recommended future work product is presented as a standalone product.

- Launch site activation includes the installation, checkout, and acceptance of the new payload ground support system, including the first space vehicle/payload processing for the first launch. Activation is non-recurring, where launch operations is recurring space vehicle processing activity for launch. Recommend producing guidelines to differentiate between launch site activation for first space vehicle contrasted to recurring space vehicle processing activity for launch; add specifics for missions such as LEO, GEO, and deep space.
- The design assurance appendix is based on a definition in TOR -2009(8591)-11, Design Assurance Guide. This definition is in conflict with TOR -2010(8591)-18, Mission Assurance Program Framework. Recommend preparation of an alternate design assurance chapter that is consistent with the "Mission Assurance Framework" definition.
- During development of the appendix material for the independent review matrices it was determined that a useful product would be an in-depth analysis of all entrance and exit criteria for each review to determine mission risk classes A-D specific entrance and exit criteria.
- Determine appropriate contractor processes, command media, or government/industry standards by which supplier quality assurance tailoring can be formalized and institutionalized on a consistent basis.
- As was documented in the "Recommended Next Steps and Future Work" portion of the TOR -2010(8591)-18, Mission Assurance Program Framework document (2010 MAIW effort), the MAIW should consider sponsoring a future topic team to create work products for the Corrective/Preventive Action Board process

8. Acronyms

Acronym	Name/Phrase
ANSI/PMI	American National Standards Institute Project Management Institute
Ao	Operational Availability
BIST RR	Baseline Integrated System Test Readiness Review
BRR	Build Readiness Review
CAB	Change Boards
CCB	Configuration Control Board
CDR	Critical Design Review
CFO	Chief Financial Officer
CI	Configuration Item
CIL	Critical Items List
CM	Configuration Management
CMMI-A	Capability Maturity Model Integration - Acquisition
CMP	Change Management Planning
CMP	Configuration Management Plan
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
CSA	Configuration Status Accounting
DAU	Defense Acquisition University
DDRE	Deputy Director for Research and Engineering
DOD	Department of Defense
EC	Environmental Compatibility
EEE	Electrical, Electromechanical and Electronics
ESS	Environmental Stress Screening
EM	Engineering Model
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EOL	End of Life
ESD	Electrostatic discharge
ESS	Environmental Stress Screening
EVA	Extreme Value Analysis
FCA	Functional Configuration Audit
FMEA	Failure Modes and Effects Analysis
FFP	Firm Fixed Price
FMECA	Failure Modes Effects and Criticality Analysis
FRB	Failure Review Board
FRR	Flight Readiness Review
FTA	Fault Tree Analysis
GIDEP	Government/Industry Data Exchange Program

Acronym	Name/Phrase
govt	Government
GSE	Ground Support Equipment
HW	Hardware
I&T	Integration and Test
IBR	Integrated Baseline Review
ICD	Interface Control Document
ICR	Initial Checkout Review
IDR	Internal Design Review
IDR	Independent Design Review
IEC	International Electrotechnical Commission
IPT	Integrated Product Team
IR	Independent Review
IRRT	Independent Review Readiness Team
IRT	Independent Review Team
ISO	International Standards Organization
IV&V	Independent Verification and Validation
JIMO	Jupiter Icy Moon Orbiter
KPP	Key Performance Parameter
LL	Limited Life
MA	Mission Assurance
MAIW	Mission Assurance Improvement Workshop
MAM	Mission Assurance Manager
MDA	Missile Defense Agency
Mev	Mega(Million) Electron-Volts
MIL-STD	Military Standard
MRR	Mission Readiness Review
MTTR	Mean Time To Repair
MUA	Material Usage Agreement
NADAP	Third party certification authority for special processes
NASA	National Aeronautical and Astronautics Administration
NDT	Non-destructive Test
NEPA	National Environmental Policy Act
ng	Nanogram
NSS	National Security Space
ODC	Other Direct Costs
OEM	Original Equipment Manufacturer
OSHA	Occupational Health and Safety Administration
PCA	Physical Configuration Audit
PCB	Printed Circuit Board
PDR	Preliminary Design Review

Acronym	Name/Phrase
PER	Pre-Environmental Review
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard List
PM	Program Manager
PMBOK	Program Managers Book Of Knowledge
PRA	Probabilistic Risk Assessment
PRR	Production Readiness Review
PSA	Parts Stress Analysis
PSR	Pre-Ship Review
QA	Quality Assurance
QMS	Quality Management System
R&D	Research and Development
RDM	Radiation Design Margin
RMB	Risk Management Board
RMP	Risk Management Plan
RR	Readiness Review
SAE AS (as in AS9100)	Society of Automotive Engineers Aeronautical Standard
SCAR	Supplier Corrective Action Requests
DCMA	Defense Contract Management Agency
SDR	System Definition Review
SEB	Single Event Burn-Out
SEE	Single Event Effects
SEGR	Single Event Gate Rupture
SEL	Single Event Latch-Up
SEU	Single Event Upset
SHA	System Hazard Analysis
SMC-S-nnn	Space and Missile Systems Center Standard
SPF	Single Point Failure
SQA	Supplier Quality Assurance
SQCM	Supplier Quality Configuration Management
SQIC	Space Quality Improvement Council
SRCA	Safety Requirements/Criteria Analysis
SRR	System Requirements Review
SSHA	Subsystem Hazard Analysis
STE	Special test equipment
subassy	Subassembly
SV	Space Vehicle
SW	Software
TECR	Test and Evaluation Campaign Review

Acronym	Name/Phrase
TID	Total Ionizing Dose
TOR	Technical Operating Report (a product of The Aerospace Corporation)
TPM	Technical Performance Measure
TRR	Test Readiness Review
U.S.	United States
V&V	Verification and Validation
WCA	Worst Case Analysis

Appendix A: Program Execution Processes

Appendix A captures the mission risk class matrixes for the program execution of the MA framework processes for mission success. Processes include:

- A1: Requirement Analysis and Validation
- A2: Design Assurance
- A3: Parts, Materials and Processes
- A4: Environmental Compatibility
- A5: Reliability Engineering
- A6: System Safety
- A7: Configuration/Change Management
- A8: Integration, Test and Evaluation

Appendix A1: Requirements Analysis and Validation Process

Matthew Fahl, Harris Corporation
Gail Johnson-Roth, The Aerospace Corporation
David Michel, Raytheon
David Kalian, The Boeing Company

A1-1 Introduction

The primary objective of the requirements analysis and validation process is to ensure (a) a complete and optimal set of requirements is established and that (b) a one-to-one association exists between a derived requirement and its source, the implementation, the verification method and verification results. Key mission assurance activities include: evaluation of requirements traceability; mission effectiveness; cost and schedule element evaluation; mission analysis validation; and evaluation of models and simulations used to analyze requirements. These activities are performed both in-line with development, typically by systems engineering and independently as a crosscheck typically by a company mission assurance function. The requirements analysis and validation matrix highlights both independent and in-line execution of this process. This process establishes the requirements in the earliest phases of the program life cycle and establishes the technical baseline of the space system development activities.

This chapter provides guidelines for applying effective requirements analysis and validation to space systems. The methods of requirements development, validation, and verification planning may be tailored to meet the needs of the program; however, a requirements process is either required or recommended for any space system development activity to ensure clarification of users' needs. The process may be applied to all space flight systems; to include deliverable payloads, space vehicles, or other associated products. Formal requirements analysis and validation management may be dictated by the acquisition authority per the contract or developed in accordance with the contractor's best practices commensurate with the level of risk associated with the specific mission. Ultimately, the developer is responsible for implementing an organized, systematic requirements process to increase the likelihood of achieving mission success.

A1-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, and are not intended as general standalone industry standard definitions.

Requirements Development

- Evaluation of requirements quality. Requirements should be evaluated as to the "goodness" based on several factors. Requirements should be measurable, verifiable, unambiguous, and specific. They should not dictate design.
- Evaluation of requirements traceability. An evaluation should be conducted to ensure requirements trace to top-level system requirements documents such as capability development documents, concept of operations, and government or procuring agency directives and policy. Top-to-bottom traces are conducted as well as bottom to top to identify orphaned or childless requirements. The resulting set of allocated system requirements (functional, performance, interface, environment, and process) are subjected to a final review to assure that they are verifiable with the verification methods selected. Different system and operational views are also developed to assure self-consistency across the functional areas, 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 is required.

- Mission effectiveness evaluation. The expected system performance should be verified through system modeling and simulations. The system performance attributes are quantified and compared against baseline design reference case tests that are conducted by the developing contractor, and independently conducted on a different set of tools than those used by the developing contractor(s).
- Cost and Schedule Evaluation. Cost and schedule elements should be independently evaluated at different levels within the government to assure that realistic cost profiles and detailed schedules are being used by the procuring agency and that adequate management reserves exist to handle unforeseen problems. It is important to recognize that without adequate resources, the desired technical performance may not be achievable.
- Mission Analysis Validation. An evaluation should be conducted to ensure users' needs are correctly captured and system performance parameters distilled to evaluate system capabilities as the system concepts evolve and trade studies emerge.
- Models and Simulations. Models and simulations used in requirements analysis must be verified and validated in order to have confidence in their output. This activity 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.

Requirements Validation

The objective of requirements validation is to ensure that the right set of requirements, if used properly to guide a system's development, will result in a system that meets the users' expectations and needs. The primary means to accomplish this is through modeling and simulation. Stakeholder buy-in is imperative early in the requirements development process including mission assurance. The active participation of users and other important stakeholders during the requirements validation effort is an important aspect of the process.

- Evaluate CONOPS. Ensure that the operational environment(s) in which the system will operate have been defined. The CONOPS should show how the system fits into its intended operational environment. It should also include a description of how people use the system (operations, maintenance, and support).
- Evaluate user scenarios. Operational user scenarios describe the individual operations that are used to fulfill the mission scenarios. These can be used individually or in sequence to complete the mission scenarios. The user scenarios should be defined to be representative of actual system use. These are the sequence of actions taken by the operator and performed by the system for different system operations.
- Evaluate system readiness. Refers to the ability to meet Key Performance Parameters (KPPs). KPPs are those system attributes considered most critical or essential for an effective space system capability. Effectiveness measures are decomposed to KPPs, which are critical to meeting system effectiveness thresholds (i.e., availability, reliability). KPP requirements must be validated to ensure system readiness meets user needs.

Verification Planning

Verification is a systematic, thorough, rigorous, and iterative, hierarchical process that certifies system requirements (including interfaces and mission requirements and all lower-tier requirements) have been fully satisfied by the end item being acquired. During the Requirements Analysis process, verification planning is conducted to the level necessary to ensure that each requirement is verifiable and the recommended method of verification is appropriate. Verification methods include Test, Demonstration, Inspection, and Analysis.

A1-3 Matrix - Requirements Analysis and Validation

Requirement	Class A	Class B	Class C	Class D
Requirements Development Process	• Required by contract with deliverables Customer approved. Contract requires prime contractor to flow to subs for major elements.	• Same as Class A	• Contract requires prime contractor's best practices. Customer reviews evidences.	• Recommended. (Not required by contractor) Discretion of SV/payload developer that accepts risk. • Level of effort determined by developer commensurate with program and best practices.
Evaluation of requirements quality (measurable, verifiable, etc.)	• Independent customer assessment conducted to the unit level	• Same as Class A	• Contractor assessment usually performed to the system level.	• Recommended. Discretion of developer based on requirements fidelity
Evaluation of requirements traceability conducted	• Independent customer evaluation conducted down to the unit level	• Same as Class A	• Contractor conducted in accordance with their best practices mitigating development risk	• Discretion of developer. Not always conducted. Dependent on fidelity of flow down
Mission effectiveness evaluation	• Contractor evaluation; independent assessment conducted by customer	• Same as Class A	• Recommended, but not required. Dependent on performance expectations	• Discretion of developer based on performance expectations
Cost and schedule evaluation	• Contractor required to conduct evaluation; independent assessment conducted by customer	• Same as Class A	• For CP contract contractor required to conduct evaluation and customer performs independent evaluation at higher level. For FFP contractor best practices	• Not usually performed, as contract is almost always FFP. Dependent on contractor best practices
Mission Analysis Validation	• Required by contract and customer approved	• Same as Class A	• Negotiated at discrete intervals during development	• Recommended. Developer Discretion to conduct and evolve concept and conduct trades for mission success

Requirement	Class A	Class B	Class C	Class D
Verify and validate models and simulations	• Required by contract. Independent assessment conducted of actual/predicted behavior	• Same as Class A	• Contractor required to verify and validate; customer reviews evidences of compliance	• Models and simulations use as well as verification/validation at discretion of experimenter
Requirements Validation	• Required by contract. Customer approved	• Same as Class A	• Required by contract, using contractor's best practice. Customer reviews.	• Discretion of SV/ payload developer that accepts mission risk.
Evaluate CONOPS	• Required by contract. Customer approved	• Same as Class A	• Required by contract, using contractor's best practice. Customer reviews.	• Detail dependent on acquiring agency
Evaluate user scenarios	• Required by contract. Customer approved	• Same as Class A	• Based on contractor's best practice. Customer reviews.	• Discretion of SV/payload developer that accepts mission risk.
Evaluate system readiness (ability to meet KPPs)	• Required by contract. Customer approved	• Same as Class A	• Based on contractor's best practice. Customer reviews.	• Discretion of SV/ payload developer that accepts mission risk.
Verification Planning	• Required by contract. Customer approved	• Same as Class A	• Based on contractor's best practice. Customer reviews.	• Discretion of SV/ payload developer that accepts mission risk.

A1-4 Summary of Risk Classes

Class A. The government, or its representative agency, will approve the results of the requirements development process to the subsystem level. The prime contractor is required to approve the requirement development process of subcontractors for major elements. Independent assessment is conducted to ensure the quality of the requirements, traceability, mission effectiveness, cost and schedule, mission analysis, and verification and validation of the models and simulations. The contractor is required to perform requirements validation to include evaluation of the CONOPS, user scenarios, and evaluation of the system readiness, and provide evidences of compliance for government approval. The government also approves evidences supplied by the contractor that all requirements have been verified.

Class B. For the most part, the requirements analysis and development processes is the same for Class B systems as it is for Class A systems, although the deliveries and subsequent approvals may be less formal than that conducted on Class A systems. For Class B a prime contractor may be the oversight agency with reduced government oversight. The customer will approve the results of the requirements development process to the subsystem level. The prime contractor is required to approve the requirement development process of subcontractors for major elements. Independent assessment is usually conducted to ensure the quality of the requirements, traceability, mission effectiveness, cost and schedule, mission analysis, and verification and validation of the models and simulations. The contractor is required to perform validation and verification of the requirements, and deliver evidences of completion that are subject to approval by the customer or its representative agency.

Class C. The customer requires the contractor to conduct the requirements development process according to best practices. The government reviews the outputs of the process and will independently evaluate the requirements to the system level. An independent assessment of the traceability and the mission effectiveness may also be conducted. An informal evaluation of the cost and schedule will be conducted with the risk emphasis on the meeting the budgetary constraints of the program dependent on the contract funding vehicle, e.g., cost plus or fixed price. The contractor performs mission validation activities as well as verification and validation of models and simulations that are commensurate with the risk posture of the program. The customer reviews the outputs of these efforts. The contractor performs validation and verification of the requirements in accordance with their best practices, and provides evidences of completion for customer review.

Class D. Programs conduct requirements development at the developer's discretion, accepting any resultant mission risk. All associated development activities are optional and are at the discretion of the developer given the nature of the customer requirements flow down. Requirements may be further assessed if they are determined to be critical components of the mission; a mission analysis validation is recommended but not required; and models and simulation verification and validation is again at the discretion of the developer. Requirements validation and verification activities are recommended, and if performed are in accordance to the developer's best practices.

A1-5 Effectiveness TIPS (Lessons Learned)

- All requirements need to be decomposed and flowed down
  - Identify each requirement with a unique ID
  - Use requirements management software to assist process
- Critical to write clear and concise requirements
  - Specify what is needed rather than how solution is implemented

  - State requirements in positive (shall) instead of negative (shall not)

- Requirements should be written with system verification in mind

  - Requirements must have at least one verification method, preferably including a test

A1-6 References

1. Aerospace Report TOR-2007(8546)-6018, *Mission Assurance Guide*.
2. Aerospace Report TOR-2011(8591)-5, *Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space*.
3. MAIW Aerospace Report TOR-2010(8591)-18, *Mission Assurance Program Framework*.

Appendix A2: Design Assurance

Dave Michel (Raytheon)
Andy Penner (Lockheed Martin)

A2-1 Introduction

The design assurance "process" consists of multiple processes or activities that ensure the conceptual, preliminary, and detailed designs perform their intended function over all the operating conditions and throughout the design life. The 15 separate activities that make up the design assurance process each contribute to mission success by providing a framework in which the program may achieve its goals. It is expected that multiple technical disciplines (systems and design engineering, quality assurance, systems safety test, manufacturing, etc.) will each play a role in the development and execution of the various design assurance elements. This section will document the elements and identify the key differences between execution of the elements across the four mission classes. The definition and elements of design assurance were extracted from Appendix E of TOR-2009(8591)-11, Design Assurance Guide. This definition is not in accordance with the TOR -2010(8591)-18, Mission Assurance Program Framework, definition of design assurance.

The primary differences between the mission classes revolve around the degree to which the customer (government) is involved in the execution of the design assurance elements, and in the process execution rigor, depth of analysis required, and level of effort expended to complete the various tasks. For Class A missions, the customer typically requires formal element plans, approves these plans, and then closely monitors the effectiveness of the contractor in the process implementation. Class B missions generally follow a similar tact; however, the level of oversight may be reduced, and minor deviations may be accepted. Notable variation occurs with the Class C and D missions, where process review may take the place of process approval, and execution of company practices is deemed sufficient instead of required formal program plans. These decisions result in lower costs, but a higher risk profile.

The material in this appendix provides further detail regarding the different elements, and relates how each element supports overall mission success for a particular mission risk class. A matrix of the 15 design assurance elements is provided to provide a summary of the mission class differences for each of the elements.

A2-2 Definitions of the Design Assurance Elements

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which the risk profile can be developed and are not intended as general standalone industry standard definitions.

Planning. The various plans required for the successful execution of a program are listed. Each of these plans identifies how the contractor will complete key tasks needed to design, build, analyze, inspect, test, and operate the system. Properly developed, monitored, and executed planning leads to a controlled program with a higher likelihood of achieving mission success.

Requirements. A complete understanding of the mission requirements is vital to achieving a successful mission. The mission requirements must be analyzed, allocated and/or derived, verified, and validated to ensure that the product delivered to the customer meets their needs. (Appendix A1 addresses requirements analysis and validation in more detail.)

Design. The design process includes trade studies, choice of part reliability levels, the number and depth of design reviews, and architecture decisions regarding the type and level of redundancy and fault protection.

Analysis. Multiple analyses are needed for every mission, as it is impractical or impossible to expose the flight hardware to all environments or situations that will be encountered during the mission.

Requirements Verification/Validation. Perhaps the most critical of the design assurance elements is the process that demonstrates that the design meets the intended requirements (verification) and that the right requirements were chosen to complete the mission (validation). Because of the fundamental nature of the element, all programs perform verification and validation. (Appendix A1 addresses requirements analysis and validation in more detail).

Testability. The use of foresight to develop flight hardware and systems, along with the associated ground support equipment, that furthers the testability of the spaceflight hardware will improve the odds for mission success. Hardware that is readily tested using equipment optimized for the effort will more likely meet its objectives than that subjected to a poorly planned test plan performed with equipment designed for another task.

Product Design. The control of product drawings can have a dramatic impact on a program's ability to achieve mission success. A formal, organized drawing release process, with an established drawing structure that includes checked and incorporated drawing changes will help ensure the intent of the designers is realized at product delivery. Unincorporated drawing redlines, an informal drawing release process with few or no independent checks, can result in confusion of hardware configuration, both during build and on-orbit. (Appendix A7 addresses configuration/change management in more detail).

Manufacturing. The processes involved with manufacturing include development of program-specific tooling, detailed development and maintenance of the assembly flow, and (especially for multi-vehicle programs) assessment of machinability.

Producibility. The tenets of producibility are designing hardware with manufacturing in mind and building hardware using well-established processes and materials that lead to superior product quality. This ensures that the design can be successful implemented into a compliant product.

Inspectability. By designing components or systems with inspectability in mind, a conscientious engineer can improve the odds of mission success by creating conditions that allow verification of workmanship or other requirements.

System Safety. Safety includes the federal regulations (such as OSHA requirements) intended to protect worker safety, the resulting company policies, and the Range Safety requirements that are levied on all spaceflight programs. Hazards to either personnel safety or flight hardware are identified, and then mitigations to preclude the hazard are put in place and monitored for effectiveness. (Appendix A6 addresses system safety in more detail).

Risk. A structured approach to identify and manage risk during the course of a program is vital to executing a successful mission. (Appendix B1 addresses risk assessment and management in more detail).

Lessons Learned. By reviewing and taking action of previously learned lessons, a program enhances its chances to achieve mission success. While the effectiveness of the lessons learned to aid program execution is dependent on the quality of the lessons that were captured, a dedicated process to actively seek out those lessons and act on them will yield positive results.

Cost/Schedule. The cost and schedule profile of a program can have a direct bearing on being able to achieve mission success. When cost and schedule pressures intrude into the resolution of technical problems, mission success is threatened. Therefore, it is vital that the schedule and cost performance be measured and monitored to flag potential threats.

Process Assessment. By mentoring program progress through a series of milestone reviews, the overall design assurance process can be assessed for effectiveness (i.e., ability to achieve mission success). (Appendix B2 exists solely to address independent reviews.)

A2-3 Matrix - Design Assurance

Requirement	Class A	Class B	Class C	Class D
Planning				
Design Plans Production Plans Subsystem/Payload Integration Plans Quality Plan Tooling/Manufacturing/Ground Support	• Design Assurance plan required • Customer approval of Design Plan required • Plan to include HW design assurance, certifications (facilities, equip, processes and personnel), verification approach, quality assurance, and manufacturing	• Design Assurance plan required • Customer approval of Design Plan required (minor exceptions allowed) • Plan to include HW design assurance, quality assurance, and manufacturing	• Design Assurance plan developed per company requirements • Customer review or cognizance of Plan optional (recommended) • Plan to include HW design assurance, quality assurance, and manufacturing	• Design Assurance plan developed per company requirements • Plan to include HW design assurance, quality assurance, and manufacturing
Requirements				
Functional Requirements Performance Requirements Internal/External Interface Requirements Operational Requirements Environmental Requirements Reliability and Lifetime Requirements Software Requirements Requirements Traceability	• Comprehensive verification plan require • Multiple deliverable products to the customer • Plan to include reqt's traceability, interface reqt's documentation and control, verification methods (performance, operation, environmental, reliability, and software), verification matrix	• Same as Class A	• Verification plan developed per company requirements • Some deliverable products to the customer • Plan to include reqt's traceability, interface reqt's documentation and control, verification matrix	• Verification plan developed per company requirements • No deliverable products to the customer • Plan to include reqt's traceability, verification matrix

Requirement	Class A	Class B	Class C	Class D
Design				
Trade Studies Parts, Materials, and Processes Requirements versus Capabilities Design Reliability Maintenance Packaging Architecture Product Design Design for Manufacture/Assembly/Test	• Thorough design development and maturation process with fully documented results of design process • Approved by subcontractor, prime contractor and customer • Use of funded Engineering Development Units (EDUs) is common, wide spread and expected	• Thorough design development and maturation process with fully documented results of design process • Approved by subcontractor, prime contractor and customer • Use of funded Engineering Development Units (EDUs) is common, but limited	• Tailored design development and maturation process aligned with SOW and contract • Documented in controlled program database • Approved by subcontractor and reviewed by prime contractor • Use of funded Engineering Development Units (EDUs) is unusual	• Tailored design development and maturation process aligned with SOW and contract • Documented in controlled program database • No funded EDUs
Analysis				
Feasibility Analysis Mission Analysis Functional Analysis Operational Analysis Performance Analysis	• Thorough analysis performed including: risk assessment, single point failure, reliability analysis, margin assessment in addition to all mission, functional, operational and performance analysis • Reviewed and approved by prime contractor and customer	• Thorough analysis performed including: risk assessment, single point failure, reliability analysis, margin assessment in addition to all mission, functional, operational and performance analysis • Reviewed and approved by prime contractor and customer, but not applied to 100% of subprocesses or to the same depth as with Class A	• Analyses performed to meet company reqt's • A mixture of approval and concurrence on the product by the customer • Several products may be approved as presented not as formal CDRLs but as part of milestone reviews	• Minimum set of analyses will be performed to meet contractor best practices for understanding the integrity of interfaces and safety • Customer approval will nominally be at a limited number of milestone reviews

Requirement	Class A	Class B	Class C	Class D
Requirements Verification/ Validation				
Verification and Validation Plan Verification and Validation Execution	• Low risk verification and validation approach • Approved by prime contractor and customer • "Test Like You Fly" exceptions identified, with mitigations formally documented and approved by the customer	• Low/medium risk verification and validation approach • Approved by prime contractor and customer • "Test Like You Fly" exceptions identified, with mitigations documented and reviewed by the customer	• Medium risk verification and validation approach • Reviewed by prime contractor • "Test Like You Fly" exceptions identified, with mitigations assessed on program	• Medium/high risk verification and validation approach • Reviewed by prime contractor • "Test Like You Fly" exceptions identified and mitigated per company requirements
Testability				
Integration and Test Plan Test Support Equipment	• Minimum practicable risk I&T plan • Full STE/GSE FMECA and safe to mate checkout	• Low risk I&T plan • Full STE/GSE FMECA and safe to mate checkout	• Low/medium risk I&T plan • STE/GSE safe to mate checkout prior to use in accordance with company requirements	• Medium risk I&T plan • STE/GSE safe to mate checkout prior to use in accordance with company requirements
Product Design				
Drawing Release Plan Flight Drawings Product Data Structure	• Ensure existence of product data structure and drawing release plan • Customer approves plan • Independent design assessment reviews and engineering models req'd to verify design prior to start of flight unit	• Ensure existence of product data structure and drawing release plan • Customer approves plan • Independent design assessment reviews and engineering models req'd to verify design prior to start of flight unit • Minor deviations more common than with Class A	• Ensure existence of product data structure and drawing release plan • Customer may review plan but without formal approval • Independent design assessment reviews and engineering models req'd to verify design prior to start of flight unit	• Review product data structure and drawing release plan per company requirements • Independent design assessment reviews and engineering models not req'd but recommended as needed to verify design prior to start of flight unit

Requirement	Class A	Class B	Class C	Class D
Manufacturing				
Parts and Materials Assembly Flow Drawings Tooling Machinability	• Manufacturing plans include EEE parts list review, mandatory inspection points, assembly flows, first article approach, and quality assurance plan • Review and approval by prime contractor and customer	• Manufacturing plans include EEE parts list review, mandatory inspection points, assembly flows, first article approach, and quality assurance plan • Review and approval by prime contractor and customer • Minor deviations more common than with Class A	• Manufacturing plans include EEE parts list review, mandatory inspection points, assembly flows, first article approach, and quality assurance plan • Independent internal review per company requirements	• Independent internal review of manufacturing plans as applicable, and may deviate from company processes
Producibility				
	• Independent review of producibility process and application of standards • Financial assessments of potential suppliers undertaken to ensure supply chain "health" • Active parts obsolescence program • Use on "sole source" suppliers requires customer review or approval	• Independent internal review of producibility process and application of standards to company practices • Active parts obsolescence program • "Sole source" suppliers likely on heritage components, though monitored	• Independent review of hardware producibility, on as "as-needed" basis • Limited parts obsolescence program • Use of "sole source" suppliers on heritage components common	• No specific Producibility actions taken beyond standard company practice
Inspectability				
	• Program inspection plan includes multiple customer mandatory inspection points (MIPs), non-destructive evaluation methods, and acceptance criteria • Inspection plan reviewed and approved by customer	• Program inspection plan includes multiple customer mandatory inspection points (MIPs), non-destructive evaluation methods, and acceptance criteria • Inspection plan reviewed by customer	• Program inspection plan and acceptance criteria per "standard" company practices, including Quality MIPs and selected customer MIPs • Inspection plan internally reviewed by company	• Program inspection plan and acceptance criteria per company practice, with minimal company Quality mandatory inspections (few or no customer MIPs) • Inspection plan internally reviewed by company

Requirement	Class A	Class B	Class C	Class D
System Safety				
Safety Plan System Safety Requirements	• System safety plan includes hazard identification and control, safe-to-mate, GSE interface failure mode and effect analysis • Plan reviewed and approved by company, customer, and site organizations	• Same as Class A	• Same as Class A	• Same as Class A
Risk				
Risk Management Plan Risks Assessment Risk Analysis Risk Handling	• Risk management plan includes risk assessment, analysis and mitigation • Risk plan reviewed and approved by customer • Mandatory customer participation is risk processes	• Same as Class A	• Risk management plan includes risk assessment, analysis and mitigation • Risk plan reviewed and approved by company (customer invited) • Plan executed per company practices	• Risk management plan includes risk assessment, analysis and mitigation • Independent review of risk management plan as required • Risk processes would be informal, and driven by company requirements
Lessons Learned				
	• Independent review to evaluate incorporation of lessons learned • Ensure program lessons learned database is established	• Same as Class A	• Independent review to evaluate incorporation of lessons learned	• Same as Class C

Requirement	Class A	Class B	Class C	Class D
Cost/Schedule				
	• EVM system in place and utilized on program • IBR required to demonstrate compliance • Large Management Reserve, with customer likely in control • Formal IMS developed, provided to the customer for review, and monitored at standard program reviews	• EVM system in place and utilized on program • IBR recommended to demonstrate compliance • Large Management Reserve, with customer/contractor control • IMS developed per company processes, shared with customer, and monitored at standard program reviews	• EVM system in place and utilized on program in accordance with company processes • Some Management Reserve, with joint customer/contractor control • IMS developed to and monitored per company requirements	• EVM system in place and utilized on program in accordance with company processes • Limited Management Reserve under contractor control • IMS developed to and monitored per company requirements
Process Assessment				
	• Planned program reviews include SRR, PDR, CDR, MRR, TRR, PSR, and peer reviews • Customer and internal company off-program participation expected in most of the reviews	• Same as Class A	• Planned program reviews include SRR, PDR, CDR, MRR, TRR, PSR, and peer reviews • Customer participation unlikely (though invited) and limited internal company independent attendance at the reviews	• Only those reviews required by company processes are held • Limited (or no) customer participation

A2-4 Summary of the Classes

Class A. Class A programs execute the design assurance processes to the greatest extent possible. Many of the elements require contract deliverable items (e.g., risk plan, integration and test plan, and mission analysis) with review and approval by the customer. It is expected that the customer will actively participate or maintain close oversight. The review of the requirements will be formal and rigorous, with customer approval. Designs use high-reliability parts, redundant hardware, and rigorous maintenance of margins. Multiple analyses will be performed to characterize the mission, with the analyses typically subject to review and approval by the customer. Verification is by test to the greatest extent as is practical. Any Test-Like-You-Fly exceptions are documented and subject to customer review and approval. The V&V plans are formal documents requiring customer approval. Detailed manufacturing flow using many specially design tools will be reviewed by independent company and (possibly) customer subject matter experts prior to the start of hardware build. Inspection plans are developed and reviewed by off-program personnel, including the customer. The customer will also levy multiple mandatory inspection points (MIPs) for critical hardware or processes. Class A programs are expected to have a formal risk management plan, with routine meetings attended by the customer, and formal risk handling plans to deal with the various risks that occur during program execution. Programs are expected to have access to a healthy (20% or greater) management reserve, with a formal process for release of the funds.

Class B. The main difference from Class A to Class B lies primarily in the role of the customer. As with Class A missions, most of the design assurance elements require contract deliverable products. However, while Class A missions typically include customer approval of these documents, Class B missions only need customer review. Similarly, the customer will have less direct participation in the element execution and some of the oversight may be on a sample basis or delegated outright. Class B programs will have multiple requirements documents that are contract deliverables to the customer. The review of the requirements will be formal and rigorous, with customer approval of the final requirement set, though Class B programs may have more minor non-compliances than Class A programs. One would expect more Test-Like-You-Fly exceptions, though customer approval is still the norm. Class B programs would be expected to have inspection plans, though the level of rigor in their review would likely be less and have fewer MIPs. Class B programs would be expected to have access to a healthy (20% or greater) management reserve, with a formal process for release of the funds.

Class C. While all of the design assurance elements are executed, the programs typically perform the efforts to contractor's best practices (not to be defined by customer standards). There are fewer deliverable products, and many of these are provided for information only. There will be little (and in many cases no) direct customer participation in the execution of the element processes, and much of the oversight will be performed on a sample basis or fully delegated to the contractor. Missions will have fewer design reviews and less rigorous design reviews, typically with few customer and some off-program company personnel making up the design review panel. Class C programs perform fewer analyses (typically those required by company practice), and may not deliver the analyses to the customers. Class C programs use less formal V&V planning, although the V&V documentation is still likely reviewed and approved by the customer. The use of analyses to verify requirements will be common, and the Test-Like-You-Fly exception process is according to the contractor's best practices and likely without customer approval. A manufacturing flow process is typically developed, but reviewed only by the customer and contains less detail. Class C programs would be expected to execute inspections in accordance with company best practice, with only the most critical hardware reported to the customer as MIPs. The risk management process typically is performed to contractor best practices and would likely include a risk board that meets semi-regularly. The attendance at these boards would likely be limited to program management (customer may be invited), and any risk

handling plans would be informal. Class C programs typically have less management reserve, and it is not unusual for the funds to be under contractor control.

Class D. The tasks levied in design assurance are performed to (sometimes tailored) contractor best practices, and are minimally reviewed by the customer. Few formal deliverable products are required, with the majority of the independent review performed ad hoc by either program or contractor personnel. The program may choose commercial parts, have little or no redundancy, and will have lower design margins. The verification process is typically informal, though most likely in accordance with contractor guidelines. There would be a limited validation process, and a reduced emphasis on Test-Like-You-Fly exception identification and mitigation. The manufacturing flow is informal, and likely under the control of a few program personnel. The tooling used will be what is available, with any specialty tooling likely developed on program. Class D programs execute inspections to contractor best practice, with MIPs reported for program personnel to verify key hardware processes. The risk management process is typically performed to contractor best practices, and likely includes a risk board that meets semi-regularly. The attendance at these boards would likely be limited to program management, and any risk handling plans would be informal. Class D programs have the least management reserve.

A2-5 Effectiveness Tips

- Trade Studies should be widely vetted across the program and with company off-program subject matter experts to leverage a wide knowledge scope before making a final decision.
- It is never too soon to begin working with Range Safety for any spaceflight program, as the Range is a true (and active) gate keeper to proceeding to launch.
- When possible, adding an external test connector to complex electronic boxes will ultimately prove to be worth the effort when the inevitable box failures occur after delivery.
- Develop, maintain, and vet the program Test-Like-You-Fly exceptions list early in the program, as disagreements are best (and most inexpensively) handled earlier.
- Attempt to categorize lessons learned by the program phase and discipline to filter the lessons for maximum utility.

A2-6 Reference Documents

1. Aerospace Report TOR-2009(8591)-11, *Design Assurance Guide*, 4 June 2009.
2. NASA NPR 8705.4, *Risk Classification for NASA Payloads*, 9 July 2008.
3. Aerospace Report TOR-2010(8591)-18, *Mission Assurance Program Framework*, 2010.

Appendix A3: Parts, Materials and Process

Eli Minson, General Dynamics
David Pinkley, Ball

A3-1 Introduction

The primary objective of the parts, materials and process (PMP) "process" is to ensure that parts, materials, and processes used in the deliverable products and ground equipment will function and perform in accordance with the requirements of their intended application. The PMP function includes oversight of electrical and mechanical parts and components as well as specific materials and the processes used in the manufacturing of deliverable hardware. It also includes definition of expectations for attributes such as derating and performance as well as review of non-standard or non-compliant items. PMP activities include:

1. verification of all subcontractor's performance to assure that delivered products satisfy contractually flowed down requirements
2. regularly scheduled PMP meetings to resolve issues
3. verification of worst-case circuit analysis
4. validation of piece part failure rates
5. verification of degradation limits of critical parameters for worse case design.

This chapter provides guidelines for applying effective PMP to space systems. The elements of PMP may be tailored to meet the needs of the program; however, the PMP process is either required or recommended for any space system development activity to ensure clarification of users' needs. The process may be applied to all space flight systems to include deliverable payloads, space vehicles, or other associated products. Formal PMP may be dictated by the acquisition authority per the contract or developed in accordance with the contractor's best practices commensurate with the level of risk associated with the specific mission. Ultimately, the developer is responsible for implementing an organized, systematic PMP process to increase the likelihood of achieving mission success.

A3-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which risk profile can be developed and are not intended as general standalone industry standard definitions.

Parts Selection. Establishes the baseline criteria for standard and non-standard parts, part type specification, and quality level for use on a given program. NASA uses EEE-INST-002 Instructions for EEE Parts Selection, Screening, Qualification and Derating as their governing document. However NASA centers can have their own parts management plan. National Security Space (NSS) uses the following TORs:

- TOR-2006(8583)-5235, Parts, Materials and Processes Control Program for Space and Launch Vehicles
- TOR-2006(8583)-5236, Technical Requirements for Electronic Parts, Materials I Processes used in Space and Launch Vehicles (also published as SMC-S-010-2009) for the EEE parts space quality baseline for standard parts.

Screening Program. Establishes the baseline criteria for screening tests for flight parts to: remove nonconforming parts; to remove parts with random defects, or parts likely to experience infant

mortality, from an otherwise acceptable lot and thus increase confidence in the reliability of the parts selected for use.

Part Qualification. Establishes the qualification criteria for all parts used in flight designs. Standard parts selected per the parts selection criteria are considered qualified. Qualification testing consists of mechanical, electrical, and environmental testing and is intended to verify that the materials, design, performance, and long-term reliability are consistent with program objectives.

Precap Inspections. Examination of customer-purchased product performed at the supplier's facility to verify product integrity and conformance to specified requirements prior to delivery. Precap Inspection is commonly performed prior to sealing or encapsulating high-reliability microelectronic components.

Destructive Physical Analysis (DPA). DPA is a systematic, logical, detailed examination, wherein parts are evaluated for a wide variety of workmanship, design, and processing problems that may not be identified during the normal screening process.

Standard Part Drawings. Standard Part Drawings supplement existing part documentation that is inadequate for control or test of the procurement of parts to their selection, screening, and qualification requirements.

Part History Evaluation. Parts are evaluated to ensure that they are not reliability-suspect parts. Evaluations include a GIDEP search, radiation performance, and previous usage data, such as failure and DPA history. Suspect parts must be subject to compensating provisions to ensure that the suspect issue has been resolved. Compensating provisions may include DPA, additional screening, or selecting/denying a specific manufacturer or data code.

Program Materials Parts Control Board (PMPCB). The responsibility of the PMPCB is to ensure all parts used on the program meet the program's mission requirements, including life, reliability, performance, cost, and availability. Technical rationale will be captured for any use of non-standard parts. The PMPCB reviews and acts on any noncompliance with or deviation from the parts requirements.

Program Approved Parts List. The approved parts list covers parts selection, review, and analysis activities for all EEE parts planned for use of a given program. The list contains the necessary information to allow clear communications within the EEE parts disciplines and provide documented approvals by Parts Engineering, Radiation Effect Engineering, Materials Engineering and the customer.

Global Parts Substitution. List of parts substitutions that are "better-than-or-equal-to" parts. Parts that are form, fit, function, radiation tolerance, and reliability substitutes.

Parts Age and Storage Restrictions. Controls placed on part usage based on age and storage conditions. Used by PMPCB and program manufacturing controls. Parts age restrictions are typically on the order of five years at which point the PMPCB will determine the need for re-screen. Parts stored in conditions where moisture or ESD are not controlled will typically not be usable.

Part Obsolescence. Process to ensure that inactive or obsolete parts are not considered for design. The obsolescence process ensures the continued availability of parts as an integral part of the parts selection process and is considered by PMPCB before any part is approved for the program. Parts that

are scheduled to be discontinued are evaluated by the PMPCB and appropriate measures (life time buys or redesign) are taken.

Prohibited Items. The identification of items, which are prohibited for use. Typical prohibited items include pure tin plating (97% or greater) on external or internal surfaces of EEE parts and associated hardware such as cadmium, zinc, chemically coated cadmium or zinc, or silver usage as a connector or contact finish; silver usage as an under plate, variable resistors, etc.

Part Failure Analysis. Analysis of part failures verifying failure, cause, and suggested corrective action. Failure of parts prior to next assembly level is documented in nonconformance reports and supported by parts and radiation engineering. At higher assembly levels reliability engineering will coordinate failure analysis of EEE parts.

Radiation Analysis. Performing radiation evaluation of EEE parts against safety margins required based on their specific application. Heritage radiation analysis must be supported by a GIDEP review and delta analysis with PMPCB approval. The delta analysis must include comparison of spacecraft shielding, environment, duty cycle, bill of materials, and electrical schematics.

Radiation Testing. Given radiation analysis determination that existing data does not meet program requirements, characterization tests are performed on a representative lot of those components. If the test results do not show sufficient radiation design margin (RDM), radiation lot acceptance test (RLAT) is performed.

Supplier Oversight and Control. Regulation of the flow down of EEE parts requirements to suppliers via product specs, SOWs, or other contractual documentation. Includes evaluation of each supplier for their ability to comply with program requirements. Any noncompliance to parts flow down requirements are documented and dispositioned by a discrepancy report and submitted to PMPCB for approval.

COTS assemblies. The use of commercial off-the-shelf (COTS) assemblies, if allowed per the program parts plan. This typically involves sensors or other equipment of commercial origin. PMPCB will review COTS assembly function and reliability for mission criticality.

Material Selection. Establishes the baseline criteria for materials and processes that meet the required conditions specified for a given payload and integrated space vehicle. Heritage materials that have space-proven usage are preferred, otherwise materials and processes require representative qualification via test and/or analysis to the given environment. Qualification planning will identify conditions and testing necessary to meet the program and mission survivability and qualification requirements.

Contamination Control. The selection of hardware, materials, and processes used in production hardware that meet the requirements for volatile condensable materials. Allowed materials typically have maximum permissible losses of 1.0% TML (Total Mass Loss) and 0.1% CVCM (Collected Volatile Condensable Material based on ASTM E595.

Materials Control. Material Control includes usage lists, constraints, traceability and lot control, and shelf life control. Usage lists consist of both Materials and Processes List that lists all materials used on a program along with their quantities. Material Usage Agreements (MUAs) are required for all materials that don't meet selection criteria and must include applicable specifications, justification for usage, and pertinent qualification data as applicable. M&P constraints impose restrictions on materials such as material properties, lubricants, dissimilar metals, corrosion, fungus, fasteners,

finishes, cleaning, organic materials, etc. Traceability and Lot Control provides materials traceability to their manufacturer and lot/batch identifications to a given assembly level. Shelf life controls address aging, storage, and any associated limitations on life.

Materials Requirements. Material requirements include items such as Electrostatic Discharge (ESD) control, soldering requirements, harnessing, crimping, corrosion control, hazardous and toxic materials. The program will have general ESD control program commensurate with sensitivity of materials used. Soldering requirements will typically follow the NASA 8739 series or IPC-J-STD-001DS. Harness and crimping will be per internal standards and relevant specifications. Corrosion control will ensure only materials that are compatible with each other will be used in direct contact including prevention of galvanic corrosion and stress corrosion cracking. Hazardous and toxic materials usage will meet all federal and state occupational health, and safety, and environmental protection laws.

A3-3 Matrix - Parts, Materials, and Process

Requirement	Class A	Class B	Class C	Class D
EEE Parts and Radiation Effect Engineering				
Parts Selection	• EEE-INST-002 Level/Grade 1 equivalent SCD, or TOR-2006(8583)-5235 TOR-2006(8583)-5236, Per space quality baseline, Class SV, Grade 1	• EEE-INST-002 Level/Grade 2 equivalent SCD or space quality baseline, Class SV, Grade 1 for selection, screening and part qualification	• EEE-INST-002 Level/Grade 3 equivalent SCD. Class B/Q, Grade 2	• Parts management plan defined. Class C or best commercial practice
Screening Program	• Level/Grade 1 Requirements, Per space quality baseline, Class SV, Grade 1	• Level/Grade 2 Requirements, Class SV, Grade 1 for selection, screening and part qual	• Commensurate with Level/Grade 3 program, Class B/Q, Grade 2	• Part Characterization based on best commercial practice
Part Qualification	• Level/Grade 1 Requirements, Per space quality baseline, Class SV, Grade 1	• Level/Grade 2 Requirements, Class SV, Grade 1 for selection, screening and part qual	• Commensurate with Level/Grade 3 program Class B/Q, Grade 2	• Not required
Precap Inspections	• Required for all Parts (TOR-2006(8583)-5236) Note: Class V, K, S impose a rigorous internal visual.	• Required for hybrid microcircuits, custom microcircuits and based on History: DPA, flight, failure, discrepancies, procurement, GIDEP	• Not required	• Not required
Destructive Physical Analysis	• Required per MIL-STD-1580, Metal surfaces verified for absence of prohibited materials: (e.g., pure tin, zinc, or cadmium) Required for all parts	• Class M, Q, B microcircuits; JANTXV, Level M Caps, all EMI Filters, All Hi-Rel, and MIL-STD-883 Compliant. Required for all parts	• Class M, Q, B microcircuits; JANTXV, Level M Caps, all EMI Filters, All Hi-Rel, and MIL-STD-883 Compliant. Required for critical parts	• Recommend for evaluation of design, workmanship, fabrication problems
Standard Part Drawings	• Required on all non-standard parts and/or parts with inadequate control of parts with respect to required quality level	• Required on all non-standard parts and/or parts with inadequate control of parts with respect to required quality level	• Required on all non-standard parts and/or parts with inadequate control of parts with respect to required mission quality level. Vendor drawings are permitted with PMPCB approval	• Standard Part Drawings options dependent on screening and qualification baseline used in parts management plan

Requirement	Class A	Class B	Class C	Class D
Part History Evaluation	• Required, evaluation for reliability-suspect parts	• Required, evaluation for reliability-suspect parts	• Required, evaluation for reliability-suspect parts	• Recommended, evaluation for reliability-suspect parts
Program Parts Control Board (Assess life, reliability, performance, cost, and availability)	• Required, evaluation of life, reliability, performance, cost and availability. Nominally customer has voting membership	• Required, evaluation of life, reliability, performance, cost and availability. Customer may have voting membership.	• Required, evaluation of life, reliability, performance, cost and availability. Nominally no customer signoff	• Optional, as required in support of the parts management plan.
Program Approved Parts List (selection, review, and analysis activities)	• Required for selection, review, analysis, and communication between EEE parts, Radiation effects, Materials and customer	• Required for selection, review, analysis, and communication between EEE parts, Radiation effects, Materials and customer	• Required for selection, review, analysis, and communication between EEE parts, Radiation effects, Materials and customer	• Optional, as required in support of the parts management plan. Highly recommended for cost and schedule control of parts program
Global Parts Substitution (Better Than or Equal to Parts)	• Required, to ensure form, fit, function, radiation tolerance, and reliability or Engineering/MRB approval. Global Substitutes require PMPCB approval	• Required, to ensure form, fit, function, radiation tolerance, and reliability or Engineering/MRB approval. Global Substitutes may require PMPCB approval	• Required, to ensure form, fit, function, radiation tolerance, and reliability or Engineering/MRB approval	• Recommended, to ensure form, fit, function, radiation tolerance, and reliability
Part Age and Storage Restrictions	• Required: 5 year limit on environmentally uncontrolled parts	• Required: 5 year limit on environmentally uncontrolled parts	• With potential for PEMs (popcorning and corrosion) period must be evaluated and could be much less than 5 yrs	• With PEMs (popcorning and corrosion) period recommend evaluation and could be much less than 5 yrs
Part Obsolescence	• Obsolescence integral part of part selection	• Obsolescence integral part of part selection	• With potential introduction of commercial parts with short product life development time versus product life must be evaluated	• With introduction of commercial parts with short product life development time versus product life recommended
Prohibited Items	• Pure Tin, Cadmium, Zinc, Silver, variable resistor prohibited, 100% tin finishes, Mercury, dissimilar metals, corrosive sealants, etc; include validation – reference std for full list	• Same as Class A	• Pure Tin, Cadmium, Zinc, Silver, variable resistor prohibited, 100% tin finishes; less validation rigor – Screen risk parts	• Optional enforcement for these items: Cadmium, Zinc, Silver, variable resistor prohibited, 100% tin finishes.

Requirement	Class A	Class B	Class C	Class D
Part Failure Analysis	• Required for root cause evaluation of random vs. systemic issues for all failures	• Same as Class A	• Required for root cause evaluation of random vs. systemic issues for critical risk areas	• Optional per suppliers command media
Radiation Analysis	• RDM 2X Lot Specific TID and displacement data, and SEE No SEL <75MeV /mg / sqcm, No SEGR / SEB <37 MeV / mg / sqcm RDM 3 if shielding taken into account, slant ray analysis required, TOR requirements higher than this. EMI EMC TOR	• RDM 2X Lot Specific, 4X non-lot Specific TID and displacement data, and SEE No SEL<75MeV/mg/sqcm, No SEGR/SEB <37 MeV/mg/sqcm . • Review for rolloff Look at EI EMC TOR for relationship 461G	• RDM 2X TID and displacement Damage, SEE No SEL <75MeV/mg/sqcm, No SEGR / SEB <37 MeV/mg/sqcm .	• Optional - Reduced scope to specific critical designs
Radiation Testing	• Testing/verification required for parts without required margin	• Testing/verification required for parts without required margin	• Testing required evaluated on available data with focus on critical areas	• Optional - Reduced scope to specific critical designs
Supplier Oversight and Control	• Full level 1 requirements flow down for all parts	• Full level 2 requirements flow down for all parts	• Flow down product specification compliance based on heritage, less rigor in flow down	• Optional - Flow down product specification compliance tailored to mission requirements
COTS assemblies	• PMPCB review and approval for function, quality, reliability for mission criticality	• Same as Class A	• Assess for development process risk balance to manage risk uncertainty	• Recommend assess for development process risk balance to manage risk uncertainty
Materials				
Material and Process Selection	• Heritage when possible otherwise all require qualification to environment via test • TOR-2010(8591)-19 Objective Criteria for Heritage Hardware Reuse • TOR-2009(8546)-8604 Rev. A Reuse of Hardware and Software Products	• Heritage when possible otherwise all require qualification to environment test and analysis	• Heritage when possible otherwise all require qualification to environment by analysis at a minimum	• PMPCB acceptance of all materials recommended

Requirement	Class A	Class B	Class C	Class D
Contamination Control	• TML < 1%, CVCM <0.1% per ASTM E595 unless approved per analysis	• Same as Class A	• Same as Class A	• TML < 1%, CVCM <0.1% per ASTM E595 unless approved per analysis by compatibility with ride share
Materials and Process control	• REF TOR-2006(8583)-5235 or NASA doc for class 1 programs	• REF TOR-2006(8583)-5235 or NASA doc for class 2 programs	• REF TOR-2006(8583)-5235 or NASA doc for class 3 programs	• Optional per TOR, NASA doc for class 4 programs
Material and Process Requirements	• REF TOR-2006(8583)-5235 or NASA doc for class 1 programs	• REF TOR-2006(8583)-5235 or NASA doc for class 2 programs	• REF TOR-2006(8583)-5235 or NASA doc for class 3 programs	• Optional per TOR, NASA doc for class 4 programs

A3-4 Summary of Risk Classes

Class A. Required to apply PMP technical requirements per standard with minimum tailoring consideration. PMP plan as a deliverable should detail how requirements will be met and tailored and modified in accordance with requirements definition. Class A systems require high reliability, and Class S, Grade 1 parts. PMPCB with government approval integrated throughout the sub/supplier chain. Verification of heritage of previous-use materials required. All new or change materials and configurations must be qualified. Source controls required on all procured materials and acceptance test for each lot/batch.

Class B. Required to apply PMP technical requirements per standard with tailoring consideration of risk acceptance. PMP plan as a deliverable should detail how requirements will be met and tailored/modified in accordance with requirements definition. High reliability Class S, Grade 1 parts are required. PMPCB with government approval at prime-level; government may opt for review at sub/supplier chain. Quality and parts requirements should be flowed to the sub-contractors, but not always required. Program may use previously tested/flown materials or qualify new materials and configurations. Acceptance test each lot of procured material.

Class C. Adherence to a PMP plan is required that details how requirements will be met and tailored. Class B and/or commercial parts may be used; parts are rarely Class S because of the short acquisition time and expense.

Class D. A PMP is recommended per the contractor's best practices. Class C parts, commercial parts are usually used. Contract requirements based on safety and contamination standards so not to cause harm in the case of ride sharers or determined by LV provider.

A3-5 Effectiveness TIPS (Lessons Learned)

- Establish formal PM&P control document capturing both standards and process execution ground-rules and execute to it consistently.

A3-6 References

1. Aerospace Report TOR-2006(8583)-5235, *Parts, Materials and Processes Control Program for Space and Launch Vehicles* (also published as SMC-S-009-2009).
2. Aerospace Report TOR-2006(8583)-5236, *Technical Requirements for Electronic Parts, Materials I Processes used in Space and Launch Vehicles* (also published as SMC-S-010-2009).
3. EEE-INST-002 *Instructions for EEE Parts Selection, Screening, Qualification and Derating* (NASA/TP-2003-212242).
4. Aerospace Report TOR-2010(8591)-19, *Objective Criteria for Heritage Hardware Reuse*.
5. Aerospace Report TOR-2009(8546)-8604, Rev. A, *Reuse of Hardware and Software Products*.

Appendix A4: Environmental Compatibility

Ed Hume, Johns Hopkins APL
David Michel, Raytheon

A4-1 Introduction

Environmental Compatibility (EC) works to ensure that products are designed to withstand all environmental conditions encountered in service. For space systems, especially the integrated spacecraft, risks related to EC requirements are among the most critical to identify and either be eliminated or reduced to a minimum based on program constraints. For space systems this is accomplished by:

1. defining environmental requirements
2. considering these requirements in system design and implementation
3. supporting environmental testing and evaluation
4. supporting post launch environmental response evaluation.

The Environmental Compatibility process should begin as early in the design process as possible. In most cases it starts during the feasibility study phase of a pre-project, continues through launch, and occasionally continues during the mission. The EC process is implemented in a mission through several paths such as a specific application of systems engineering (i.e., as part of Mission Assurance or as specialized design engineering processes), to ensure all environmental requirements are defined and flowed to the appropriate levels, and that appropriate analysis and test methods are employed to verify the design will withstand the environments encountered in service with margin.

Applicable space system environments that should be considered in the EC process are shown in Figure A4-1. Figure A4-1 was adapted from the NASA Preferred Reliability Practices, Environmental Factors (PD-EC-1101). This figure also illustrates a significant complication for EC, some factors must be considered both as a single entity but also in combination with other environmental factors. As can be seen from Figure 1, the EC process must include factors related to the complete life cycle of the system under development including the build process, launch conditions, and operations. A well-written system specification addressing EC will establish requirements for normal (benign) conditions as well as extreme episodic events such as solar flares, and geomagnetic storms. Demonstration of Environmental Compatibility against the suite of requirements captured in the specification through a robust design, analysis, manufacturing, and test is essential for all class of space systems.

Failure to perform a detailed life cycle environment profile can lead to overlooking environmental factors whose effect is critical to equipment reliability. If these factors are not included in the environmental design criteria and test program, environment-induced failures may occur during space flight operations.

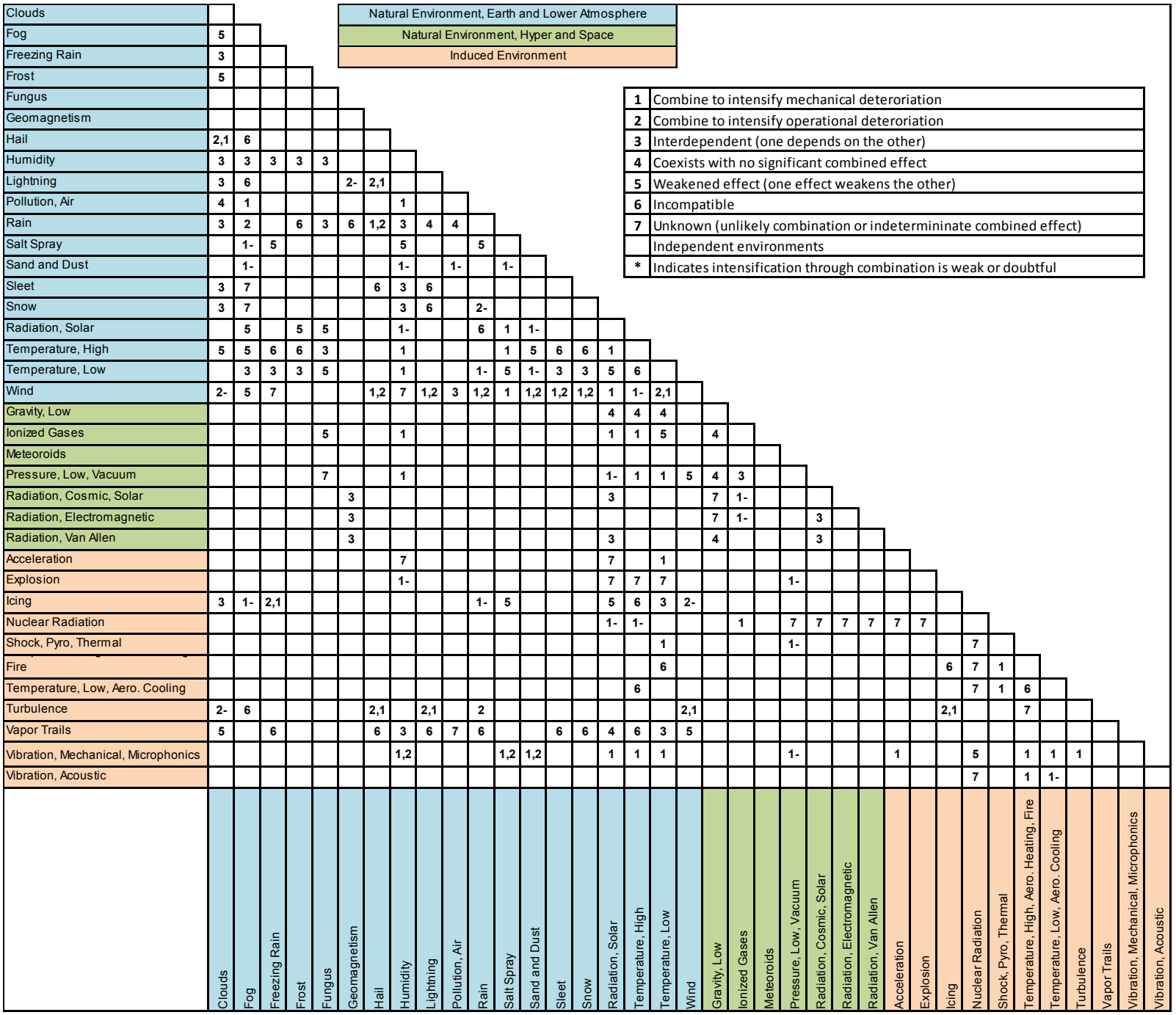


Figure A4-1. Effects of combined environments.

A4-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which a risk profile can be developed and are not intended as general standalone industry standard definitions.

Environmental Compatibility Analysis (ECA) is a part of the mission and system design process for a space system. ECA uses mission scenarios and factors (proposed orbit, mission life, launch, etc.) to establish requirements for system design and testing of a spacecraft.

System and Mission Requirements Definition is an established process for environmental compatibility that is used to establish the design and performance parameters of a space system. The process is used to ensure the system designed has been validated to perform as expected during its operational lifetime.

Testing Requirements are developed for environmental compatibility in response to the ECA and the system and mission requirements definition process. The space system program plan must address each established EC requirement to include the sufficient criteria to address the requirement and its associated risks.

Natural Space Environment refers to the environment as it occurs independent of the presence of a spacecraft. It includes both naturally occurring phenomena such as atomic oxygen and radiation and man-made factors such as orbiting debris. Specifically, the natural space environment includes nine environments: the neutral thermosphere, thermal environment, plasma, meteoroids and orbital debris, solar environment, ionizing radiation, geomagnetic field, gravitational field, and the mesosphere.

Hardness is an attribute defining the environmental stress level, which a space system can survive.

The **reliability** of a system is the probability that, when operating under stated environmental conditions, the system will perform its intended functions adequately for a specified time interval.

Survivability is the ability of a space system to perform its intended function after being exposed to a stressing environment created by an enemy or hostile agent.

Electromagnetic Environment specifies the Electromagnetic Compatibility (EMC) and Electromagnetic Interference (EMI) requirements of a space system or component. Electromagnetic compatibility is the branch of electrical sciences, which studies the unintentional generation, propagation, and reception of electromagnetic energy with reference to the unwanted effects (Electromagnetic interference, or EMI) that such energy may induce. The goal of EMC is the correct operation, in the same electromagnetic environment, of different equipment, which uses electromagnetic phenomena, and the avoidance of any interference effects.

System/Component Environment covers the launch and operational environments that a space system or components must survive. These typically include launch vibration/shock requirements, thermal operational/survival limits, radiation levels, design margins, etc.

Contamination is the presence of minor and unwanted constituents in materials, the development and operating environments.

Outgassing is the release of a gas that was dissolved, trapped, frozen or absorbed in some material. It can include sublimation and evaporation of a substance into a gas, as well as desorption, seepage from cracks or internal volumes and gaseous products of slow chemical reactions.

Radiation is a process in which energetic particles or energy or waves travel through a medium or space. The word **radiation** is commonly used in reference to ionizing radiation only (i.e., having sufficient energy to ionize an atom), but it may also refer to non-ionizing radiation such as radio-waves and light.

Thermal Environment encountered by a satellite system and is primarily driven by differential stresses from direct solar heating on one part of the spacecraft and excessive cooling on the surfaces in shadow. Thermal control must address the bulk heating and cooling as well as maintaining the operating temperature requirements of payloads and systems.

Dynamic Environment of a spacecraft, which encompasses the mechanical stresses placed on a system during all phases of the life cycle. The span of environments includes ground shipping and handling, quasi-static, vibrations and acoustic loads at launch, pyrotechnic shocks during stage separations, on orbit jitter and planetary landings.

Micro-meteoroids are small meteoroids, usually with a diameter below a few mm, which are not detectable with ground observations methods. Natural particles have high velocities, relative to Earth or spacecraft.

Orbital debris refers to man-made particulates released in orbit resulting from normal operations and malfunction conditions, and on-orbit collisions.

Pressure Environment of a space system generally refers to the operational environment but also includes venting of air pockets and chambers that must decompress during launch to prevent pressure differentials across walls sufficient to cause minor structural failures and loss of adhesion between spacecraft parts.

Operational Environment of spacecraft is the near-perfect vacuum of space. The Earth's atmospheric pressure drops to about 1 Pascal (10^{-3} Torr) at 100 km of altitude, the Kármán line which is a common definition of the boundary with outer space. Beyond this line, isotropic gas pressure rapidly becomes insignificant when compared to radiation pressure from the sun and the dynamic pressure of the solar wind, so the definition of pressure becomes difficult to interpret. Although it meets the definition of outer space, the atmospheric density within the first few hundred kilometers above the Kármán line is still sufficient to produce significant drag on satellites.

A4-3 Matrix - Risk Management and Assessment

Guidelines	Class A	Class B	Class C	Class D
Program Characteristics				
Environmental Compatibility Analysis	• Key part of mission system design process • Driven by mission/science objectives • Considers all mission factors such as proposed orbit, mission life, launch factors, etc. • Mission scenarios are well defined and used to develop Environmental Compatibility Analysis	• Same as Class A	• Component of mission system design process • Mostly driven by mission design/science objectives of primary payloads and systems • Accounts for primary mission orbit, mission life, stressing environmental design drivers, and launch factors based on mission flow down	• Same as Class C
System/Mission Requirements Definition	• Well documented process • Stakeholder input and agreement • Sponsor endorsed/ authorized • PM Acceptance • Individually addressed in program plans • No waivers allowed on KPPs as defined in Spec and/or SSOW	• Same as Class A except as follows • Allows limited waivers on non critical items	• Follows an approved process • Stakeholder input • Sponsor review of requirements • PM Acceptance • Critical requirements individually addressed in program plans • Non critical requirements may be aggregated • Waivers on non critical items	• Determined by prior experience and developers practices • Minimal stakeholder and sponsor review and oversight • Limited approval for requirements • Only critical mission impact requirements addressed in program plans • Waivers on non critical requirements
Testing Requirements	• Established for each requirement • Mandatory physical testing to satisfy requirements • Must meet or exceed all established safety margins	• Same as Class A except as follows • May allow Analysis and Models and Simulation (M&S) for non-critical requirements only	• Established for critical requirements • Mandatory physical testing to satisfy mission critical requirements • Analysis and M&S may be used for most requirements Must meet all established safety margins	• Established for major requirements or as designated by primary mission • Analysis, M&S, non stressing tests acceptable for most requirements • Must meet basic safety margins and those mandated by primary payload and mission

Guidelines	Class A	Class B	Class C	Class D
Environment Categories				
Operational Environment (Thermal, Radiation, Micro-meteoroid, Space debris, Natural Space Environments)	• Fully vetted for the planned orbit/ position • Tested to meet or exceed most stressing margins over expected lifetime of system • Use of physical testing required where practical	• Same as Class A	• Same as Class A	• Same as Class A except as follows: • Tested to meet requirements without margins • Minimal use of physical testing
Electromagnetic Environment (EMI/EMC/Magnetics)	• Payloads must be tested to ensure non- interference with other systems and payloads • Practices follow established standards and guidelines MIL-STD-461G, TOR-2005 (8583)-1 Rev A MIL-STD-1541A, TOR-2011(8591)-5	• Same as Class A	• Same as Class A	• Same as Class A
Mechanical Environment (Loads, Acceleration, Shock, Vibration and Acoustics)	• Fully vetted for the launch environment and planned orbit/ position • Tested to meet or exceed most stressing margins over expected lifetime of system • Use of physical testing required where practical 2X life testing of mechanisms required	• Same as Class A except as follows: • 2X life testing of mechanisms recommended	• Fully vetted for the launch and operational environment to ensure no detrimental impact to other systems and payloads • Tested to meet or exceed most stressing margins for launch and analyzed for operating environment over expected lifetime of system • Mechanism life testing not required	• Same as Class C except as follows: • Analyzed to meet or exceed most stressing margins for launch and for operating environment over expected lifetime of system • May be tested at space vehicle level for stand-alone payloads • Minimal use of physical test
Pressure Environment (Pressure, Vacuum, Venting, Contamination, Out-gassing)	• Fully vetted for ascent and planned orbit/ position • Proof testing required for all pressure/vacuum vessels	• Same as Class A	• Fully vetted for ascent and operational environments to ensure no detrimental impact to other systems and payloads • Proof testing required for all pressure vessels	• Same as Class C except as follows • Proof testing required for all pressure vessels to ensure range safety

A4-4 Summary of Risk Classes

The identification and handling of Environmental Compatibility requirements for space systems is critical to success. EC requirements also allow flexibility tailoring by a program based on schedule, fiscal, and technical constraints. Much of the residual risk and the established risk margins that determine the risk class for a particular space system are either driven by or are directly attributable to EC requirements.

The mission risk class are defined Section 3. Based on the issues such as risk acceptance, service life cycle profile, and launch constraints, environmental design requirements are established for units, subsystems, vehicles and systems. Design requirements for each mission class must include sufficient design margins to ensure that the space systems and components exceed the TR-2004(8583)-1/SMC-S-016 (MIL-STD-1540E) worst case service life environments. Aerospace Report TR-2004(8583)-1 specifies attention be given to the following EC items:

1. Probability of environmental occurrence
2. Effect of combined environments (e.g., temperature, vibration, acceleration)
3. Mitigation of failure modes and effects including propagation and criticality
4. The impact of the operations or failure of a payload on the remaining components of the space system or mission
5. Effect of equipment performance and criticality to mission success
6. Experience gained from identical equipment similarly used
7. Effects of planned acceptance and qualification testing

Class A missions and payloads are defined as high-priority, minimum-risk efforts. The Environmental Compatibility standards for Class A systems are the most stringent and can significantly drive the system risks and the risk mitigation strategy. All Class A systems perform an Environmental Compatibility Analysis that considers all mission factors such as proposed orbit, mission life, launch factors, etc. and uses well defined mission scenarios. The mission and system requirements definition is a well-defined process. The defined mission requirements are individually addressed in program plans. As part of the EC, all requirements must be satisfied through physical testing, and waivers are not allowed on key performance parameters. The required environmental design margins for Class A equipment are those specified in Aerospace Report TR-2004(8583)-1 and Aerospace Report TOR-2011(8591)-5.

Class B missions and payloads are defined as high-priority, medium-risk effort, with cost-saving compromises made primarily in areas other than design and construction. The Environmental Compatibility standards for Class B are similar to those for Class A and are only somewhat less stringent but can still significantly drive the system risks and the risk mitigation strategy. All Class B missions perform an Environmental Compatibility Analysis, which considers all mission factors such as proposed orbit, mission life, launch factors, etc. and uses well defined mission scenarios. The mission and system requirements definition is a well-defined process. The defined mission requirements are individually addressed in program plans. Analysis, Modeling and Simulation may be substituted for physical testing and limited waivers may be allowed on non-critical requirements. The required environmental design margins for Class B are specified in Aerospace Report TR-2004(8583)-1 and Aerospace Report TOR-2011(8591)-5.

Class C missions and payloads are defined as a medium or higher risk effort that is economical, reflyable, or is repeatable. Vehicle and experiment retrievability or in-orbit maintenance is at times possible such as typified by International Space Station or Orbiter attached payloads. Class C missions and payloads must be fully vetted for the launch and operational environment to ensure no

detrimental impact to other payloads. The environmental compatibility standards for Class C systems are similar to those for Class B, but less stringent. An environmental compatibility analysis is part of the mission system design but is driven mostly by the requirements of the primary payload. The mission requirements definition should follow an approved process with stakeholder inputs and sponsor review. The critical mission requirements are individually addressed in program plans while non-critical requirements may be aggregated in the plan. In a Class C mission, physical testing is usually used to satisfy mission critical requirements with analysis, modeling, and simulation for testing remaining requirements. Because of the greater allowable risk, and the potential recoverable nature of some Class C equipment, the environmental design values for Class C equipment are modified from those specified in TR-2004(8583)-1, Test Requirements for Launch, Upper-Stage, and Space Vehicles.

Class D missions and payloads are defined as a high risk, minimum-cost effort that is economical, reflyable, or is repeatable. The loss of a Class D system or payload must not negatively affect the success or mission of the primary payload, do no harm to other payloads on the space vehicle. Vehicle and experiment retrievability or in-orbit maintenance may or may not be possible. Class D must be fully vetted for the launch and operational environment to ensure there is no detrimental impact to other systems and payloads. The environmental compatibility standards for Class D are less stringent. An environmental compatibility analysis is a component of the mission system design but is driven by the requirements of the primary payload and mission. The mission requirements definition is determined usually by prior experience, and the developer practices with minimal stakeholder and sponsor review and with limited approval for requirements. Only critical mission impacting requirements are addressed in program plans. For a Class D, testing is only established for major requirements or as designated by primary mission. The use of analysis, modeling, and simulation or non-stressing tests is acceptable for most requirements. Because of the greater allowable risk, and the potential recoverable nature of some Class D equipment, the environmental design values for Class D equipment are similar to those for Class D as specified in TOR-2011(8591)-5, Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles.

A4-5 Effectiveness TIPS (Lessons Learned)

- One of the most effective means of ensuring environmental compatibility is through a well defined and executed review process
- The key tasks are to establish and implement, early in the development phase, the design and test recommendations and requirements that lead to robust, cost effective hardware designs that can be adequately environmentally tested and are delivered on time
- Concurrent or combined environments may be more detrimental to reliability than the effects of a single environment. In characterizing the design process, design/test criteria must consider both single and/or combined environments in anticipation of providing the hardware capability to withstand the hazards identified in the system profile.
- Each environmental factor requires a determination of impact on the operational and reliability characteristics of the materials and parts comprising the equipment being designed. Packaging techniques should be identified that afford the necessary protection against degrading factors.
- To ensure a reliability-oriented design, the needed environmental resistance of the equipment should be determined. The initial requirement is to define the operating environment for the equipment. A life-cycle environment profile that contains this information should be developed.

A4-6 References

1. SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A (MIL-STD-1540E), *Test Requirements for Launch, Upper Stage and Space Vehicles*, 6 September 2006.

2. MIL-STD-461G, *Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment*, 10 December 2007.
3. Aerospace Report TOR-2005 (8583)-1 Rev A (MIL-STD-1541A), *EMC Requirements for Space Systems*, 1 January 2008.
4. MIL-STD-1542B, *EMC and Grounding Requirements for Space Systems Facilities*, 15 November 1991.
5. DOD-W-8357A, Notice 1, *General Specifications for Space Vehicle Wiring Harness Design and Testing*, 4 September 2002.
6. ASTM E1548-09, *Standard Practice for Preparation of Aerospace Contamination Control Plans, Tailoring and Background*, 2009.
7. Aerospace Report TOR-2004 (8583)-3291, *Criteria for Explosive Systems and Devices Used of Space Vehicles*, 9 August 2004.
8. Aerospace Report TOR-2003 (8583)-2894, *Space Systems Structures Design and Test Requirements*, 2 August 2004.
9. Aerospace Report ATR-2009(9369)-1, *Critical Clearances in Space Vehicles*, 31 October 2008.
10. *Space Vehicle Mechanisms-Elements of Successful Design*, Conely. P.L. (editor), Wiley and Sons, 1998.
11. *Space Mission Analysis and Design*, Wertz, J.R., and Larson, W.J. (editors), Kulwer Academic Publishers, 1991.
12. *Fundamental of Space Systems*, Pisacane, V.L. and Moore, R.C., (editors), Oxford University Press, 1994.
13. PD-EC-1101, *NASA Preferred Reliability Practices Environmental Factors*, NASA Lewis Research Center.
14. NASA NPR 8705.4, *Risk Classification for NASA Payloads*, 14 June 2004 (revalidated 9 July 2008).
15. DoD-HBDK-343, *Design, Construction, and Testing Requirements for One of a Kind Space Equipment*, 1 February 1986.
16. MIL-STD-1540D, *Product Verification Requirements for Launch, Upper Stage, and Space Vehicles*, 15 Jan 1999.
17. NSS 1740.14, *Guidelines and Assessment Procedures for Limiting Orbital Debris*, Aug 1995.
18. John J. Scialdone, "Spacecraft compartment venting", Proc. SPIE 3427, 23 (1998); doi:10.1117/12.328500.
19. NASA Reference Publication 1390, *Spacecraft System Failures and Anomalies Attributed to the Natural Space Environment*, K.L. Bedingfield, R.D. Leach, and M.B. Alexander, Editor, Aug 1996.
20. Aerospace Report TOR-2011(8591)-5, *Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles*, September 13, 2010.

Appendix A5: Reliability

David Pinkley, Ball Aerospace
Gail Johnson-Roth, The Aerospace Corporation

A5-1 Introduction

The primary objective of the reliability engineering process is to ensure that design risks are balanced with program requirements and constraints through comprehensive reliability analysis and closed-loop problem failure reporting and closure. Reliability engineering is the process that provides independent insight, planning, and validation for reliability, end-of-life capability, and environmental capability of deliverable hardware design through concurrent analyses, reviews, and test assessments. Activities include performing a structured set of reliability analyses as an integral part of the design process for the purpose of assessing product reliability and to highlight any potential problems for timely resolution. These analyses include, but are not limited to:

1. reliability prediction and allocation
2. failure mode and effects
3. probabilistic risk assessment
4. part-level electrical, mechanical, and thermal stress analysis
5. worst-case analyses
6. fault-tree analysis
7. limited life analysis
8. critical item assessment analysis; and trend analysis.

A closed-loop failure and corrective action system is also a key element of the reliability program. These topics are addressed in more detail in Appendices A5-3, A5-4, and C2. The effectiveness of these measures is determined and supported by design analyses, design reviews, hardware tests, and failure data evaluation.

This chapter provides guidelines for applying effective reliability engineering to space systems. The methods of reliability engineering may be tailored to meet the needs of the program; however, a reliability engineering process is either required or recommended for any space system development activity to ensure clarification of users' needs. The process may be applied to all space flight systems to include deliverable payloads, space vehicles, or other associated products. Formal reliability engineering may be dictated by the acquisition authority per the contract or developed in accordance with the contractor's best practices commensurate with the level of risk associated with the specific mission. Ultimately, the developer is responsible for implementing an organized, systematic, reliability engineering process to increase the likelihood of achieving mission success.

A5-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which risk profile can be developed and are not intended as general standalone industry standard definitions.

Reliability Monitoring and Control. Reliability monitoring and control captures policy, procedures, monitoring, and control processes addressing limited life analysis, critical items management, supplier control, reliability of Government Furnished Equipment (GFE), and usage of previously flown component analysis.

System Reliability and Trade Studies. System reliability and trade studies capture system level models, reliability growth trending processes addressing reliability modeling and predictions, single point failure policy and redundancy, software reliability, Probabilistic Risk Assessment (PRA), mission/system level fault tree analysis, trending of test data, and maintainability and availability models.

Design Analysis and Review. Design analysis and review captures baseline design analysis performed including independent analysis, Failure Mode Effects and Criticality Analysis (FMECA), ground support equipment IFMEA, mechanical fault tree analysis/FMEAs, radiation analysis, parts stress analysis, worst case analysis.

Reliability Testing. Reliability testing captures subassembly/part level qualification required and assembly level ESS on volume production. Testing includes radiation testing, reliability life testing, and Environmental Stress Screening.

Anomaly Reporting; Failure Review, and Corrective Action. Anomaly reporting, failure review, and corrective action capture formal systems used to support Failure Review Board for root cause isolation and systemic anomalies. Section includes failure reporting, failure analyses on failed devices, and anomaly risk rating.

A5-3 Matrix - Reliability

Requirement	Class A	Class B	Class C	Class D
Reliability Monitoring and Control	• Comprehensive Policy, Procedures, Monitoring, and Control processes supporting minimum practical risk • Formal reliability program plan required by contract as an approved deliverable	• Policy, Procedures, Monitoring, and Control processes supporting low risk profile. • Formal reliability program plan required by contract as an approved deliverable	• Streamlined Policy, Procedures, Monitoring, and Control processes assessing compliance in support of moderate risk. • Formal reliability program plan required by contract	• Policy, Procedures, Monitoring, and Control processes required to ensure hardware and personnel safety. • Reliability program plan recommended (may be required)
Limited-Life (LL) Items Analysis	• Required. Tracking not required for > 3X margin	• Required. Tracking not required for >2X margin	• Required. Combined with CIL list; Tracking not required for >1X margin	• Not required
Critical Control Plan and Critical Item List (CIL)	• CIL tracked to closure on workoff sheets, Eliminate single point failures (SPFs)	• CIL tracked to closure on workoff sheets, SPFs minimized and mitigated	• Tracked within CIL list	• CIL of space vehicle interfaces only
Control of Suppliers	• On-going with continuous monitoring • Active and Accepted risks integrated with program	• Extensive monitoring • Active and Accepted risks integrated with program	• Monitoring for Product Specification Compliance	• Minimal monitoring for Product Specification Compliance
Reliability of Government Furnished Equipment	• Assess for reliability baseline support	• Assess for reliability baseline support	• As required	• As required
Previously Flown Component (Heritage)	• Assess fully enveloped application requirements	• Assess fully enveloped application requirements. Some deviations allowed	• Assess compliance to heritage specifications. deviations allowed	• Assess function and performance. Deviations allowed
System Reliability and Trade studies	• System level models, growth trending, supporting lifecycle minimum practical risk	• System level models, growth trending, supporting lifecycle low risk profile. Some reductions in Probabilistic Risk Assessment (PRA) for NASA programs and FMECA analysis for NSS	• Minimum level of system reliability modeling required for meeting system requirements for reliability and maintainability. PRA and Mission Fault Tree Analyses (FTAs) required for NASA programs; FMECA required for NSS	• System level models, growth trending, supporting lifecycle high-risk profile. PRA, System FTA, FMECA not required

Requirement	Class A	Class B	Class C	Class D
Reliability Modeling and Prediction	• System Model, Parts Count and Parts Stress with high fidelity	• System Model, Parts Count and Parts Stress with high fidelity	• System Model, Parts Count. Only Fidelity as appropriate	• Parts Count Only, if required
Single Point Failure (SPF) Policy and Redundancy	• SPFs not allowed. Redundancy required for all essential SV functions and key instruments Hi-reliability cross-strapping methods followed	• SPFs accepted by exception. • Redundancy required for all essential SV functions and key instruments • Hi-reliability mitigations and with tracking to closure for low risk profile	• SPFs allowed. • Single string design allowed with selective redundancy for higher risk assemblies	• SPFs allowed. • Single string design or selective redundant design approaches used
Software Reliability	• Software reliability growth program required	• Software reliability growth program required	• Required for new development critical software	• Not required
Probabilistic Risk Assessment (PRA) – NASA Requirement	• Limited scope mission end states	• Limited scope on mission-related end states of interest	• Not required	• Not required
Mission/System Fault Tree Analysis (FTA)	• Mission/System Level qualification FTA required	• Mission/System level qualification FTA required for critical aspects of the mission	• Recommend, but not required. Only to ensure no effect on bus or other payloads	• Not required. Only to ensure no effect on bus or other payloads
Trending of Test Data	• Critical components trended including BIST, TVAC and FIST performance	• Key performance parameters trended as required	• Not required	• Not required
Maintainability and Availability	• Required for development maintenance and mission ground system MTTR and Ao, including spares philosophy	• Required for development maintenance and mission ground system MTTR and Ao	• Recommended for MTTR and Ao management	• Not required

Requirement	Class A	Class B	Class C	Class D
Design Analysis and Review	• Design analysis to support minimum practical risk Program	• Baseline design analysis supporting low risk program. Some reductions in worst case analysis (WCA)	• Selected reliability analysis performed in support of Moderate risk program. Limited WCA and FMECAs/FTAs	• Analysis recommended for management of safety and risk uncertainty against higher risk profile. WCA and parts stress analysis (PSA) not required
Independent Design Analysis Review	• Independent review required	• Independent review required	• Selected analysis independently reviewed based on risk assessment	• Audits may be performed
Failure mode effects and criticality analysis (FMECA) – NSS requirement	• NSS-FMECA required to parts level • NASA - Interface FMEA minimum with analysis supporting no fault propagation, hardware part Level at safety critical, redundancy switching circuits, detection and recovery circuits, and electronic pyrotechnic circuits, full redundancy	• NSS- FMECA required to parts level • NASA- Interface FMEA in component interface parts, at redundancy boundary, redundancy on essential functions	• Functional FMECA required at the component level Interfaces, Single string fault propagation	• Functional FMECA required at Spacecraft/Payload Interface, Single string fault propagation
Ground support equipment (GSE) IFMEA	• IFMEA to demonstrate GSE, STE, EM hardware cannot propagate to flight equipment or adversely affect the mission	• IFMEA to demonstrate GSE, STE, EM hardware cannot propagate to flight equipment or adversely affect the mission	• IFMEA to demonstrate GSE, STE, EM hardware cannot propagate to flight equipment or adversely affect the mission	• IFMEA to demonstrate GSE, STE, EM hardware cannot propagate to flight equipment or adversely affect the mission. Can be informal
Mechanical Fault Tree Analysis/ FMECAs	• Mechanism FTAs/FMECAs required	• Mechanism FTAs/FMECAs required	• Mechanisms FTA/FMECAs for mission critical hardware	• Mechanisms FTA/FMECAs for safety critical hardware

Requirement	Class A	Class B	Class C	Class D
Radiation Analysis	• RDM 2X Lot Specific TID and displacement data, and SEE No SEL and SEU <75MeV /mg/sqcm, No SEGR / SEB <37 MeV / mg / sqcm	• RDM 2X Lot Specific, 4X non-lot Specific TID and displacement data, and SEE No SEL and SEU <75MeV/mg/sqcm, No SEGR / SEB <37 MeV / mg / sqcm	• RDM 2X TID and displacement Damage, SEE No SEL <75MeV /mg / sqcm, No SEU and SEGR / SEB <37 MeV / mg / sqcm	• Reduced scope to specific critical designs. (e.g., Quick look review of parts list for obvious problem parts)
Parts Stress Analysis (PSA)	• Required using approved derating criteria	• Required using approved derating criteria	• Required using approved derating criteria	• Recommended, but not required (minimal review for exceeding manufacturer's specs)
Worst Case Analysis (WCA) (Includes circuits that are interfaces to supplier assemblies)	• WCA EVA required on all circuits	• WCA EVA on circuits susceptible to EOL degradation. RSS may be used as alternative method	• Limited to high risk designs, timing analysis recommended	• Not required
Reliability Testing	• Subassembly/Part level qualification required and assembly level ESS on volume units	• Subassembly/Part level qualification required and assembly level ESS on volume units	• Selected part level qualification based on critical mission reliability. Reduced ESS on volume units. Use of data more acceptable as well as reduced margins	• Qualification limited to safety critical items only
Radiation Testing	• Testing required for parts without required margin	• Testing required for parts without required margin	• Testing required evaluated on available data	• Reduced scope to specific critical designs
Reliability Life Testing	• Assuring qualification margins to life requirements	• Assuring protoflight margins to life requirements	• Assuring acceptance margins to life requirements	• Recommended for management of unknown qualification margins on new hardware
Environmental Stress Screening (ESS)	• Required for NSS programs. Recommend for volume units, per customer and developer accepted processes	• Required for NSS programs. Recommended for volume units, per customer and developer accepted processes	• Recommended for volume units, per customer and developer accepted processes. Reduced screening may be used	• Not required

Requirement	Class A	Class B	Class C	Class D
Anomaly Reporting, Failure Analysis, and Corrective Action	• Formal System used to support Failure Review Board for root cause isolation and systemic anomalies assuring minimum practical risk throughout development and operations	• Formal System used to support Failure Review Board for root cause isolation and systemic anomalies assuring low-risk throughout development and operations	• Formal System used to support Failure Review Board for root cause isolation and systemic anomalies for moderate risk in later part of development as a minimum	• Less formal system used to support Failure Review Board for root cause isolation and systemic anomalies for high risk
Failure Reporting	• Failure Reports at first power application, captured in formal closed loop system for all levels	• Failure Reports negotiated at first power application level, captured in formal closed loop system for all levels	• Failure reporting at acceptance testing captured in formal closed loop system for all levels. Customer participation may vary depending contract	• Failure reports captured in nonconformance system – may be informal.
Failure analyses on failed devices	• Required for all failures to the point that lot dependency of the failure mode can be determined	• Required for all failures to the point that lot dependency of the failure mode can be determined	• Required for life test and post integration failures to the point that lot dependency of the failure mode can be determined	• Recommended, but not required
Anomaly Risk Rating	• Required	• Required	• Required	• Required/Recommended –developer accepts risk

A5-4 Summary of Risk Classes

Class A. System requirements dictate the implementation of a formal reliability program plan (sometimes combined with availability and maintainability). The plan is a formal contract deliverable with government review and approval. Reliability requirements are allocated from the system level down to the parts level. Requirements flow to the subcontractors and suppliers and are monitored by the contractor and government to ensure full compliance. Specific reliability requirements include all of those listed in the matrix (e.g., FMECA, FRB, trend analysis, critical items lists, worst case performance, and parts electrical stress analysis for all parts and circuits.) Reliability engineering requirements defined for first of fleet Class A systems are designed to achieve 100 percent mission success for the mission life. Any tailoring of the requirements entails a risk (which may be compounded by actions or lack of actions during the overall system acquisition process) that has to be weighed against mission criticality, performance, and life expectancy.

Class A. Reliability requirements dictate that no single-point failures are allowed; exceptions require justification based on risk analysis and mitigation measures. Redundancy is required for all space vehicle functions and key instruments. The contractor's reliability organization will be a major factor in the effectiveness of the implementation of the reliability requirements and is responsible for the definition of major reliability tasks as an integral part of the design, development, and verification process.

Class B. System requirements may be tailored to meet the unique needs of the Class B system. Exceptions may be where structures have heritage flight history and the level of analyses may be tailored as appropriate. Deliverables with customer approval should include a reliability plan that includes the following analyses: IFMECA for flight and interfacing GSE, mission and mechanism FTA, critical items list at black box level as a minimum, worst-case performance, and parts electrical stress analyses for all parts and circuits. Class B reliability requirements dictate single-point failures acceptance by exception with appropriate justification. Redundancy is required for all essential space vehicle functions and key instruments. The contractor's reliability organization and processes are heavily leveraged to define the major reliability tasks as an integral part of the design, development, and verification process.

Class C. System requirements should incorporate tailored requirements commensurate with the risk posture of the program. The contract may require a reliability plan to be developed and heavily depends on the contractor's internal reliability engineering function, processes, and analyses. The plan is usually available for customer review and is sometimes a contract deliverable. The scope of the FMECA and the detail of the critical items list are determined by the program. Parts electrical stress analysis is sometimes performed for all parts and circuits, but not always required. Analysis is required at interfaces to meet safety standard requirements. Single-point failures are permitted; single string or selectively redundant design approaches may be used.

Class D. Class D may not have formal or specific contractual requirements other than those imparted by applicable safety standards or interface requirements. Reliability assessment is left to the discretion of the experimenter/developer. Single-point failures are permitted based on the experiment requirements; single string or selective redundant design approaches are often used due to the small size and limited life and budgets of the program.

A5-5 Effectiveness TIPS (Lessons Learned)

- Ensure trade studies consider relative reliability
- Ensure critical failure modes are identified and adequately mitigated

- Ensure parts are reviewed for reliability with adequate derating
- Ensure testing failures are driven to root cause with good correction action

A5-6 References

1. Aerospace Report TOR 2007(8546)-6018, *Mission Assurance Guide*.
2. Aerospace Report TOR-2010(8591)-18, *Mission Assurance Framework*.
3. Aerospace Report TOR-2011(8591)-5, *Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles*.
4. Aerospace Report TOR-2007(8583)-6889, *Reliability Program Requirements for Space Systems*.
5. Aerospace Report TOR-2006(8506)-4494, *Space Vehicle Systems Engineering Handbook*.
6. Aerospace Report TOR-2009(8591)-13, *Space Vehicle Failure Modes, Effects, and Criticality Analysis (FEMCA) Guide*.
7. Aerospace Report TOR-2006(8583)-5236 (Also published as SMC-S-10), *Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles*.

Appendix A6: System Safety

David Pinkley, Ball
Gail Johnson-Roth, The Aerospace Corporation

A6-1 Introduction

The primary objective of the system safety process is to ensure potential hazards to personnel, equipment, systems, the environment, and facilities are identified, tracked, evaluated, eliminated and associated residual risks controlled or reduced to acceptable levels or better. A hazard is a condition that is prerequisite to a mishap (accident) or presents the potential for harm; therefore, the objective of a particular system safety process is somewhat dependent on how the customer defines an accident, and on the type of system. The system safety process ensures the development of safe systems and in doing so, it supports timely design for safety, coordinates and deploys system safety policies, standards, procedures, plans, instructions, guidance and practices, and assists/assesses programs in an efficient and effective application. Significant activities include the following:

1. provide safety requirements, safety design, safety testing, safety operations, and disposal checklists for programs and users
2. tailor system safety requirements consistent with mission requirements
3. perform hazard analyses and risk assessments, such as, preliminary hazard analysis, safety requirements/criteria analysis, subsystem hazard analysis, system hazard analysis, and operating and support hazard analysis
4. input of safety considerations into design and procedures
5. ensuring that residual mishap risks are accepted by the appropriate authority and that the acceptance is documented, monitor safety-critical designs and procedures (e.g., hazard control verification and tracking)
6. investigate and formally report mishaps and safety-related failures; and provide input to the safety data packages such as: the Mishap Risk Assessment Report (MRAR), the Missile System Pre-launch Safety Package (MSPSP) and/or the Safety Assessment Report (SAR)

System safety is a major part of the environment, safety, and occupational health (ESOH) assurance effort, which addresses issues relating to compliance with the Occupational Safety and Health Administration (OSHA), the Environmental Protection Agency (EPA), and other federal, state, and local regulations.

This appendix provides guidelines for applying system safety to space systems. The methods of system safety generally are applicable to all space missions. A system safety program is required for all NASA and NSS space system development programs. The MIL-STD-882 consistent system safety process is applied to all space systems to include deliverable payloads, space vehicles, and associated systems and equipment including ground systems. Formal system safety requirements may be dictated by the acquisition authority per the contract or developed in accordance with the contractor's best practices commensurate with the level of risk associated with the specific mission. Ultimately, the developer and program manager (PM) are responsible for implementing an organized, systematic system safety process to meet system safety requirements while optimizing the likelihood of achieving mission success.

A basic heuristic/tenet in system safety is the application of the system safety order of precedence for hazard control/mitigation: design for minimum risk, incorporate safety device, provide warning device, and develop procedures and training.

System Safety is applicable to the entire life cycle and to all system levels.

A6-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which risk profile can be developed and are not intended as general standalone industry standard definitions.

Requirements Identification, Allocation and Verification. Program, integration, and operational (e.g., user, operator, facility or launch site) requirements are reviewed for applicability and allocated to systems engineering and responsible design, test, and operations personnel. Safety compliance checklists are used to track implementation and verification of applicable requirements.

Safety Analysis. There are various tools available to assist in implementating a system safety program to identify hazards. The tools identify hazards in particular settings or at particular times in the system life cycle dependent on the type of analysis being 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 of the subsystems.

- **Software Safety Analysis (SSA)** determines flight and ground software contributions to system hazards, including hazards arising from software's interaction with other aspects of the system. Actions are identified to eliminate or control hazards from software to an acceptable level.

- **Operating and Support Hazard Analysis** (O&SHA) is conducted to identify hazards that may arise during operations at integration facilities internal or external to the contractor and designated launch site process facilities, to find causes of these hazards, recommend risk reduction alternatives, and ensure an acceptable risk to and from the system. The O&SHA evaluates activities for hazards or risks introduced into the system by facilities, operations, and test procedures, and evaluates the adequacy of procedures used to eliminate or control identified hazards or risks.

- **Other/Combined Hazard Analyses; On-Orbit Hazard Analysis.** Other analyses may be performed that incorporate one or more of the analytical tools described above. Of particular importance is the On-Orbit phase hazard analysis that must be performed to address safety of a system that includes an orbiting asset. An on-orbit hazard analysis includes orbital safety considerations, such as collision avoidance, directed energy, orbital debris minimization, end-of-life safing, and the space environment. An on-orbit hazard analysis also includes other safety risks that may exist for a particular system for the on-orbit phase, such as risks to human populations, risks of system loss, risks of loss of mission capability, and end-of-life considerations. An on-orbit hazard analysis supports development of required documents such as the PESHE, Space Debris Assessment Report or End-Of-Life Plan.

Safety Risk Assessment. Safety hazards are categorized based on probability of occurrence and severity resulting in an assigned risk index or level. Various deductive tools are used to systematically assess the potential of hazard risks and the assignment of a risk index to 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.

- **Event tree analysis** is a bottom-up method that determines system responses to an initiating "challenge." It can assess the probability of either an unfavorable or a favorable outcome. The initiating system challenge may be a failure or fault, an undesirable event, or normal operative commands. The method is especially useful for command-start/command-stop protective devices, emergency response systems, and engineering safety features. It is also useful for analyzing operating procedures, management decision options, and other non-hardware systems. Multiple coexisting system faults/failures can be analyzed. The method identifies and analyzes potential single-point failures, and it identifies areas of system vulnerability and low-payoff countermeasures.

- **Cause-consequence analysis** is a bottom-up symbolic logic technique that explores system responses to an initiating "challenge." It enables assessing the probabilities of unfavorable outcomes at each of a number of stepwise, mutually exclusive loss levels. The system challenge may be a failure or fault, an undesirable event, or a normal system operating command.

Safety Risk Documentation. The acquisition authority may require formal safety documentation and other documentation required by federal, state, and local regulations. The documentation also supports a contractor's need to show that it has performed due diligence in developing, operating, testing, or maintaining safe systems, or to maintain a record of safety features. The documentation is also useful to support potential legal/liability activities, such as accident investigation, indemnification reviews, or the government contractor legal defense.

- **System Safety Management Plan** (SSMP) provides guidance on how the Program Office (PO) will implement system safety requirements. The SSMP is the parent document where requirements to be flowed-down to the contractor's System Safety Program Plan (SSPP) will be derived.

- **System Safety Program Plan** establishes a system safety organization to execute required system safety tasks, establishes lines of communication with other elements of the system,

establishes authority for resolution of identified hazards, establishes incident alerting and notification and mishap reporting, and defines the system safety milestone for inputs/outputs. A main purpose of this plan is to provide a basis of understanding between the contractor and the managing activity to ensure that adequate consideration is given to safety during all life cycle phases of the program and to establish a formal, disciplined program to achieve the system safety objectives.

- **Missile System Prelaunch Safety Package (MSPSP) and Mishap Risk Assessment report (MRAR)** captures complete hazards analysis, hazard mitigation activities, hazardous procedures, and packaging handling and transportation planning associated with the completed system hardware. Early participation and involvement in the life cycle of a system will ensure that system safety is properly addressed during system reviews and meetings with Range safety and other regulating organizations and MRAR/MSPSP preparation. For programs involved with Range Safety approval process, a MSPSP may be the preferred data to be submitted to the Range(s) over the MRAR. The MRAR could then be formatted to have two parts: Part 1 will be the MSPSP, and Part 2 will be the rest of the required contents for the MRAR. Other MRAR contents might typically include analyses from parts of the life cycle outside the purview of the Range, such as pre-launch analyses or on-orbit hazard analyses. The MSPSP will then be submitted to the Range(s), but, both Part 1 and Part 2 will still be required to be submitted to the program office.

- **Programmatic Environment, Safety, and Occupational Health Evaluation (PESHE)** document may or may not be produced by the contractor but is required for all DOD programs regardless of acquisition category to ensure that a good system safety process is in place and accessible by the system program office. Creation of an environmental, safety, and occupational health database is recommended to identify hazards, archive risk assessments and mitigation decisions, document residual risk acceptance and ongoing assessment of the effectiveness of mitigation efforts.

- **Federal documentation** requires compliance to National Environmental Policy Act (NEPA) and Occupational Health and Safety Administration (OSHA) regulations.

- **Space Debris Assessment Report (SDAR)** addresses and documents the potential for debris generation during normal operations or malfunction conditions, the potential for generating debris by collision with space debris (naturally- or human-generated) or other space systems and post-mission retirement/disposal.

- **End-Of- Life Plan (EOLP)** programs shall develop appropriate disposal plans for orbital space systems to either reenter the atmosphere safely or else be moved into a disposal orbit at the end of its useful life where it will be less likely to interfere with operational spacecraft. Programs will provide an EOLP for the disposal of the space system at the end of its useful life.

- **Safety Assessment Report** documents a comprehensive evaluation of the mishap risks being assumed prior to test or operation of a system, prior to the next contract phase or at contract completion (Reference ANSI/GEIA-STD-0010-2009, Standard Best Practices for System Safety Program Development and Execution, Table A-1 page 23 and Task 301 Page 97). The SAR can be used to document safety tasks and activities such as such as non-launch related analyses or on-orbit hazard analyses, if not obtained in other reports.

- **On-Orbit Hazard Analysis (OOHA) Report** On-Orbit hazard analysis must be performed to characterize prevention or possibility of accidental explosions, intentional breakups, and probable collisions with active satellites and large and small objects.

Hazardous and Safety-Critical Activities are followed through participation in hazardous procedure reviews and approval and test readiness reviews and through test monitoring of hazardous and safety critical activities.

Mishap Reporting and Investigation includes system safety participation in the investigation of all safety mishaps and safety-related failures involving program hardware, systems, equipment, or operations. Mishap investigation results are incorporated into subsequent program activities to avoid recurrence.

Integration Site and Launch Site Safety Support is a system safety coordination activity with the integration site, launch site with customer representatives to verify applicable safety requirements are met. Hazardous operations and procedures for use at integration and launch sites are submitted for review and approval by the customer safety organizations.

A6-3 Matrix - System Safety

Recommended System Safety activities vary widely by system and application. For example, a relatively inexpensive space or missile test or experiment that is otherwise considered Class D might not warrant as much concern over loss of system as a full-scale operational system would. However if the Class D system poses a potential risk to personnel, the public, the environment, or valuable assets, its risk might more appropriately be addressed in a similar way to operational systems with similar hazard potential. Levels of System Safety activity should be formulated using recognized standards such as ANSI/GEIA-STD-0010 or MIL-STD-882C. Provided below is a summary of risk class profile support from System Safety Mission Class Matrix.

Requirement	Class A	Class B	Class C	Class D
System Safety				
Requirements Identification, Allocation, and Verification	• Assess program, integration, and launch site safety requirements and incorporate as appropriate in design, test, and operations documentation. • Covers prelaunch, launch, post launch and operations, including end-of-life	• Same as Class A	• Same as Class A. Need to provide support and necessary data to satisfy primary mission	• Same as Class A. Need to provide support and necessary data to satisfy primary mission
Safety Analysis	• PHL; PHA; SSHA; SHA; Software Safety Analysis; Support for On-Orbit Hazard Analysis, Space Debris Assessment, EOLP and COLA; O&SHA per program operations outside of contractor facility; Health Hazard Assessment; Safety Review of Engineering Change Proposals, Specification Change Notices, Software Problem Reports, and Requests for Deviation/ Waiver	• Same as Class A but may have a more limited scope	• Same as Class A with exception that input may be provided to satisfy primary mission requirements	• Same as Class A with exception that inputs may be provided to satisfy primary mission requirements
Safety Risk Assessment	• Hazard probability of occurrence and severity	• Same as Class A	• Same as Class A	• Same as Class A
Safety Documentation	• Formal system safety plan is required as deliverable. MSPSP/MRAR, Hazard Reports or Input to prime if subcontractor effort is on contract	• Same as Class A	• MSPSP/MRAR and hazard reports required but less detailed, System safety plan may leverage contractor best practices and is tailored to the scope of the mission Class C system	• MSPSP/MRAR and hazard reports required but less detailed. System safety plan may be required; as a minimum developer must ensure payload is safe to integrate and launch
Support of Hazardous and Safety-Critical Activities	• Hazardous procedure review/approval, test readiness reviews, test monitoring	• Same as Class A	• Same as Class A	• Same as Class A
Mishap Reporting and Investigation	• Formal Mishap investigation and reporting	• Same as Class A	• Same as Class A	• Same as Class A

Requirement	Class A	Class B	Class C	Class D
System Safety				
Integration Site and Launch Site Safety Support	• Coordination, hazardous procedures submittal	• Same as Class A	• Same as Class A	• Same as Class A

A6-4 Summary of Risk Classes

Recommended System Safety activities vary widely by system and application. For example, a relatively inexpensive space or missile test or experiment that is otherwise considered Class D might not warrant as much concern over loss of system as a full-scale operational system would. However if the Class D system poses a potential risk to personnel, the public, the environment, or valuable assets, its risk might more appropriately be addressed in a similar way to operational systems with similar hazard potential. Levels of System Safety activity should be formulated using recognized standards such as ANSI/GEIA-STD-0010 or MIL-STD-882C. Provided below is a summary of risk class profile support from System Safety Mission Class Matrix.

Class A. System safety process applies assessment and analyses throughout the life cycle of a system to control system hazards within the constraints of operational effectiveness, schedule, and cost. System safety should be incorporated as an inherent element of system design with relevant system safety requirements incorporated and allocated. Successful efforts depend on clearly identifying and mitigating hazards. System safety must be planned and integrated as a comprehensive effort employing engineering and management resources. A formal systems safety program is required, with well-understood tasks agreed to by the customer; a plan and an analysis/hazard tracking report are required as a deliverable. The plan includes direction to support formal mishap safety investigations in case of unintentional mission loss or major mission impact resulting from unplanned or catastrophic events.

Class B. Same as Class A. A formal systems safety program with a plan is a required deliverable. In the case of FFP contracts that may be applied to mission Class B systems, system safety is required to be assessed early on and the contractor team has the responsibility to work and resolve issues, and raise issues to the independent government safety team.

Class C. A formal system safety program is required and often leverages the contractor best practices in their facility. System safety is required to be assessed early on and the contractor team has the responsibility to identify, work, and resolve issues.

Class D. As a minimum the developer needs to prove the space vehicle is safe to integrate and launch. The system safety program is dependent on the contractor best practices for their facility.

A6-5 Effectiveness TIPS (Lessons Learned)

- Prevent unnecessary hazards by designing in safety.
- Define the interactions between the customer and contractor in executing system safety requirements.
- Identify the management and approval process for new and unresolved hazard risks with technically qualified support safety staff to advise and assist.
- Manage residual hazard by assuring the proper level of management acceptance for residual hazard risks.

A6-6 References

1. Aerospace Report TOR 2007(8546)-6018, *Mission Assurance Guide*.
2. Aerospace Report TOR-2010(8591)-18, *Mission Assurance Framework*.
3. Aerospace Report TOR-2011(8591)-5, *Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles*.
4. SMCI 63-1201, *Assurance of Operational Safety, Suitability, and Effectiveness for Space and Missile Systems Center*.

5. SMCI 63-1205, *Space System Safety Policy, Process, and Techniques*.
6. AFI 91-202, *USAG Mishap Prevention Program*.
7. ASSPCMAN 91-710, *Range Safety User Requirements Manual*.
8. *Programmatic Environmental, Safety, and Health Evaluation Guide*, Space and Missile Systems Center.
9. MIL-STD-882C, System Safety Program Requirements.
10. MIL-STD-882D, *Department of Defense Standard Practice for System Safety*.
11. ANSI/GEIA-STD-0010, *Standard Best Practices for System Safety Program Development and Execution*.
12. Aerospace Report TOR-2006(8506)-4494, *Space Vehicle Systems Engineering Handbook*.

Appendix A7: Configuration Change Management

Mark Oja, ATK

A7-1 Introduction

This appendix provides guidelines for applying effective configuration and change management to space systems. The methods of configuration management may be tailored to meet the needs of the program; however, a configuration management process is required at some level for any space system development activity and should be addressed over the lifecycle of the program. The process may be applied to all space flight systems; to include deliverable payloads, space vehicles, or other associated products. Formal configuration management requirements are typically dictated by the acquisition authority per the contract or developed in accordance to the contractor's best practices commensurate with the level of risk associated with the specific mission. Generally, the developer is responsible for implementing an organized Configuration Management Program (CMP) commensurate with the risk profile of the program and mission. This CMP is generally outlined in a Configuration Management Plan which is endorsed by the customer early in the program lifecycle.

The primary objective to the contractors' CMP is to establish and maintain consistency and accurate knowledge of a product's performance, functional, and physical attributes with its requirements, design, and operational information throughout its life cycle. Configuration management is a process, which implements efficient application of configuration management principles and practices to the identified context and environment. Change management is the practice of effective communication and managing of potential or actual changes affecting a program. Communication of potential or actual changes combined with effective analytical tools and processes allow the program team to evaluate and make informed decisions regarding technical performance, cost, and schedule impacts.

A7-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which risk profile can be developed and are not intended as general standalone industry standard definitions.

Configuration Management Planning. The establishment of the configuration management(CM) approach for a given program including the programs planned processes and practices for CM. Configuration management planning covers:

1. Definition of the configuration management system
2. Identification and management of project data and configuration items
3. Planning and control of project baselines
4. Planning of configuration audits and status accounting
5. Build and release management
6. Data backup and recovery planning

Configuration Identification. The purpose of configuration identification shall be to incrementally establish and maintain a definitive basis for control and status accounting for a configuration item (CI) throughout its life cycle. Configuration identification includes:

1. the selection of CIs; the determination of the types of configuration documentation required for each CI
2. the issuance of numbers and other identifiers affixed to the CI and to the technical documentation that defines that CI's configuration, including internal and external interfaces
3. the release of CIs and their associated configuration documentation
4. the establishment of configuration baselines for CIs

Change Control. The systematic proposal, justification, evaluation, coordination, approval or disapproval of proposed changes, and the implementation of all approved changes, in the configuration of a CI after establishment of the configuration baseline(s) for the CI.

Interface Control. The process of identifying, documenting, and controlling all functional and physical characteristics relevant to the interfacing of two or more items provided by one or more organizations.

Configuration Status Accounting (CSA). The recording and reporting of information needed to manage configuration items effectively, including:

1. A record of the approved configuration documentation identification numbers
2. The status of proposed changes, and deviations, to the configuration
3. The implementation status of approved changes
4. The configuration of all units of the configuration item in the operational inventory

Configuration Verification/Audits. Includes both Functional Configuration Audit (FCA) and Physical Configuration Audit (PCA). FCA is the formal examination of functional characteristics of a configuration item, prior to acceptance, to verify that the item has achieved the requirements specified in its functional and allocated configuration documentation. PCA is the formal examination of the "as-built" configuration of a configuration item against its technical documentation to establish or verify the configuration item's product baseline.

Additional Definitions:

Baseline. A formally approved version of a configuration item, regardless of media, formally designated and fixed at a specific time during the configuration item's life cycle. (Source: ISO/IEC 12207)

Computer software documentation. Technical data or information, regardless of media, which documents the requirements, design, or details of computer software; explains the capabilities and limitations of the software; or provides operating instructions for using or supporting computer software during the software's operational life cycle.

Configuration. Configuration is defined as the functional and physical characteristics of existing or planned hardware, firmware, or software or a combination thereof as set forth in technical documentation and ultimately achieved in a product.

Configuration baseline. Configuration documentation formally designated by the government at a specific time during a CI's life cycle. Configuration documentation, plus approved changes from that documentation, constitutes the current approved configuration baseline. There can be three formally

designated configuration baselines in the life cycle of a configuration item, the functional, allocated, and product baselines.

Configuration Control Board (CCB). A board composed of technical and administrative representatives who recommend approval or disapproval of proposed engineering changes to a CI's current approved and baseline configuration documentation. The board also recommends approval or disapproval of proposed deviations from a CI's current approved and baseline configuration documentation.

Configuration documentation. The technical documentation, including architectural and design products, that identifies and defines the item's functional and physical characteristics. The configuration documentation is developed, approved, and maintained through three distinct evolutionary increasing levels of detail. The three levels of configuration documentation are the functional (build-to) configuration documentation, the allocated (design-to) configuration documentation, and the product (as-built) configuration documentation.

Configuration Management Plan (CMP). The CMP document defines how configuration management will be implemented (including policies and procedures) for a particular acquisition or program.

Fit. Fit is the ability of an item to physically interface or interconnect with or become an integral part of another item.

Form. Form is the shape, size, dimension, mass, weight, and other visual parameters, which uniquely characterize an item. For software, firmware form denotes the language and media.

Function. Function is the action or actions, which an item is designed to perform.

Interface. The functional and physical characteristics required existing at a common boundary.

Interface Control Documentation (ICD). Interface control drawings, requirements, or other documentation, which depicts physical and functional interface of related or co-functioning items.

A7-3 Matrix – Configuration/Change Management

Tasks	Class A	Class B	Class C	Class D
Configuration Management (CM) Planning	• Developer generates a configuration management plan, which describes the programs planned processes and practices for CM • Plan is reviewed and approved by the governing agency	• Same as Class A	• Planned CM practices are describe in a CM plan or as outlined in the program plan • Governing agency involvement is through contract requirements not plan approval • Contractor best practices	• Similar to Class C • CM processes are as defined in company policies and procedures
Configuration Identification	• Product identifiers, product information, product structure and document identification at a level such that unique item identification is employed for changes that could affect form, fit or function • Government oversight includes periodic auditing of the CM system	• Same as Class A	• Similar to Class A with fewer defined part identification points. • Government oversight is minimal	• Same as Class C
Change Control including program changes	• Changes, following production baseline, to product designs, build processes or software code are reviewed using a systematic change process • Classification is employed to distinguish significance of changes. Change Boards are used to review changes • The customer is fully involved in the review/approval process. • All Class I changes (those that change form, fit, or function) must be approved by customer • All Class II changes are reported to the customer	• Same as Class A	• Same as Class A, exception that all Class II changes may not be reported but available for review	• Minimal change review beyond the working team. • Peer review of significant changes. • Documentation of changes may be less formal but should exist in some form

Tasks	Class A	Class B	Class C	Class D
Interface Control	• Interfacing features are identified in the design. • Changes are formally coordinated with the affected parties • An interface control plan is generated and approved by the governing agency	• Same as Class A	• Interface features are identified in the design. • Changes are coordinated with the affected party	• Same as Class C
Configuration Status Accounting	• Real time data can be generated regarding product use, build history, change information and tractability	• Same as Class A	• Data can be generated regarding product use, build history, change information and tractability	• Same as Class C
Configuration Verification/Audits including Functional and Physical configuration Audits	• Periodic audits are performed to assure products design and build products conform to defined product requirement attributes. • Government representative are often represented in these audits	• Same as Class A with less government involvement	• Similar to Class A with less frequency of audits • Minimal to no government involvement	• Audits are not generally performed

A7-4 Summary of Risk Classes

Class A. For low-risk tolerant programs (Class A), the CMP will establish and maintain consistency with the highest standards for CM requirements. Requirements are defined by contract and practices employed by the contractor and are codified in a CM plan approved by the contracting body. The plan would define processes and practices necessary to mange configuration identification, change management, configuration status, interface control and configuration audits. For Class A programs, government agencies typically have full approval of changes and provide oversight to the contractor's configuration control and management practices.

Class B. The only difference in the CM program between a Class A and a Class B program is less than full customer involvement in changes deemed low risk.

Class C. Class C programs allows for a CM program with much less customer involvement in the execution of the program. Change identification, change documentation, configuration status and change control principles are still employed to accomplish effective configuration management however baseline definition, government and contractor internal oversight to changes and auditing are often accomplished with less rigor, relying more on the developers and executors to assure acceptability of changes and the management of changes. Supporting CM databases and information systems may be less responsive to configuration requests for a Class C program.

Class D. Class D programs allow even more tailoring of configuration management program. Audits are not typically performed. Change review may be done by peers or area leadership. The customer would typically only be involved with interface control changes.

A7-5 Effectiveness TIPS (lessons learned)

- Early definition of planned CM activities in the Program Plan or CM Plan helps assure a common understanding of planned CM activities
- Judicious identification of critical features during the design phase help focus CM activities and resources
- First article inspection and rigorous process control is effective in managing multi-unit fabrication programs
- Early evaluation of the strengths and weaknesses and risk with the planned supply base to focus supplied CM
- CM applies equally to software products as hardware products
- Program involvement in the readiness for planned audits helps assure effective execution
- The instruction of a Change Control Board is fundamental to a good CM program
- The transition from development to production should be well defined since CM requirements generally change at this point in the program lifecycle
- All changes should include some sort of independent review prior to implementation

A7-6 References

1. ISO 9001:2008, *Quality Management Systems, Requirements*, 11 November 2008.
2. ISO 1007, Guidelines for Configuration Management.
3. SAE AS9100C, *Quality Management Systems – Requirements for Aviation, Space and Defense Organizations*, 15 January 2009.
4. ANSI/EIA 649, *National Consensus Standard for Configuration*, 29 October 2004.
5. SMC Standard SMC-S-002, *Configuration Management*, 13 June 2008.

Appendix A8: Integration, Test and Evaluation

David Kalian, The Boeing Company
Jean-Claude Inauen, Northrop Grumman

A8-1 Introduction

Integration, Test and Evaluation (IT&E) is a broad process whose purpose is to: (1) integrate space systems in a typically tiered structure comprised of components, subassemblies, assemblies, and subsystems, (2) validate (in some cases verify) through test that the hardware and software meet program/project requirements and (3) provide documentation on the performance and overall compliance. From a systems or responsible engineering perspective, the focus is on ensuring that the elements are physically and functionally compatible and on providing data which verifies end item requirements satisfaction (e.g., functionality, performance, design/construction, interfaces, and environment). The emphasis for mission assurance extends to validating compliance to assembly and test processes which ensure mission success as well as ensuring that robust design margins have been retained, results have been properly documented and reviewed, and that appropriate configuration control has been maintained. Where tailoring is called out in the matrix it is intended to be consistent with Aerospace Report No. TOR-2011(8591)-5, Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles, dated September 13, 2010. Note that the MAIW 2010 framework calls out lower tier assemblies down to components. For the purposes of this appendix, these are considered part of hardware quality.

The table in Section 3 is divided into integration, test, and evaluation subsections in order to emphasize the important aspects of each. Where specifics are given they are meant to illustrate the intent versus being rigid standards. It is noted that while quality and other forms of independent inspections are part of evaluation in the broader sense, they are also ingrained into the fabric of the integration and test process and so are called out in those sections. In order to further clarify the intent of the entries, definitions are given in Section 2. These definitions are meant to guide the reader in interpreting the table and are not intended as industry standards.

A8-2 Definitions

The following define the intended definition used to build the row entries of the risk matrix A8-3 Integration, Test, and Evaluation. The intent was to follow the guidelines of the Mission Assurance Program Framework Document Table 4-2, entry 8.

Integration. The process of physically assembling hardware and/or software and checking out the functionality of such assembled hardware/software.

Ground Support Equipment (GSE). Any hardware or software required for integration and test of a vehicle which is not part of the delivered vehicle.

Interfaces. The meeting of mechanical, electrical, or software boundaries.

Integration Functional Testing. Testing performed to validate successful integration steps, which may or may not demonstrate compliance of the integrated assembly.

In Process Screening. Inspection steps inserted during integration to validate mechanical/physical process steps.

Testing Requirements Compliance and Validation. Those test activities specifically intended to demonstrate compliance to environmental, functional, or performance requirements.

Software Validation Testing. Testing to demonstrate software requirements and interface compliance and system stability.

Qualification. The process of demonstrating that the hardware and software will perform under the required mission environments over the required mission life.

Performance Testing. Testing performed under specific environmental conditions to demonstrate capability to operate and be compliant with mission requirements.

System Test/External Interfaces. Testing that demonstrates compliance to vehicle external interfaces such as ground segments, relays (if applicable), and launch vehicle systems.

End-to-End System Test. Extended operational testing intended to exercise the vehicle against the ground segment command and control and data processing, in as flight-like a condition as possible.

Launch Support and Compatibility Testing. Testing to validate launch vehicle interfaces as well as launch system compatibility including command and control and telemetry.

Evaluation. Activities performed to determine the suitability of the product to perform its intended mission. The evaluation process involves all aspects of program execution and as such is generally integral to the program execution plan. Evaluation, in the context of integration and test, includes the activities necessary to assess all of the aspects of the integration and test process as well as the results. This would include the suitability of a planned test program to provide adequate proof of performance, the comparison of analytical results and predictions with test result, the adequacy of the test program as actually executed, and the assessment of test data to determine the suitability of the product to perform the mission.

Independent Reviews. Formal or informal reviews performed by subject matter experts outside the program office chain of command. See Appendix B2 Independent Reviews.

GSE HW Validation. The process utilized to validate the readiness of GSE HW as safe and properly configured for use on flight hardware.

GSE SW Validation. The process utilized to validate the readiness of GSE SW as safe and properly configured for use on flight hardware.

Integration Records. Documentation kept during the integration process.

Data Analysis Tools. Tools used to process vehicle test data to trend performance and demonstrate compliance.

Hardware Acceptance. Process of buying off hardware delivered for integration as compliant and ready. Also see Appendix B3 Hardware Quality.

Analysis Model Validation. The process of verifying or validating, generally through test data, any analytical model used to manipulate data as part of the requirements compliance process.

Test Evaluation. The process of validating that the conditions of the test and the test results demonstrate compliance.

Test Logs. Test documentation that captures the execution of steps and specific observations, which may have bearing on the system, GSE, or test results.

Test Execution. The process of demonstrating readiness for, execution of, and close-out steps from planned testing.

Non-Conformances. Noted conditions in hardware, software, or GSE data which is outside defined operating conditions. Also see Appendix C1 Failure Review Board.

The following additional definitions were utilized in developing the risk matrix entries for this appendix.

Copper Paths. Port-to-port hardline connections including all electrical or mechanical switch configurations, which are touched in the integration step being performed.

Critical. Any system element that has some inherent risk either due to the required technology or technology maturity, and/or which represents a significant mission risk. System elements that do not have redundancy and which, upon failure, would compromise the primary mission.

Customer. The agency and/or agent for the agency that is responsible for the procurement of the integrated system.

Electrical interfaces. Any joining of wires or materials whose purpose is the electrical conduction of power or analog or digital signals.

Day-In-The-Life (DITL). The running of a system or sub-system in a configuration and sequence representative of a nominal on-orbit day for the system.

High Fidelity Simulator. Simulators that have flight-like hardware running flight code which, to fullest extent possible, represent the ground system and interface to the space system.

Mechanical interfaces. The structural union between two mechanical assemblies mated together. Mounting of units or components or other mechanical materials and assemblies such as EMI gasket seals, thermal interfaces, and mechanical assembly points with specific electrical, thermal, or EMI significant properties.

Program Office. The primary contractor management team responsible for the design, fabrication, integration, test, and delivery of deliverable product.

Quality Assurance (QA). Individuals with responsibility for verifying processes, executed work, and documentation meet established standards and requirements.

Space Vehicle. A space vehicle is an integrated set of subsystems and units capable of supporting an operational role in space. A space vehicle may be an orbiting vehicle, a major portion of an orbiting vehicle, or a payload which performs its mission while attached to a launch or upper-stage vehicle.

Test. Any program or procedure that is designed to obtain, verify, or provide data for the evaluation of research and development (R&D), other than laboratory experiments; progress in accomplishing

development objectives; or performance and operational capability of systems, subsystems, components, and equipment items. An activity performed to determine output characteristics of the IUT as a function of variable inputs. Tests are used to learn aspects of design in new items and to verify performance in comparison to requirements. “Aspects of design” include, but are not limited to, proof of concept, functionality, performance, margins, and failure modes. Tests are also performed to verify aspects of mathematical analysis.

Validation. The efforts involved in showing that the correct design was built. This can apply to delivered systems prior to flight, asset operations post-launch, and the equipment and software used to test, characterize, and calibrate the delivered system. The function of ensuring that the design developed for the delivered system will result in assets that meet the operational needs of the customer is accomplished in stages.

Verification. An evaluation of the performance of the as-designed and as-built end-items with respect to defined requirements. The verification methods are: inspection, test, analysis, demonstration, similarity, process control, physical measurement, and destructive physical analysis. Similarity and process control are not particularly applicable to space systems, as these are best suited for high volume production; inspection, physical measurement, and destructive physical analysis will not be elaborated on in this version. Analysis and demonstration have aspects that are related to test.

A8-3 Matrix - Integration, Test and Evaluation

Category	Class A	Class B	Class C	Class D
Integration	• Integration follows all quality standards and processes. • Independent inspections and QA sign-offs employed at each integration tier	• Integration follows all quality standards and processes • Independent inspections at system and subsystem levels • QA sign-offs employed at each integration tier	• Integration follows all quality standards and processes • Limited independent inspections for critical items • QA sign-offs employed at each integration tier	• Subsystem integration uses contractor best practice
Ground Support Equipment (GSE)	• GSE is treated as flight hardware/software and has flight safety checks in place	• GSE is treated as flight hardware/software and has flight safety checks in place	• GSE follows best practices and has flight hardware/software safety checks in place	• Contractors' best practices used in order to meet the mission objectives
Interfaces	• Pre-mate connector checks are implemented on every mate • Electrical and mechanical mates are independently inspected by QA • Photo records kept of critical in process work for both electrical and mechanical mates • Mate/De-mate and installation logs are independently certified	• Pre-mate connector checks are implemented on all critical mates • Electrical and mechanical mates are independently inspected by QA • Photo records kept of critical in process work for both electrical and mechanical mates • Mate/De-mate and installations logs are independently certified	• Pre-mate connector checks are implemented on all critical flight mates • Integration team employs own second party inspection for critical flight mates • Electrical and mechanical mates are performed to quality standards and signed off • Mate/De-mate and installation logs are maintained by I&T team and audited by QA	• Best practices are employed, QA reviews and approves approach • Electrical and mechanical mates follow best practices tailored for program requirements
Integration Functional Testing	• All functions are tested at each level of integration (all copper paths) • Final integration verifies complete functionality including T&C. Subsystems utilize GSE high fidelity simulators to validate interfaces • Box and component tests utilize GSE validated against interface specs	• At each integration level all functions impacted (all copper paths) are tested • Final integration verifies complete functionality including T&C • Subsystems utilize GSE simulators • Box and component tests utilize GSE validated against interface specs	• All functions are tested at final integration • Final integration validates complete functionality including T&C • Subsystem, box, and component tests utilize GSE validated against interface specs	• All mission critical functions (all copper paths) are tested at final integration • Final integration validates functionality and T&C consistent with program risk posture • Subsystem, box, and components tested against GSE representing interface

Category	Class A	Class B	Class C	Class D
In process screening	• Harnesses are inspected, cleaned and continuity checked prior to installation • Blankets are inspected and checked against drawings prior to installation • All tie downs, brackets, and fittings are inspected and checked against drawings prior to installation • Flight parts and GSE are each logged and accounted for prior to and after each shift • Quality signs off on all screening steps	• Same as Class A	• Harnesses are inspected and cleaned for any obvious damage • Flight parts and GSE are each logged and accounted for prior to and after each shift	• Contractors' best practices used in order to meet the mission objectives
Testing – Requirements Compliance and Validation	• Full implementation of TOR-2006(8546)-4591 "Space Vehicle Test and Evaluation Handbook." • Full compliance to SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A or NASA document GSFC-STD-700 General Environmental Verification Specification dated April 2005 for qualification requirements	• Full implementation of TOR-2006(8546)-4591 "Space Vehicle Test and Evaluation Handbook" • Compliant to SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A or NASA document GSFC-STD-700 General Environmental Verification Specification dated April 2005 for protoqualification requirements	• Implementation of TOR-2006(8546)-4591 "Space Vehicle Test and Evaluation Handbook" with minimal tailoring • Compliant to SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A or NASA document GSFC-STD-700 General Environmental Verification Specification dated April 2005 for protoqualification requirements with minimal tailoring	• Implementation of TOR-2006(8546)-4591 "Space Vehicle Test and Evaluation Handbook" with tailoring • Compliant to SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A or NASA document GSFC-STD-700 General Environmental Verification Specification dated April 2005 for acceptance requirements with minimal tailoring
SW Validation	• SW meets all quality standards • Databases are verified through test and configuration controlled • T&C is verified through test • Independent validation performed • *Reference Appendix B4: Software Assurance*	• SW meets standards tailored for program requirements • Data bases are validated and configuration controlled • T&C is verified through test • Independent validation performed • *Reference Appendix B4: Software Assurance*	• SW based on best practices. • Data bases are validated and configuration controlled • T&C is validated • Independent validation of critical algorithms performed • *Reference Appendix B4: Software Assurance*	• SW based on best practices. • Data bases are validated • Mission critical T&C is validated • *Reference Appendix B4: Software Assurance*

Category	Class A	Class B	Class C	Class D
Qualification	• Qualification method selected is documented with customer approval • Qualification article and levels, minimum use of proto-qualification testing of flight units • Subsystems and units functionally tested to environments plus margin at qualification/proto-qualification levels	• Qualification method selected is document with customer review. • General use of proto-qualification testing of flight units versus Qualification articles • Subsystems and Units similar to Class A, except number of cycles, margins, and duration of test may be tailored based on program risk assessment and acceptance	• System test plan required with customer review • System functional and proto-qualification tests to acceptance levels, to include acoustic, random vibration, shock, thermal vacuum, deployment, EMI/EMC • Subsystems functionally stress tested to margins exceeding what will be experienced during system testing Component/box testing conducted to meet mission requirements, usually at acceptance levels • Tailoring of Environmental Test requirements	• No formal qualification testing. Safety and compatibility testing required by the launch vehicle provider and/or launch base • Other testing at discretion of developer with an informal test program usually followed. Unit tests at discretion of developer • Limited if any customer or other independent review
Performance Testing	• Verifies specification requirements per SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A or NASA document GSFC-STD-700 General Environmental Verification Specification dated April 2005 • Mission profile test performed for all mission phases (Test Like You Fly) consistent with TOR-2009(8591)-15, Space Vehicle Checklist for Assuring Adherence to "Test-Like-You-Fly" Principles, June 2009 • Test compliance per TOR-2005 (8583)-1 Rev A (MIL-STD-1541A), EMC Requirements for Space Systems, dated January 2008 • Test performed to assess operability of item under test within design requirements	• Verifies specification requirements per SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A or NASA document GSFC-STD-700 General Environmental Verification Specification dated April 2005 • Mission profile test performed for all mission phases consistent with TOR-2009(8591)-15, Space Vehicle Checklist for Assuring Adherence to "Test-Like-You-Fly" Principles, June 2009 • Test compliance per TOR-2005 (8583)–1 Rev A (MIL-STD-1541A), EMC Requirements for Space Systems, dated January 2008 • Test performed to assess operability of item under test within design requirements • Test before and after each environmental test	• Verifies specification requirements per SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A or NASA document GSFC-STD-700 General Environmental Verification Specification dated April 2005 with minimal tailoring • Mission profile test performed consistent with program risk posture. Tailored use of TOR-2009 (8591)-15, Space Vehicle Checklist for Assuring Adherence to "Test-Like-You-Fly" Principles, June 2009 • Test with limited tailoring compliance per TOR-2005 (8583)-1 Rev A (MIL-STD-1541A), EMC Requirements for Space Systems, dated January 2008 • Test performed to assess operability of item under test within design requirements	• Verifies specification requirements per SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A or NASA document GSFC-STD-700 General Environmental Verification Specification dated April 2005 with tailoring consistent with program risk posture • Limited mission profile test performed • Test tailored consistent with program risk posture compliance per TOR-2005(8583)-1 Rev A (MIL-STD-1541A), EMC Requirements for Space Systems, dated January 2008 • Test performed to assess operability of item under test within design requirements. • *Reference Appendix A4: Environmental Compatibility*

Category	Class A	Class B	Class C	Class D
	• Test before and after each environmental test • Redundancy tested • *Reference Appendix A4: Environmental Compatibility*	• Redundancy tested • *Reference Appendix A4: Environmental Compatibility*	• Test before and after each environmental test • *Reference Appendix A4: Environmental Compatibility*	
System Test/External Interfaces	• Full Test-Like-You-Fly approach applied to ensure space-ground and mission compatibility	• Same as Class A, but may use high-fidelity simulators/emulators for end-to-end testing	• Same as Class B, but fidelity of simulators/emulators for end-to-end testing tailored based on programmatics.	• Limited if any end-to-end testing, external interfaces modeled
End-to-End System Test	• System test performed at the factory and at the launch site. RF link may be enabled by GSE • Day in the life (DITL) run in the factory initially against GSE and then through ground site	• System test performed at the factory and at the launch site. RF link may be enabled by GSE • Day in the life (DITL) run in the factory initially against GSE and then through ground site	• System test performed at the launch site. RF link may be enabled by GSE • Limited Day in the life (DITL) testing may be enabled by GSE	• Depends on ground system used • Needs to work with ground system which is usually home grown; testing deferred to satellite • Limited to no DITL tests
Launch Support and Compatibility Tests	• Full Compliance to SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A • Pre-compatibility test performed generally at contractor factory with AFSCN/DSN Tester Van • Final compatibility test performed late in flow (preferably after final integration with the LV) and encompasses flight vehicle in final configuration prior to launch (configuration frozen) • Tests all compatibility functions with LV and operations (RF interfaces, command and telemetry paths, critical mission modes) • Redundant and cross-strapping paths included • All mechanical and electrical mates 'fit" checked prior to spacecraft shipping	• Same as Class A	• Compliance to SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A • Pre-compatibility test performed generally at contractor factory with AFSCN Tester Van • Final compatibility test performed late in flow (preferably after final integration with the LV) and encompasses flight vehicle in final configuration prior to launch (configuration frozen) • Tests critical compatibility functions with LV and operations (RF interfaces, command and telemetry paths) • All mechanical and electrical mates checked prior to spacecraft shipping	• Compliance to SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A • Pre-compatibility test recommended • Final compatibility test performed late in flow (preferably after final integration with the LV) and encompasses flight vehicle in final configuration prior to launch (configuration frozen) • Tests critical compatibility functions with LV and operations (RF interfaces, command and telemetry paths) • All launch critical mechanical and electrical mates checked prior to spacecraft shipping

Category	Class A	Class B	Class C	Class D
Evaluation	• Customer engaged at subsystem level and below	• Same as Class A, except with customer review/involvement for certain reviews (review rather than approval authority)	• Customer review and approval at system level only	• Customer reviews approves program plan and interacts at program reviews and established program milestones
Independent Reviews	• Formal Independent Reviews/ Audits will be performed by customer/contractor teams • *Reference Appendix B2: Independent Reviews*	• Formal Independent Reviews/Audits will be performed • *Reference Appendix B2: Independent Reviews*	• Independent reviewers will track the IT&E activities and will perform IRs at an Ad Hoc Basis • *Reference Appendix B2: Independent Reviews*	• No formal IRs. Independent reviewers will monitor IT&E work • *Reference Appendix B2: Independent Reviews*
Verification and Test Plans and Procedures	• Complete system to subsystem to unit requirement verification plan, test plans, procedures, test reports, and requirement verification are developed and delivered • Customer approves verification plans, test plans, and procedures • QA sign-off and configuration controlled, independent reviews of plans and procedures utilizing independent subject matter experts • As run procedures configuration controlled and are part of acceptance data package	• Complete system to subsystem to unit requirement verification plan, test plans, procedures, test reports, and requirement verification are developed and delivered • Customer review and approval of verification plans, test plans, and procedures at system and subsystem levels • QA sign-off and configuration controlled, independent reviews of plans and procedures utilizing independent subject matter experts • Redlines permissible signed off by QA and with independent review • As run procedures configuration controlled and are part of acceptance data package	• Complete system to subsystem to unit requirement verification plan, test plans, procedures, test reports, and requirement verification are developed. System level documents delivered • QA sign-off and configuration controlled, independent reviews of system and subsystem level test plans and procedures utilizing independent subject matter experts • Redlines permissible signed off by QA • As run procedures configuration controlled and are part of acceptance data package.	• System verification plan, test plans, procedures, test reports, and requirement verification are developed consistent with contractor best practices • Customer approval of system test plans • Test plans and procedures configuration controlled, independent reviews of system and subsystem level test plans and procedures consistent with program risk posture • Peer review of test plans and procedures • Redlines permissible • As run procedures maintained
GSE HW Validation	• GSE is treated as flight HW with same configuration control and anomaly RCCA • GSE is validated as meeting GSE requirements as well as being safe for use on flight HW	• GSE is treated as flight HW with same configuration control and anomaly RCCA • GSE interface requirements are verified and are certified as safe to use on flight HW	• GSE is configuration controlled and certified as safe to use on flight HW • GSE interface requirements are verified consistent with program risk posture	• GSE is certified as safe to use on flight HW • GSE interface requirements are validated consistent with program risk posture
GSE SW Validation	• GSE SW treated as flight SW • *Reference Appendix B4: Software Assurance*	• GSE SW configuration controlled and validated like flight SW • *Reference Appendix B4: Software Assurance*	• GSE SW is validated and version control maintained • *Reference Appendix B4: Software Assurance*	• GSE SW is validated • *Reference Appendix B4: Software Assurance*

Category	Class A	Class B	Class C	Class D
Integration Records	• Formal log required that captures integration step completion, mechanical activation, environment exposure including ambient temperature and humidity, and data specific to any component or assembly with limited life risks • Customer audits and signs off all logs and inspection points. QA signs off on recorded data, with periodic independent audits • Formal As-Built and As-Integrated logs kept with QA review and sign off • Formal Red Tag/Green Tag logs kept with QA sign-off required	• Same as Class A	• Formal logs are kept with QA auditing process using contractor best practices • Formal Red Tag/Green Tag logs kept with QA monitoring and auditing process	• Informal logs are kept (i.e., MS Excel spreadsheet) with QA periodically auditing process and logs to contractor best practices
Data Analysis Tools	• Tools are documented, controlled, and validated against flight like data • All data handling interfaces are verified through test	• Tools and interfaces are formally documented and validated	• Tools and interfaces are validated	• Tools are informal engineering development
Hardware Acceptance	• Formal gated practices used for hardware sell-off to next level. Customer involvement at all levels • Independent reviewers involved with all hardware non-conformances • See Appendix B3: Hardware Quality	• Formal gated practices used for hardware sell-off to next level • Customer involvement at subsystem and system level and for critical units • Independent reviewers involved with all hardware non-conformances • See Appendix B3: Hardware Quality	• Tailored gated practices used for hardware sell-off to next level • Customer involvement at subsystem and system levels • Independent reviewers involved with critical hardware non-conformances • See Appendix B3: Hardware Quality	• Informal gated practices used for hardware sell-off to next level. Customer involvement system level • Independent reviewers Monitors and audits process • See Appendix B3: Hardware Quality
Analysis Model Validation	• Analysis models used in verification process meet Verification and Validation (V&V) standards • Models used for functional or performance assessment have independent validation	• Analysis models used in verification process meet Verification and Validation (V&V) standards • Models used for functional or performance assessment have independent validation	• Models used for functional or performance assessment are validated	• Models used in performance assessment are validated

Category	Class A	Class B	Class C	Class D
Test Evaluation	• Formal test reports are generated and customer approved at system and subsystem level • Formal Review and approval of all test reports by independent reviewers and QA • Independent subject matter experts review test reports	• Formal test reports are generated and customer approved at system and subsystem level • Formal Review and approval of all test reports by independent reviewers and QA • Independent subject matter experts review test reports	• Formal test reports are generated and customer reviewed at system and subsystem level • QA sign-off, independent reviewers review process and survey results • Independent subject matter experts review key test reports	• Test reports are generated and delivered at system and subsystem level consistent with contractor best practices • Independent subject matter expert review of critical reports consistent with program risk posture
Test Logs	• Formal Configuration Controlled Test Logs signed off by QA and independent reviewers	• Formal Configuration Controlled Test Logs, signed off by QA and independent reviewers	• Informal (MS Excel) Test Logs monitored and audited by independent reviewers	• Informal (excel) Test Logs maintained. Limited if any independent review
Test Execution	• Independent (customer and/or contractor) review of contractor test plans, procedures, set-up, execution, and data analysis • Customer approves BOCs and Test Readiness Reviews (TRRs) at system and subsystem levels	• Test Readiness Reviews (TRRs), Post Test Reviews and Break of Configuration (BOC) Reviews are performed • Independent (customer and/or contractor) review of critical items and survey of processes and procedures	• Limited customer oversight and participation during system and subsystem test activities • Independent (customer and/or contractor) review of critical items and survey of processes and procedures • Some independent review	• Customer reviews available integration and test documentation, and interacts at established program reviews • Critical test set-ups, procedures, and data may be reviewed based on program risk posture
Non-Conformances	• Formal MRB Process shall be documented and approved by customer • Customer approval of all non-conformity dispositions and system/subsystem FRB actions • Formal FRB Process. • *Reference Appendix C1: Failure Review Board* • *Reference Appendix B3: Hardware Quality Assurance* • *Reference Appendix B4: Software Assurance*	• Formal MRB Process shall be documented and approved by customer • Customer approval of all non-conformity dispositions • Formal FRB Process • *Reference Appendix C1: Failure Review Board* • *Reference Appendix B3: Hardware Quality Assurance* • *Reference Appendix B4: Software Assurance*	• Formal MRB Process shall be documented • Non-conformances shall be documented and dispositioned by engineering with independent reviewers auditing process • Limited customer participation • Squawk logs (excel) may be used to document rework, scrap and standard repair dispositions • Tailored FRB process to meet the program requirements • *Reference Appendix C1: Failure Review Board* • *Reference Appendix B3: Hardware Quality Assurance* • *Reference Appendix B4: Software Assurance*	• Non-conformances shall be documented on squawk logs (excel) and dispositioned by engineering with independent reviewers auditing process • MRB process may replace a formal FRB process • *Reference Appendix C1: Failure Review Board* • *Reference Appendix B3: Hardware Quality Assurance* • *Reference Appendix B4: Software Assurance*

A8-4 Summary of Risk Classes

Class A. Class A is a high-priority, minimum practical-risk effort. Key characteristics for IT&E include:

- Integration steps and records that are independently verified with photo documentation where applicable
- GSE HW and SW that is treated as flight
- Full Verification and Validation (V&V) on models used to sell-off system requirements
- Full Test Like You Fly Compliance
- Customer and contractor independent reviewer engagement down to subsystem levels and IRRs
- All telemetry and data bases are verified and configuration controlled
- Formal MRB/FRB with customer approval of non-conformances
- Customer attends and approves TRRs and BOCs, independent (customer and/or contractor) review of test set-ups, data analysis, and test execution
- Customer reviews and approves all test plans, procedures, and test reports

Class B. Class B is a high-priority, low-risk effort with cost saving compromises made primarily in areas other than design and construction. Key characteristics for IT&E, which differ from Class A include:

- Customer attends TRRs and BOCs, independent (customer and/or contractor) survey of test set-ups, data analysis, and test execution
- GSE simulators may not have full engineering unit fidelity
- System test may use high fidelity simulators/emulators
- TRRs and BOCs are informal with limited customer participation
- May employ protoqualification of flight units
- SW standards may be tailored
- Subsystem and unit tests may have durations, number of cycles, and margin requirements tailored for program risk posture

Class C. Class C is a moderate risk effort that is economically reflyable or repeatable. Key characteristics for IT&E include:

- Full quality sign off, little independent customer or contractor review
- GSE follows contractor best practices
- System and subsystem interfaces may be sold off against GSE simulators
- No formal qualification plan, tailored protoqualification may be employed
- SW follows contractors best practices
- Tailored subsystem and unit test programs
- Limited DITL test, system test performed at launch site possibly enabled by RF GSE
- GSE SW is validated and version controlled
- Tailored FRB process, non-conformances signed off by QA with independent reviewers auditing, limited customer participation

Class D. Class D is defined as a higher-risk, minimum-cost effort. Key characteristics for IT&E include:

- Integration uses contractor best practices
- GSE HW and SW comply with standards for flight HW safety
- SW follows contractors best practices
- No formal qualification testing
- Limited if any system level or end-to-end testing
- LV compatibility testing validates LV interfaces
- MRB may replace formal FRB process
- Independent reviewers audits process and mission critical activities consistent with program risk posture
- Customer reviews plans, procedures, and reports and interacts at established program reporting milestones

A8-5 Effectiveness TIPS (Lessons Learned)

- A comprehensive test program with emphasis on resolving issues at the lowest level of integration reduces total system cost by minimizing schedule delays.
- Software should be given full consideration in TLYF constraints as small apparently inconsequential changes in SW late in I&T flow have resulted in significant impacts.
- GSE is part of the integration and test flow and while it does not have the same reliability requirements, its readiness at each phase is equally important and so should be included in the appropriate reviews including GSW SW versions and calibrations.
- Sell-off reviews are important milestones that validate readiness by demonstrating completion (and compliance) of specific products called out in the entrance and exit criteria. Sufficient schedule should be provisioned to ensure that reviews can be performed to include comment disposition prior to the milestone.
- Model verification and validation should be started early in program life cycle so that deficiencies in available data can be addressed in program planning.
- Determining root cause is essential in resolving integration and test issues such that they do not re-occur or are repeated elsewhere in the system.
- Integration requires an effective MRB and FRB set of processes with customer and independent reviewers engaged so that issues are resolved expeditiously.

A8-6 References

1. Aerospace Report TOR-2011(8591)-5, *Acquisition Risk Planning and Tailoring Guidelines for National Security Space Vehicles*, September 13, 2010.
2. Aerospace Report TOR-2006(8546)-4591, *Space Vehicle Test and Evaluation Handbook*, 6 November 2006.
3. SMC Standard SMC-S-016, TR-2004(8583)-1 REV. A (MIL-STD-1540E), *Test Requirements for Launch, Upper Stage and Space Vehicles*, 6 September 2006.
4. MIL-HDBK-340A (USAF), Military Handbook, *Test Requirements for Launch, Upper-stage, and Space Vehicles*, 1 April 1999.
5. Aerospace Report ATR-2009(9369)-1, *Critical Clearances in Space Vehicles*, 31 October, 2008.
6. Aerospace Report TOR-2009(8591)-12, *Suggested Checklist to Improve Test Performance in the System Test Equipment Area*, 21 May 2009.

7. Aerospace Report TOR-2009(8591)-15, *Space Vehicle Checklist for Assuring Adherence to "Test-Like-You-Fly" Principles*, 30 June 2009.
8. Aerospace Report TOR-2005 (8583)–1 Rev A (MIL-STD-1541A), *EMC Requirements for Space Systems*, January 2008.
9. GSFC-STD-700 (NASA document), *General Environmental Verification Specification*, April 2005.
10. Aerospace Report TOR-2011(8591)-5, *Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles*, September 13, 2010.
11. Aerospace Report TOR- 2009 (8591)-15, *Space Vehicle Checklist for Assuring Adherence to "Test-Like-You-Fly" Principles*, June 2009.

Appendix B: Risk, Oversight and Assurance Processes

Appendix B captures the Risk Classes Matrixes for the Risk, Oversight and Assurance MA framework processes for mission success. Processes include:

- B1: Risk Assessment and Management
- B2: Independent Reviews
- B3: Hardware Quality Assurance
- B4: Software Assurance
- B5: Supplier Quality Assurance

Appendix B1: Risk Assessment and Management

Dr. Rudy Emrick, Orbital Sciences Corporation
Matthew Fahl, Harris
Ed Hume, Johns Hopkins APL
Gail Johnson-Roth, The Aerospace Corporation

B1-1 Introduction

This chapter provides guidelines for applying effective risk management to space systems. The methods of risk planning, assessment, handling, monitoring, and documentation may be tailored to meet the needs of the program; however, a risk management process is either required or recommended for any space system development activity and should be addressed over the lifecycle of the program. The process may be applied to all space flight systems to include deliverable payloads, space vehicles, or other associated products. Formal risk management requirements may be dictated by the acquisition authority per the contract or developed in accordance with the contractor's best practices commensurate with the level of risk associated with the specific mission. Ultimately, the developer is responsible for implementing an organized, systematic decision-making process for risk management to increase the likelihood of achieving mission success.

B1-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which risk profile can be developed and are not intended as general standalone industry standard definitions.

Risk Planning. Risk planning consists of developing a Risk Management Plan (RMP). The RMP should define the responsibilities of key personnel, provide definitions of risk related terms, identify the resources to conduct risk management, describe the procedures of the risk management process, integrate supplier risk management, and establish required risk management training.

Risk Assessment. The risk assessment process begins with risk identification and risk analysis. Identified risks are ranked and a point of contract (risk owner) is identified. Finally, the risk database is updated to reflect all current information and status. The risk assessment process should cover technical, programmatic risks, and subcontractor risks. Risk assessment may be performed by independent assessment teams.

Risk Handling. Mitigation plans should include specific tasks to drive down the probability and/or impact of the risk together with a defined schedule. The plan must be reviewed and approved by the Risk Management Board (RMB) and the risk database updated.

Risk Monitoring. As the mitigation plan is executed, the RMB will track status and evaluate progress, updating the risk database to show the current status. A successfully completed mitigation plan may lead to risk retirement.

Documentation. Risk documentation includes the RMP, the risk database, RMB minutes, periodic risk status reports, design review risk status, and statements of risk cost impact.

Definition of other common risk terms:

Acceptable Risk. The risk that is understood and agreed to by the program/project, governing PMC, mission directorate, and other customer(s) such that no further specific mitigating action is required. (Some mitigating actions might have already occurred.)

Acceptance of Risk. Decision to cope with consequences, should a risk scenario materialize. A risk can be accepted when its magnitude is less than a given threshold, defined in the risk management policy. In the context of risk management, acceptance can mean that even though a risk is not eliminated, its existence and magnitude are acknowledged and tolerated.

Approval. Authorization by a required management official to proceed with a proposed course of action. Approvals must be documented.

Independent Assessment Team. A group or team that is not under the supervision, direction, advocacy, or control of the program (or its chain of command) that provides and independent assessment.

Individual Risk. Risk is identified, assessed, and mitigated as distinct risk items in a project.

Margin. The allowances carried in budget, projected schedules, and technical performance parameters (e.g., weight, power, or memory) to account for uncertainties and risks. Margin allocations are baselined in the formulation process, based on assessments of risks, and are typically consumed as the program/project proceeds through the life cycle.

Overall Risk. Risk resulting from the assessment of the combination of individual risks and their impact on each other, in the context of the whole project. Overall risk can be expressed as a combination of qualitative and quantitative assessment.

Primary Risks. Those undesirable events having both high probability and high impact/severity.

Residual Risk. Risk remaining after implementation of risk reduction measures.

Resolved Risk. Risk that has been rendered acceptable.

Risk. The combination of the probability that a program or project will experience an undesired event and the consequences, impact, or severity of the undesired event, were it to occur. The undesired event may come from technical or programmatic sources (e.g., a cost overrun, schedule slippage, safety mishap, health problem, malicious activities, environmental impact, failure to achieve a needed scientific or technological objective, or success criterion). Both the probability and consequences may have associated uncertainties.

Risk Cost Estimate. The dollar cost to the program, should a specific risk not be mitigated and the risk event is realized. Cost is estimated for labor, material and Other Direct Costs (ODC).

Risk Database. The program risk list, assessments, mitigation plans, and all information relating to specific risks are kept in a risk database under configuration control by the risk manager. Configuration control includes restricted access to the program and risk managers, and date stamps on all risk list and mitigation reports.

Risk Level or Index. Score used to measure the magnitude of the risk; it is a combination of the likelihood of occurrence and the severity of consequence, where scores are used to measure likelihood and severity.

Risk Management Board (RMB). The RMB is a collection of key team members whose responsibility is to provide oversight and approval for the risk management plan (RMP). Results from risk assessment and handling are reviewed and approved by the RMB. The RMB reviews changes in risk status, progress of mitigation plans, and over-sees integration of the overall RMP within the program. The RMB, typically chaired by the risk manager, usually consists of the IPT leads for Mission Systems, Spacecraft Systems, External Interfaces, Subcontracts, Mission Assurance, Integrated Master Schedule and Earned Value Management, Program Manager, and Program Chief Engineer. Depending on the mission class, there may also be customer representation on the board. The RMB meeting frequency is determined by the risk manager and is based upon program need and class of mission. In addition to the regular board members, various program team members are invited to the meetings as needed to supply information on specific risks.

Risk Management Process (RMP). RMP is defined by the four distinct phases of risk planning, assessment (identification and analysis), handling, and monitoring. The process goal is to identify program risks and mitigate medium and high risks to a low or non-existent level of impact.

Risk Management. An organized, systematic decision-making process that efficiently identifies, analyzes, plans, tracks, controls, communicates, and documents risk, and establishes mitigation approaches and plans to increase the likelihood of achieving program/project goals.

Risk Monitoring. The risk monitoring process tracks and evaluates the effectiveness of respective risk mitigation plan steps, and insures exit criteria are met while monitoring for contingency triggers.

Risk Point of Contact. Conducts risk analysis, handling, and monitoring duties for assigned risks. Ensures accurate and on-schedule execution of assigned risk mitigation plans and status updates per selected monitoring method. Monitors the results of the risk mitigation actions, ensuring exit criteria are met and evaluates contingency triggers. Updates program risk assessments as needed, and reports status and cost impact to risk manager. Participates on RMB as an invitee when needed.

Risk Ranking. A rank ordering of program risks, typically ordered from the highest to the lowest overall assessed risk. The risk ranking will change over the course of the program as risk areas are mitigated and new risks are identified and assessed.

Risk Reduction. Implementation of measures that leads to reduction of the likelihood or severity of risk. Preventive measures aim at eliminating the cause of a problem situation, and mitigation measures aim at preventing the propagation of the cause of the consequence or reducing the severity of the consequence or the likelihood of the occurrence.

Risk Scenario. Sequence or combination of events leading from the initial cause to the unwanted consequence**.** The cause can be a single event or something activating a dormant problem.

Risk Trend. Evolution of risks throughout the life cycle of a project.

RMB Chair. Sometime also called the risk manager, as appointed by the program manager, documents program risks identified by IPTs, as well as management, administration, and the customer (when appropriate) in a risk database. As these risks are analyzed and mitigated, the risk manager summarizes status for reviews by the RMB.

Unresolved Risk. Risk for which risk reduction attempts are not feasible, cannot be verified, or have proven unsuccessful: a risk remaining unacceptable.

B1-3 Matrix - Risk Assessment and Management

- Captured on following pages

	Class A	Class B	Class C	Class D
Risk Planning	• Required (by contract) • Jointly developed: Plan is typically developed by the contractor and is submitted to the customer for approval • Customer has voting representatives on program level RMB, which is chaired by the contractor • Customer develops and maintains separate risk management process to allow for comprehensive assessment and handling of program risk • Risk process applies to sub-contractors and critical vendors • Risk management training required for all personnel - customer and contractor teams • Risks reported at monthly management meetings and major milestone reviews	• Required (by contract) • Plan is typically developed by contractor submitted for: • Approval by customer (CP) • Review by customer (FFP) • Risk Management Process controlled by formal RMB • Risk process applies to sub-contractors and critical vendors • Risk management training required for all personnel-customer and contractor teams • Risks reported at monthly management meetings and major milestone reviews	• Required (by contract) • Developed by contractor and reviewed by customer • Typically follows the contractor's internal risk management processes with tailoring as needed • Risk Management Process executed by contractor, controlled by program manager, Systems Engineering, or Mission Assurance • Risk process identifies risks at sub contractors and critical suppliers • Training as required in accordance with contractor best practices • Risks reported at customer meetings and major milestone reviews	• Recommended (not required by contract) • Developed by contractor • Typically follows the contractor's internal risk management processes or a tailored subset • If no formal processes are followed, expect informal risk management to mitigate risks • Note "informal" marked by lack of objective evidence supporting processes, but can present risk material at major reviews • Risk Management Process executed by the contractor controlled by program manager, Systems Engineering, or Mission Assurance • Training as required in accordance with contractor/developer best practices. • Reported at customer meetings and major milestone reviews

	Class A	Class B	Class C	Class D
Risk Assessment	• Required (by contract) • Performed contractor, customer provides inputs and initiates new risks through participation in contractor led RMB • Customer has voting representatives on program level RMB that is chaired by the contractor • Independent assessment typical/required for all critical mission impacting risks and prior to major milestone reviews; may submit risks through the appropriate customer or contractor process • Customer develops and maintains separate risk assessment • All personnel are responsible for identifying risks; construct includes many layers from working groups and integrated product teams. Once risk is verified, it is elevated for consideration at RMB • Includes management of residual (accepted) risk, which is expected to be minimal	• Required (by contract) • Contractor develops and maintains risk assessment which is submitted for: • Approval by customer (CP), Review by customer (FFP) • Customer may maintain separate risk assessment • Independent assessment is typical/required for all critical mission impacting risks and may submit risks through the appropriate customer or contractor process • All personnel are responsible for identifying risks; construct includes many layers of risk identification from working groups, subcontractors, and integrated product teams • Process includes verification of risk. Once risk is verified, it is elevated for consideration at RMB	• Required (by contract) • Developed by contractor and reviewed by customer • Typically a mission class with higher residual risk. It is required that the contractor address risk balance and residual risk in their plans to keep the appropriate balance between cost and risk • Independent assessment may be employed to assess critical mission impacting risks; may submit risks through the contractor process or present directly to the customer • All personnel are responsible for identifying risks and elevating in accordance with established process	• Recommended (not required by contract) • Developed and approved by contractor • Typically the mission class with highest residual risk. It is recommended that the contractor address risk balance and residual risk in their plans keep the appropriate balance between cost and risk • Independent assessments may be deployed for critical risk assessment and mission-impacting risks • All personnel are responsible for identifying risks and elevating in accordance with established process

	Class A	Class B	Class C	Class D
Risk Handling	• Required (by contract) • Performed by contractor, customer provides inputs through active participation in the Program RMB • Customer representation and voting rights on program level RMB • Customer develops and maintains separate risk handling summary • Standardized reporting format dictated by customer to be consistent with acquiring agency/policy • All risks documented/ retained even if risk is accepted and/or retired • Mitigation plans incorporated into baseline with IMS task and budget. May incorporate existing tasks • Mitigation activities worked at lowest level appropriate; progress reported at RMB	• Required (by contract) • Typically performed by contractor, submitted for: • Approval by customer (CP), Review by customer (FFP) Standardized reporting format dictated by customer to be consistent with acquiring agency policy • All risks documented/ retained even if risk is accepted and/or retired • Mitigation plans incorporated into baseline with IMS task and budget or tracked separately by the RMB. May incorporate existing tasks • Mitigation activities worked at lowest level appropriate; progress reported at RMB	• Required (by contract) • Performed by contractor and reviewed by customer • Mitigation plans tracked separate from baseline. May incorporate existing tasks. Risk-specific budget may or may not be allocated in baseline	• Recommended (not required by contract) • Performance and approved by contractor • Mitigation plans tracked separate from baseline. May incorporate existing tasks. Risk-specific budget may or may not be allocated in baseline

	Class A	Class B	Class C	Class D
Risk Monitoring	• Required (by contract) • Contractor risk manager or risk owners presents monitoring status to RMB • Customer representation and voting rights on program level RMB • RMB evaluates status and reacts to developments or low mitigation performance • Customer maintains separate risk monitoring summary • Common access server and standardized format usually dictated by contract for visibility by all personnel- both contractor and customer teams	• Required (by contract) • Typically developed by contractor, submitted for: • Approval by customer (CP), Review by customer (FFP) • Common access server and standardized format usually dictated by contract for visibility by all personnel – both contractor and customer teams	• Required • Led and handled by contractor • Status reported to customer • Common access server may be required by customer • Recommended for visibility by all personnel	• Recommended (not required by contract) • At the discretion of and handled by contractor
Documentation	• Required (by contract) • Jointly developed: Typically generated by contractor and approved by customer • Customer representation and voting rights on program level RMB • Customer develops and maintains separate risk summary • Documentation required to be available to customer team on common access server	• Required (by contract) • Typically developed by contractor by internal processes, submitted for: • Approval by customer (CP), Review by customer (FFP) • Documentation may be required to be available to customer team on common access server	• Required • Developed by contractor per internal processes • Typically delivered to customer as information only	• Recommended/not required • At the discretion of and handled by contractor per internal processes

	Class A	Class B	Class C	Class D
Risk Planning	• Required (by contract) • Jointly developed: Plan is typically developed by contractor and submitted to customer for approval • Customer has voting representatives on program level RMB which is chaired by the contractor • Customer develops and maintains separate risk management process to allow for comprehensive assessment and handling of program risk • Risk process applies to sub-contractors and critical vendors • Risk management training required for all personnel – customer and contractor teams • Risks reported at monthly management meetings and major milestone reviews	• Required (by contract) • Plan is typically developed by contractor submitted for: • Approval by customer (CP) • Review by customer (FFP) • Risk Management Process controlled by formal RMB • Risk process applies to sub-contractors and critical vendors • Risk management training required for all personnel – customer and contractor teams • Risks reported at monthly management meetings and major milestone reviews	• Required (by contract) • Developed by contractor and reviewed by customer • Typically follows the contractor's internal risk management processes with tailoring as needed • Risk Management Process executed by contractor, controlled by program manager, Systems Engineering, or Mission Assurance • Risk process identifies risks at sub contractor's and critical suppliers • Training as required in accordance with contractor best practices • Risks reported at customer meetings and major milestone reviews	• Recommended (not required by contract) • Developed by contractor • Typically follows the contractor's internal risk management processes or a tailored subset • If no formal processes followed, expect informal risk management to mitigate risks • Note "informal" marked by lack of objective evidence supporting processes, but can present risk material at major reviews • Risk Management Process executed by the contractor controlled by program manager, Systems Engineering, or Mission Assurance • Training as required in accordance with contractor/ developer best practices • Risks reported at customer meetings and major milestone reviews

	Class A	Class B	Class C	Class D
Risk Assessment	• Required (by contract) • Performed by contractor, customer provides inputs and initiates new risks through participation in contractor led RMB • Customer has voting representatives on program level RMB that is chaired by the contractor • Independent assessment typical/required for all critical mission impacting risks and prior to major milestone reviews; may submit risks through the appropriate customer or contractor process • Customer develops and maintains separate risk assessment • All personnel are responsible for identifying risks; construct includes many layers from working groups and integrated product teams. Once risk is verified, it is elevated for consideration at RMB • Includes management of residual (accepted) risk which is expected to be minimal	• Required (by contract) • Contractor develops and maintains risk assessment which is submitted for: • Approval by customer (CP) • Review by customer (FFP) • Customer may maintain separate risk assessment • Independent assessment is typical/required for all critical mission impacting risks and may submit risks through the appropriate customer or contractor process • All personnel are responsible for identifying risks; construct includes many layers of risk identification from working groups, subcontractors, and integrated product teams • Process includes verification of risk; once risk is verified it is elevated for consideration at RMB	• Required (by contract) • Developed by contractor and reviewed by customer • Typically a mission class with high residual risk. It is required that the contractor address risk balance and residual risk in their plans to keep the appropriate balance between cost and risk • Independent assessment may be employed to assess critical mission impacting risks; may submit risks through the contractor process or present directly to the customer • All personnel are responsible for identifying risks and elevating in accordance with established process	• Recommended (not required by contract) • Developed and approved by contractor • Typically the mission class with highest residual risk. It is recommended that the contractor address risk balance and residual risk in their plans keep the appropriate balance between cost and risk • Independent assessments may be deployed for critical risk assessment and mission-impacting risks • All personnel are responsible for identifying risks and elevating in accordance with established process

	Class A	Class B	Class C	Class D
Risk Handling	• Required (by contract) • Performed by contractor, customer provides inputs through active participation in the program RMB • Customer representation and voting rights on program level RMB • Customer develops and maintains separate risk handling summary • Standardized reporting format dictated by customer to be consistent with acquiring agency/policy • All risks documented/ retained even if risk is accepted and/or retired • Mitigation plans incorporated into baseline with IMS task and budget. May incorporate existing tasks • Mitigation activities worked at lowest level appropriate; progress reported at RMB	• Required (by contract) • Typically performed by contractor, submitted for: • Approval by customer (CP) • Review by customer (FFP) • Standardized reporting format dictated by customer to be consistent with acquiring agency/policy • All risks documented/ retained even if risk is accepted and/or retired • Mitigation plans incorporated into baseline with IMS task and budget or tracked separately by the RMB. May incorporate existing tasks • Mitigation activities worked at lowest level appropriate; progress reported at RMB	• Required (by contract) • Performed by contractor and reviewed by customer • Mitigation plans tracked separate from baseline. May incorporate existing tasks. Risk specific budget may or may not be allocated in baseline	• Recommended (not required by contract) • Performed and approved by contractor • Mitigation plans tracked separate from baseline. May incorporate existing tasks. Risk specific budget may or may not be allocated in baseline

	Class A	Class B	Class C	Class D
Risk Monitoring	• Required (by contract) • Contractor risk manager or risk owners presents monitoring status to RMB • Customer representation and voting rights on program level RMB • RMB evaluates status and reacts to developments or low mitigation performance • Customer maintains separate risk monitoring summary • Common access server and standardized format usually dictated by contract for visibility by all personnel – both contractor and customer teams	• Required (by contract) • Typically developed by contractor, submitted for: • Approval by customer (CP) • Review by customer (FFP) • Common access server and standardized format usually dictated by contract for visibility by all personnel – both contractor and customer teams	• Required • Led and handled by contractor • Status reported to customer • Common access server may be required by customer. Recommended for visibility by all personnel	• Recommended (not required by contract) • At the discretion of and handled by contractor
Documentation	• Required (by contract) • Jointly developed: Typically generated by contractor and approved by customer • Customer representation and voting rights on program level RMB • Customer develops and maintains separate risk summary • Documentation required to be available by customer team on common access server	• Required (by contract) • Typically developed by contractor by internal processes, submitted for: • Approval by customer (CP) • Review by customer (FFP) • Documentation may be required to be available by customer team on common access server	• Required • Developed by contractor per internal processes • Typically delivered to customer as information only	• Recommended/not required • At the discretion of and handled by contractor per internal processes

B1-4 Summary of Risk Classes

Class A. System requirements dictate the implementation of a formal risk management (RM) program plan; the plan a joint effort between the contractor and the government being a formal contract deliverable developed by the contractor with government review and approval. The formal RM plan deliverable includes descriptions of the following: validated/approved process and process documentation, formal risk management boards, integration of risk management process/databases throughout the sub-contractor/supplier chain with full government participation. Both technical and programmatic risks are addressed and handled by the plan. Since a Class A program will have minimal practical risk, the plan will also fully address how residual risk will be managed and kept to a minimum. The RM plan will also clearly define how the contractor's RM process will interact with the government program office risk management process.

The government program office maintains a separate risk management process that identifies risks and handling plans as well as documents risk acceptance and evidences. The government program office should also create a separate risk management plan. The program risk management board, (RMB), is chaired by the contractor with the government in attendance and actively participating. The government may also create and chair their own RMB, (with active contractor participation), that operates in parallel with the contractor RMB. The use of dual RMBs and risk processes insures that program risk is analyzed from all possible perspectives enabling the most comprehensive approach. The full program (government and contractor) is responsible for identifying potential risks on the program and submitting appropriate potential risk information like cause, likelihood, and impact.

Typically, risks will be actively identified by the full program, (contractor, sub-contractors and government). The responsible organization will capture identified risks in accordance with the approved risk management plan. These will typically flow to the program RMB and may have one or more intermediate steps prior to reaching the program RMB. Government identified risks will typically flow through the government-led RMB where it will decide which risks will be elevated to the program RMB. Once risks are elevated to the program RMB for deliberation, allocation of resources and assigned responsibility for handling of a risk are defined and captured. Key to RM success is the identification of resources required to implement the developed risk-handling options. Risks affecting mission success and their mitigation plans must be approved by the government.

Class B. The risk planning process is a joint effort between the contractor and the government. The risk plan must be approved by the government for Cost Plus projects, and at a minimum, reviewed by the government for Fixed Price projects. Risks are identified by all stakeholders. Risk review boards are conducted at various levels within the project, and all risks affecting mission success must be approved by the government. Risk handling plans are jointly developed by the contractor and the government, with the contractor taking the lead, and must be approved by the customer. The government will monitor the status of the risk handling through reports from the contractor. The customer is responsible for maintaining the risk management tool, which will document the risks, the associated handling plans, and progress against those plans.

Class C. Space programs make compromises between minimum risk and minimum cost and may be driven toward the minimum acquisition cost. Class C programs cover medium priority space programs usually where re-flight or repeat flight is cost effective as a routine backup in the event of an in-flight failure. Class C program schedules are usually shorter than Class A and B programs and are managed by the contractor. Because Class C space programs run a greater risk of failure than Class B, contingency backup launch plans should be a factor in deciding to implement a Class C program, even though the contingency plans might not be a part of the initial acquisition contract. Due to safety risks and other mission impacts, Class C payloads that have a medium or high risk of

not achieving mission success may be considered unsuitable for launch on a crewed vehicle, unless they are secondary payloads making use of available launch capacity that would otherwise go unused.

Class C programs have several characteristics that use acceptance of higher risk to control mission costs. For Class C programs, success-critical single failure points are acceptable and there is limited availability of component flight spares. In many cases, the design margins are very small or can be zero. Only limited compliance to technical standards is required and testing is typically limited to functional, environmental screening, safety, and interface compatibility tests.

Class D. Class D programs are inherently higher risk relative to the other mission classes. There are usually no formal risk management requirements by the acquisition agent, though it is highly recommended that the contractor utilize their own risk management process for the program. Typically a contractor's internal processes will require each program to implement their own internally defined risk management process without a contract requirement. All portions of the risk process are developed and approved by the contractor. The risk management processes and activities are applied where practical with cost being a more significant factor compared to other mission classes.

The contractor is encouraged to use traditional risk management processes to identify critical components/subsystems (i.e., transponder) identified relative to critical or mission–essential services (i.e., Command and Data Handling [C&DH]). The exception is required risk reporting associated with safety and compatibility requirements imposed by launch vehicle provider, ride sharers, and Interface Compatibility Documents; Any and all risks to meeting those requirements are reported at the pre-ship review required by Launch Vehicle (LV) integrator where mass, safety, compatibility, cleanliness are verified.

Risk mitigation within Class D programs are more likely than other classes to utilize lower cost risk mitigation approaches like operational workarounds. The operational workarounds are more likely than other missions' classes to degrade mission functionality or capability in order to avoid a mission end.

Residual risk is typically the highest on Class D relative to the other classes. Risk balance should be a part of the contractor's risk management for the program in order to keep the appropriate balance between the overall program cost and risk.

B1-5 Effectiveness TIPS (Lessons Learned)

- Risks identified in the proposal phase should be documented and tracked throughout the life cycle of the program.
- Be aware of company management principles related to "cost" of risk; particularly important for FFP contracts where CFO is held accountable annually.
- Risks should be identified and tracked using a common access server for visibly by all program personnel, to include contractor and government teams.

B1-6 References

1. ISO-17666, *Space Systems Risk Management*.
2. NPR 8000.4A, *Agency Risk Management Procedural Requirements*.
3. NPR 8705.5A, *Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects*.
4. NPR 8705.4, *Risk Classification for NASA Payloads*.

5. Aerospace Report TOR-2005 (8583)-4019, *Risk Management Plan Guide for Space Acquisition Programs*.
6. *DAU Program Managers Tool Kit*, Fifteenth Edition (Ver 1.0), April 2009, http://www.dau.mil/pubs/misc/toolkit.asp.
7. *A Guide to the Project Management Body of Knowledge*, Project Management Institute, 1996.

Appendix B2: Independent Reviews

Edward Hume. Johns Hopkins University Applied Physics Laboratory
Jean-Claude Inauen, Northrop Grumman
Mark Oja, ATK
Brian Shaw, The Aerospace Corporation

B2-1 Introduction

Independent reviews are a major part of the risk management of a program. As the risk management plan for a program is developed, the amount of acceptable risk is established by program requirements, budget, and schedule constraints. The use of multiple levels of reviews can serve to retire risk in an appropriate fashion, develop alternatives to minimize risk impact to the program, and to document the residual risk that needs to be carried forward in the program.

The independent review process is a systematic evaluation of a product or system by a team of qualified personnel that examines the acceptance of the product or system for its intended use and identifies discrepancies based on program specifications and standards. Many independent reviews occur at defined points set in program schedule, and if warranted, a technical/programmatic review can be convened as needed to address problems or issues discovered as a program is being executed. Program reviews are used to assess the maturity of the development effort, determine readiness to conduct acceptance testing, and determine whether the investment should be made to continue into production (i.e., become operational). Program reviews may also provide recommendations of alternatives and examination of various alternatives to meet mission needs or to correct for a discovered deficiency. Many of the Gated Reviews and Programmatic Technical reviews feed into other reviews later on in the program life cycle. Many of these reviews work off of each other and it is critical to make sure that all actions from a previous review are closed prior to moving into the next one. An independent review team may also be reviewing the results of previous reviews to help validate their current review; i.e., the sub-system IDRs all flow into a PDR, which then flows into the CDR.

While not an exhaustive list of reviews, the tables below are divided into three major types of reviews. The first part covers the major reviews that are held over the life cycle of a space system development program and follows the defined program gates, as identified in Aerospace Report TOR-2009(8545)-8545, Guidelines for Space Systems Critical Gated Events, reference Figure B-1. The second section has reviews that are driven by the program and are used to address specific technical issues or sub-system design. The third category is government-driven reviews. These occur at the specific request of the government or designated third party organization and are usually held in addition to the other types of reviews. For each of the reviews listed in the following tables, a determination of the applicability was made for each of the mission risk Classes (A-D). For each combination of review and mission class, three major considerations are given: the requirement for the review, the level of independence required, and the level of completeness that is required. Details and definitions of each of these three items are given below. The independent review table forms a matrix that may be used to determine the recommended level of independent review a particular mission class would require.

For example, the recommendation for a requirements review is that it should be required (by contract) for Classes A and B, is recommended for Class C and is optional for Class D. For Class C missions the requirements review, if done, should be at least internally independent with members of the review panel having no connection to the program in the performing organization. It also suggests the review be done to the Class C completeness recommendation described below. The independent

review matrix was developed to allow for program tailoring to meet mission needs and risk acceptance while still supporting budget and schedule constraints.

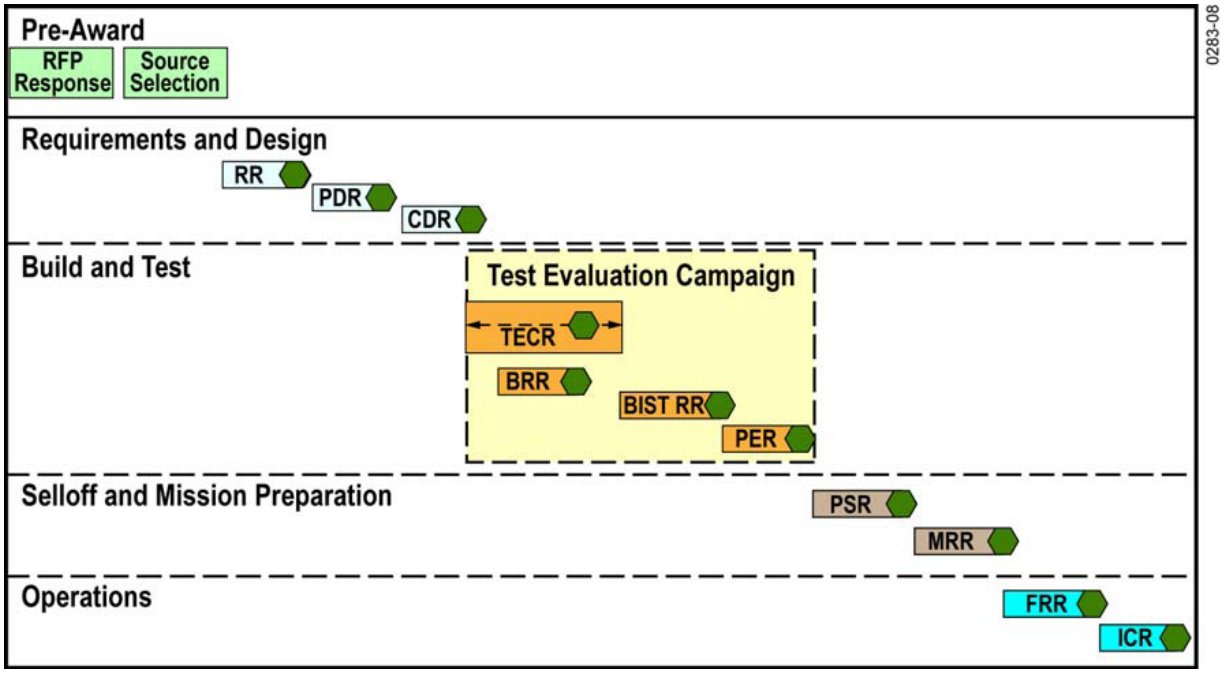


Figure B-1. Gated reviews timeline.

B2-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which risk profile can be developed and are not intended as general standalone industry standard definitions.

B2-2.1 Reviews

Requirements Review (RR)[NSS]/System Definition Review (SDR) [NASA]. For the purposes of this document, the activities and objective typically associated with the SRR, the SDR, and the system functional review have been combined into the RR. The RR demonstrates that the proposed system architecture/design, system requirements, and flow-down to all functional elements meet the system mission objectives.

Preliminary Design Review (PDR). The PDR evaluates the contractor's technical adequacy, progress, and risk resolution for the selected design-to approach for all Configuration Items (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.

Critical Design Review (CDR)

- The CDR is a multi-disciplined product and process assessment to determine whether the system design is sufficiently mature to proceed to build approval and full-scale manufacturing. It is a critical, cooperative examination of the design solution, its details and

its suitability for production and use. The CDR shall be conducted for each CI when detail design is essentially complete.

Build Readiness Review (BRR)[NSS]/Production Readiness Review (PRR) [NASA]

- The objectives for BRR/PRR are two-fold. The first objective is to ensure that the manufacturing process can produce the items and meet the specified design requirements – including any late changes due to immature design iterations, as well as incorporation of producibility changes. The second objective is to ensure that the design translates into a reliable, durable, accurately manufactured item using manufacturing processes that are highly repeatable and error-free.

Test Evaluation Campaign Review (TECR) [NSS]/Test Readiness Review (TRR) [NASA]

- The TECR is a gated event that is held to verify that the program is prepared to proceed with formal testing. The review verifies that the planned testing meets all assigned verification or validation requirements, and that the test documentation, test hardware, test software, and test resources are ready for test operations.

Assembly/Integration Readiness Review (BIST RR)

- This review is conducted before initial system test or BIST, and after successful completion of all items enumerated in the TCER. It ascertains the readiness of the integrated space vehicle (spacecraft and payload) to undergo system-level testing.

Pre-Environmental Review (PER)

- The PER is performed before the start of formal environmental testing of the integrated space vehicle to demonstrate that the vehicle has sufficient margin to permit environmental testing.

Pre-Ship Review (PSR)

- The program conducts hardware PSR to assure that flight hardware and components, software, GSE, 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.

Mission Readiness Review (MRR)

- The MRR is the final formal review prior to committing to erect the launch vehicle and mate the space vehicle. At this point, the space vehicle and all major segments of the launch vehicle have completed their respective PSR gate processes.

Flight Readiness Review (FRR)

- Collectively, the FRR evaluates the system's space flight worthiness, including the readiness of launch and support facilities (ground systems), Range and orbital operations, the readiness and training of the operating personnel, and the safety of the integrated system. For this document, the FRR's main objective is to ascertain the space vehicle's flight worthiness.

Initial Checkout Review (ICR)

- The ICR is carried out after the satellite completes its preliminary early orbit test to accomplish the following: establish command and control, characterize and test systems, achieve nominal orbit and configuration, establish operational database and documentation, perform authorization to link operational constellation, perform operational trial, perform anomaly detection and resolution, and perform operational utility evaluation(s).

Technical Issue Review

- Technical reviews are used to evaluate the status of the technical progress and are supported by other equivalent technical discipline activities, including safety reviews. Many ad hoc technical issue reviews occur as a result of a failure or unexplained anomaly.

Peer Reviews

- Peer review is a generic term for the process of self-regulation by evaluation involving qualified individuals within the relevant field. Peer reviews are employed to maintain standards, improve performance, and provide credibility. Peer reviews are particularly useful in the hardware and software design process as a means for gathering constructive feedback on a design without the overhead associated with preparing a formal review package.

Internal Design Reviews (IDR)

- Working reviews with in-depth assessments of sub-systems. These IDRs precede and support the System-level PDR and CDR. IDRs may be held as “dry runs” in preparation for the system level reviews. IDRs should be identified on the program master schedule to facilitate compliance tracking.

Independent Technology Readiness Assessment

- Conducted upon request of DOD Deputy Director of Research and Engineering (DDR&E), this review assesses key technology areas when readiness risk concerns are sufficient to have been elevated to the DDR&E level. These reviews are generally staffed by specially appointed high-level experts, much in the style of the USAF Scientific Advisory Board.

Information Technology and Joint Interoperability Test Certification

- This independent assessment/certification validates accomplishment of the key performance parameter for interoperability and net-readiness.

Independent Baseline Review (IBR)

- Periodic independent review of the program baseline, both programmatic and technical to ensure proper baseline control and to ensure effective trades between technical baseline and programmatic issues.

Space Flight Worthiness Certification

- This assessment/certification is required to validate compliance with the Space Flight Worthiness criteria and is part of the input to the APR and government FRR/MRR.

Government Independent Review (government IRRT)

- Independent assessment of technical aspects of programs (conducted by The Aerospace Corporation for SMC launches; government is the lead for space vehicle) between CDR and factory system tests. Results are presented to system program director and mission director. Normally conducted 18 months prior to launch for new systems, and three to nine months prior to launch for existing systems.

Post Flight Review (SMC/CC; POE-Space)

- Captures lessons-learned from space missions and implements those lessons prior to next flight. Covers all aspects of the mission, including space segment and supporting ground segment. Typically happens about 60 days after launch and after early-orbit operations are completed.

Aerospace President's Review

- Assesses all aspects of the launch vehicle, spacecraft, and launch base to provide The Aerospace Corporation CEO/President the information necessary to make proper go/no-go decision for an SMC launch. Typically occurs one week prior to FRR.
- Aerospace President's Consent to Ship Review (APCR). This review is focused on the space vehicle and will be linked with the decision of consent to ship. Delta APRs may be conducted for other milestones such as consent to fuel, or the mission or flight readiness reviews. During APCR, an interim status on the launch vehicle and ground system is presented as applicable.

B2-2.2 Independent Review Requirements

Required

- Independent Review is formally part of the program per contract requirement following an internal/external standard and should include the independence and completeness levels as indicated in the matrix above

Recommended

- Independent Review is highly suggested following an internal/external standard that can be tailored from the suggested levels of independence and completeness as indicated in the matrix above,

Discretionary

- Independent Review execution will be at the discretion of the program office, company and/or customer following a defined process, which, at a minimum, should include the independence and completeness levels as indicated in the matrix.

B2-2.3 Levels of Independence

Externally Independent

- An organization or personnel that are technically, managerially, and financially independent of the contractor.

Internally Independent

- An organization or personnel within the contracting organization that are technically, managerially, and financially independent of the program.

Developer Independent (Peer Review)

- An organization or personnel within the program that is technically independent of the review subject developer.

B2-2.4 Level of Completeness of an Independent Review

Class A. The IR team will review all of the exit criteria as described in TOR-2009(8583)-8545 "Guidelines for Space Systems Critical Gated Events." Interviews will be conducted with all key product/subject leads. Class A requires physical IR review of objective evidence to prove completion of review criteria (100% review of critical items for both completeness and quality). No tailoring of IR criteria is permitted. Class A must be fully compliant to company processes with all technical disciplines represented as part of the review panels. The IR Team may be a permanent presence (resident) during program execution

Class B. (Same as Class A) The IR team will review all of the exit criteria as described in TOR-2009(8583)-8545 "Guidelines for Space Systems Critical Gated Events," For less critical reviews the areas/disciplines reviewed may be reduced through agreement between the IRT leadership and the Program Office. Interviews conducted with all key product/subject leads. Class B requires physical IR review of objective evidence to prove completion of review criteria (100% review of critical items for both completeness and quality). Limited tailoring of IR criteria is permitted to allow review of summary analysis of evidence in non-critical areas. Class B requires full compliance to company processes with all technical disciplines represented as part of the review panels. The IR team members may be continuous throughout the program life.

Note: The difference between Class A and Class B may be the level of independence of the review team and the limited tailoring of criteria or type of allowable evidence

Class C. Only core mission assurance topics described in the exit criteria will be reviewed. The IR team works with program management to determine and review the high and medium-high risk/mission critical areas. Interviews conducted with key players in the high and medium risk/mission critical areas (PM, lead systems engineer). Class C requires the program to prove completion by review of examples, 100% physical review not required. For example, PSR, review a sample of completed FRB packages and use the word of interviewees to verify all others were completed to the same quality. Tailoring of IR criteria is permitted to allow review of summary analysis of evidence is acceptable through agreement between the IRT leadership and the program office. IRs are typically performed on an Ad Hoc basis.

Class D. Reviews performed only on core mission assurance required by launch safety or potentially impacting any higher-class payload (if rideshare configuration) described in the exit criteria. The IR team will work with program management will determine and review the high risk/mission critical areas. Interviews conducted on a subset of the key players in the high risk/mission critical areas (PM, lead systems engineer). Work is performed through a scaled down checklist pre-defined by agreement between the IRT leadership and the program. Class D uses word of mouth or sampling as objective evidence, not necessarily requiring physical review of objective evidence. Significant tailoring of IR criteria is acceptable through agreement between the IRT leadership and the program which may not

include subject matter experts from all technical disciplines (focus is on critical requirements of the mission). The IR is mostly considered an Ad Hoc function.

B2-3 Matrix - Independent Reviews

Gated Review	Class A[1]	Class B[2]	Class C[3]	Class D[4]
Requirements Review (RR)	• Required • Externally Independent	• Required • Externally Independent	• Recommended • Internally Independent	• Discretionary • Developer Independent
Preliminary Design Review (PDR)	• Required • Externally Independent	• Required • Externally Independent	• Recommended • Developer Independent	• Discretionary • Developer Independent
Critical Design Review (CDR)	• Required • Externally Independent	• Required • Externally Independent	• Required • Internally Independent	• Recommended • Internally Independent
Build Readiness Review (BRR)	• Required • Internally Independent	• Required • Internally Independent	• Recommended • Developer Independent	• Discretionary • Developer Independent
Test and Evaluation Campaign Review (TECR)	• Required • Internally Independent	• Required • Internally Independent	• Discretionary • Developer Independent	• Discretionary • Developer Independent
Baseline Integrated System Test Readiness Review (BIST RR)	• Required • Internally Independent	• Required • Internally Independent	• Discretionary • Developer Independent	• Discretionary • Developer Independent
Pre-Environmental Review (PER)	• Required • Internally Independent	• Required • Internally Independent	• Discretionary • Developer Independent	• Discretionary • Developer Independent
Pre-Ship Review (PSR)	• Required • Externally Independent	• Required • Externally Independent	• Recommended • (Discretionary) • Internally (Externally) Independent	• Recommended • Internally Independent

1 – Class A Completeness **2** – Class B Completeness **3** – Class C Completeness **4** – Class D Completeness

Gated Review	Class A1	Class B2	Class C3	Class D4
Mission Readiness Review (MRR)	• Required • Externally Independent	• Required • Externally Independent	• Required • Externally Independent	• Recommended • Internally Independent
Flight Readiness Review (FRR)	• Required • Externally Independent	• Required • Externally Independent	• Recommended • Developer Independent	• Discretionary • Developer Independent
Initial Checkout Review (ICR)	• Required • Internally Independent	• Required • Internally Independent	• Discretionary • Developer Independent	• Discretionary • Developer Independent
Technical Issue Review	• Required • Internally Independent	• Required • Internally Independent	• Recommended • Developer Independent	• Discretionary • Developer Independent
Peer Reviews of Sub-Assemblies	• Recommended • Internally Independent	• Recommended • Internally Independent	• Discretionary • Internally Independent	• Discretionary • Developer Independent
Internal Design Reviews (IDR)	• Recommended • Internally Independent	• Recommended • Internally Independent	• Discretionary • Developer Independent	• Discretionary • Developer Independent
Executive Risk Review	• Recommended • Internally Independent	• Recommended • Internally Independent	• Discretionary • Developer Independent	• Discretionary • Developer Independent
Independent Technology Readiness Assessment	• If required by DDRE • Externally Independent	• If required by DDRE • Externally Independent	• If required by DDRE • Externally Independent	• If required by DDRE • Externally Independent
Information Technology and Joint Interoperability Test Certification	• Required • Externally Independent	• Required • Externally Independent	• Required • Externally Independent	• Discretionary • Externally Independent
Independent Baseline Review (IBR)	• Required • Externally Independent	• Recommended • Externally Independent	• Recommended • Externally Independent	• Discretionary • Externally Independent

1 – Class A Completeness **2** – Class B Completeness **3** – Class C Completeness **4** – Class D Completeness

Government Driven Reviews	Class A[1]	Class B[2]	Class C[3]	Class D[4]
Space Flight Worthiness Certification	• Required • Externally Independent	• Required • Externally Independent	• Recommended • Externally Independent	• Discretionary • Externally Independent
Government Independent Review (government IRRT)	• Required • Externally Independent	• Required • Externally Independent	• Recommended • Externally Independent	• Discretionary • Externally Independent
Post Flight Review (SMC/CC; PEO-Space)	• Required • Externally Independent	• Required • Externally Independent	• Recommended • Externally Independent	• Discretionary • Developer Independent
Aerospace President's Review	• Required • Externally Independent	• Required • Externally Independent	• Recommended • Externally Independent	• Discretionary • Developer Independent
Interim Design Review	• Recommended • Internally Independent	• Recommended • Internally Independent	• Discretionary • Developer Independent	• Discretionary • Developer Independent

1 – Class A Completeness **2** – Class B Completeness **3** – Class C Completeness **4** – Class D Completeness

B2-4 Summary of Risk Classes

Class A Reviews. Extremely risk-averse Class A programs typical hold numerous programmatic and technical reviews during the life cycle of a program required by the contract and would require a waiver to not execute these reviews. These reviews include technical experts from within the company and the customer community. These reviews fully comply with defined industry and company standards for such reviews to satisfy documented entrance and exit criteria. Issues are systematically tracked to closure. Little deviation from company or industry standards is incorporated in the review process. The process is typically defined by contract and incorporated into the program plan.

Class B Reviews. Risk-adverse Class B programs are very similar to Class A programs regarding program and technical reviews. Reviews typically include technical experts from within the company and the customer's community. These reviews fully comply with defined industry standards for such reviews to satisfy predefined entrance and exit criteria. Issues are systematically tracked to closure. Little deviation from company or industry standards is incorporated in the review process. The process is typically defined by contract and incorporated early into the program plan.

Class C Reviews. Risk-accepting Class C program reviews may not include the full suite of reviews. Early in the program-definition phase less critical reviews may be dropped to trade off cost containment against the risk of late issue identification. Planned reviews are typically documented in the program plan. Key reviews such as SRR, CDR, MRR and HARs are generally held in compliance with company or industry standards. Review material generally follows standards for such reviews with some modification allowed to manage review cost. Items eliminated are perceived low risk to the program.

Class D Reviews. High-risk tolerant programs typically hold only at a few key milestone reviews during the lifecycle of the program. Key milestones include requirements definition, design determination, prefabrication, and post hardware fabrication prior to transfer to the customer. These reviews typically include a few key internal to the company folks who have similar project experience. External customer may be invited but are not required to participate. Review material is less formal in content and is often less than fully compliant with industry standards for such reviews. Early planning for all programs including Class D programs should include a discussion regarding the reviews to be held during the program lifecycle.

Example Criteria for Discretionary Review Events

Below are some examples of when a program might consider holding an Independent Review that has been identified as "DISCRETIONARY" in the matrixes.

Requirements Review

- Requirements not fully understood.
- Development is allocated to multiple Principal Investigators or development organizations for integration prior to flight.

Preliminary Design Review

- Design options exist but do not present a logical "best choice" of approaches.
- Development is allocated to multiple Principal Investigators or development organizations for integration prior to flight.

Build Readiness Review

- Manufacturing is allocated to organization not sufficiently controlled by the Principal Investigator or to multiple organizations for integration prior to flight.
- Using an outside vendor who requires a BRR as part of their internal requirements/processes.

Test and Evaluation Campaign Review

- Testing exceeds Class D criteria of exposing primary payloads, launch vehicle or shared bus to risks such as contamination or undesirable electromagnetic emissions.
- Testing distributed between multiple Principal Investigators or development organizations.

Baseline Integrated Test Readiness Review

- (See Test and Evaluation Campaign Review.)

Pre-environmental Review

- Formal or extensive environmental testing is to be conducted.
- The environmental testing requirements are far more extensive than typical program of this particular mission class.

Flight Readiness Review

- Development organization, sponsor, or mission leadership determines that formal assurance of flight readiness is warranted due to known/anticipated risks, un-validated application of lessons-learned resolutions, or mission priority requires achievement of mission success.

Initial Checkout Review

- (See Flight Readiness Review.)

Technical Issue Review

- Known or anticipated technical issues put the development or mission success at risk.
- Unexplained failures or anomalies present themselves during normal program execution.

Peer Reviews of Sub-Assemblies

- Considerable amount of design/development work is being conducted at the sub-system level.

Internal Design Reviews

- Considerable amount of design/development work is being conducted at the sub-system level.

Executive Risk Review

- (See Flight Readiness Review.)

Information Technology and Joint Interoperability Test Certification

- Required by contract/customer.
- Interfaces exist with government IT infrastructure or operational assets.

Independent Baseline Review

- Required by contract/customer.
- (See Flight Readiness Review and Technical Issue Review.)

Government Independent Review

- Required by contract/customer.
- (See Flight Readiness Review and Technical Issue Review.)

Space Flight Worthiness Certification

- Required by contract/customer.
- (See Flight Readiness Review and Technical Issue Review.)

Post Flight Review

- Anomaly or failure occurred that impacted launch vehicle and/or primary mission.

Aerospace President's Review

- Required by contract/customer.
- (See Flight Readiness Review and Technical Issue Review.)

Interim Design Review

- Required by contract/customer.
- (See Requirements Review and Preliminary Design Review.)

B2-5 Effectiveness TIPS (Lessons Learned)

- Prior to any review it is beneficial for a program to perform an internal readiness review to verify that they are ready to start and complete the review at hand.
- Prior to conducting an independent review the development of all entrance and exit criteria for each review to determine Mission Class A-D specific entrance and exit criteria would be useful to set the expectations for that risk profiles review.
- Define required program Independent Reviews during program kick-off defined in Program Management Plan.
- Define Independent Review criteria early on to define company policies.

B2-6 References

1. Aerospace Report TOR-2007 (8583)-6414, Vol 1, Rev 1, Technical Review and Audits for Systems, Equipment, and Computer Software.
2. Aerospace Report TOR-2009 (8583)-8545, *Guidelines for Space Systems Critical Gated Events*, 9 May 2008.

3. National Security Space Acquisition Policy 03-01, *Guidance for DOD Space Acquisition Process*, 12 December 2005.
4. SMCI 63-1201, *Assurance of Operational Safety, Suitability and Effectiveness for Space and Missile Systems*, 21 May 2001.
5. SMCI 63-1202, *Space Flight Worthiness*, 2004.
6. SMCI 63-1203, *Independent Readiness Review Team*, 2004.
7. SMCI 63-1204, *SMC Readiness Review Process*, 2004.
8. NASA NPR 8705.6A, *Safety and Mission Assurance Audits, Reviews, and Assessments*, 9 April, 2009.
9. Draft Air Force Space Command Unit Self-Inspection Checklist 90-11. Systems Engineering Management. 2010.
10. Nelson, N. and Arnold, G., *Independent Review Process – Overview and Best Practices*, Aerospace Report ATR-2009 (9369)-20, 20 August 2009.
11. SMC-G-002, *Space Flight Worthiness Criteria*, 29 May 2009.
12. SMC-G-003, *Independent Review Team*, 29 May 2009.
13. NASA NPR 7123.1A, *NASA Systems Engineering Processes and Requirements*, 26 March, 2007.

Appendix B3: Hardware Quality Assurance

Mark Oja, ATK
Matthew Fahl, Harris Corp

B3-1 Introduction

This chapter provides guidelines for applying effective hardware quality management to space systems. The methods of quality assurance may be tailored to meet the needs of the program; however, a quality management process is required at some level for any space system development activity and should be addressed over the lifecycle of the program. The process may be applied to all space flight systems, to include deliverable payloads, space vehicles, or other associated products. Formal quality management requirements are typically dictated by the acquisition authority per the contract or developed in accordance to the contractor's best practices commensurate with the level of risk associated with the specific mission. Ultimately, the developer is responsible for implementing an organized Hardware Quality Program (HQP) commensurate with the risk profile of the program and mission.

The primary objective to the contractors' HQP is to ensure that hardware built for the program meets contractual requirements and specified design documentation. The contractor's HQP is defined by the contract and the program quality plan. A good HQP includes program quality that assures the contractor's quality program meets customer contract quality requirements; quality engineering provides oversight to all contractor activities that may have impact on product quality throughout the life cycle of the contract, including procurement of items for the contract and hardware quality assurance performs specific validation of hardware features or characteristics.

A good HQP:

- 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 and evaluation of potential problems, which could result in less than satisfactory performance.
- Provides for timely and effective corrective action to less than desired performance of produces, processes or services.

B3-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which risk profile can be developed and are not intended as general standalone industry standard definitions.

Design Review. The contractor's quality organization shall participate in key program reviews to evaluate the effectiveness in implementing specific contractual QA requirements that ensure compliance with the overall contract technical requirements. These reviews include System Requirements Reviews (SRRs), Design Reviews, Producibility Reviews, Manufacturing Reviews, Test Readiness Reviews (TRRs), Material Review Boards (MRBs), Failure Review Boards (FRBs),

Pedigree Reviews, Hardware Acceptance Reviews (HARs), and Independent Readiness Reviews (IRRs).

Purchasing Documents. Validate that there is a process that assures the adequacy of the specified requirements in the purchase documentation prior to transmittal to the supplier/vendor. This includes a review to assure that the purchase is being directed to an approved supplier/vendor. Approved suppliers/vendors have been periodically reviewed/evaluated for their ability to supply products in accordance with the organization's requirements.

Records Management. Control 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.

Identification and Traceability. Maintain the identification and traceability of the product throughout product realization. Identification of the configuration of the product is maintained in order to identify any differences between the actual configuration and agreed configuration. Media used as an acceptance authority (e.g., stamps, electronic signatures, passwords) shall be controlled by established and documented controls.

Continual Quality Improvement. Maintenance of a continual quality improvement system that addresses both product and process improvement and incorporates a system for review and incorporation of lessons learned into the Quality Management System.

Audits. Conduct audit activities related to manufacturing and testing of the product, including first article inspection, functional configuration audits (FCAs), physical configuration audits (PCAs), quality system audits (QSAs), and contractor and subcontractor/supplier audits.

Process Verification. Quality Assurance (QA) evaluates engineering systems for adherence to command media.

Metrology of Measurement and Test Equipment. Determine the monitoring and measurement to be undertaken and the measuring devices needed to provide evidence of conformity of the product. The contractor maintains a register of these monitoring and measuring devices and defines the process employed for their calibration and recall to calibration. Records include data from the calibration process and acceptance requirements.

Personnel Qualification and Certification for Key Manufacturing Processes. 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. This includes establishment of workmanship standards and certifying assemblers and inspectors for special processes such as soldering and welding.

Non-conformance Handling. The contractor shall establish and maintain a system which shall identify, segregate (or control if segregation is not practical), and properly dispose of nonconforming material and shall ensure that cost-effective, positive corrective action is taken to prevent, minimize, or eliminate non-conformances.

Product Verification. Compliance, identify and control nonconforming products to prevent unintended use or delivery. A documented procedure is required for controls, responsibilities, and authorities for dealing with nonconforming product.

Inspection and Documentation of the First Article Built (FAI). The organization shall use a representative item from the first production run of a new part or assembly to verify that the production processes, production documentation, and tooling are capable of producing parts and assemblies that meet requirements. This process shall be repeated when changes occur that invalidate the original results (e.g., engineering changes, manufacturing process changes, tooling changes).

Product Preservation. Preservation of the product includes identification, handling, packaging, storage, and protection.

Environmental Controls. The organization shall provide buildings, workspace, process-equipment, and support services needed to achieve product quality.

B3-3 Matrix - Hardware Quality Assurance

Hardware Quality Tasks	Class A	Class B	Class C	Class D
Design Review	• Design reviews shall include participation of Quality Assurance, including review of changes thereafter • QA shall assure sufficient detail to control and manufacture the items, appropriate workmanship standards are defined, and features are verifiable. Customer including DCMA is often included in these reviews	• Similar to Class A with less potential of full customer involvement	• Similar to Class B with little or no customer involvement in the review process	• An independent design review shall be performed by an independent organization, which may or may not be QA and could be the customer. Procured items should be reviewed by QA
Purchasing Documents	• The contractor's supplier quality assurance program shall provide for a review of purchase documents to assure applicable quality requirements are included or referenced in the documentation for compliance by the supplier. Quality requirements for Class A would fully conform to the highest-level company standard including the use of certified suppliers. Customer review of procured documentation is often performed	• Similar to Class A with less potential of full customer involvement	• Similar to Classes A and B with more tailoring of quality requirements levied on the supplier. Quality requirements for Class C: procured items shall be limited to those most significant to the products application. Customer is not normally involved	• Same as Class C
Records Management	• Quality Assurance shall maintain a system for the collection and analysis of quality records resulting from the procurement, manufacturing, inspection, test and use of articles and materials	• Same as Class A	• Same as Class A	• Same as Class A

Hardware Quality Tasks	Class A	Class B	Class C	Class D
Identification and Traceability	• Quality shall assure a system for identification, traceability and control of parts, materials, and assemblies from acquisition through manufacturing, assembly and delivery. The system shall provide for identification and suitable marking of hardware	• Same as Class A	• The depth of traceability may not be as deep or specific. Example: Part number and lot date code may be maintained at an assembly level	• Similar to Class C
Continual Quality Improvement	• Quality shall assure a system is maintained to work toward continual improvement of quality and productivity through the initiation and monitoring of a Quality Improvement Program. This program shall seek both opportunities to improve products/process and incorporate remedies to realized problems	• Same as Class A	• Quality shall assure a systematic improvement is incorporated to remedy realized problems	• Similar to Class C
Audits	• Quality Assurance participates or sponsors audits of personnel, procedures, and operations to assure compliance with outlined requirement. Customers often perform independent audits and/or participate in the contractor's audits. Audits are also performed at subcontractor and sub-tier supplier	• Same as Class A	• Audits on Class C program are less frequent and of less depth, focusing on key elements or problematic areas within the program. Customer generally not involved	• N/A

Hardware Quality Tasks	Class A	Class B	Class C	Class D
Process verification; capability, readiness, Process FMEAs, certification and compliance	• Quality Assurance shall participate in the process to certify the qualification of the machines, equipment, and procedures used in complex, critical operations. Validation prior to production shall include measurements made on the first article produced to a given design. For new or unique processes, conduct process FMEAs. Customers may be included in the verification process	• Same as Class A	• Same as Class A minus customer involvement and process FMEAs normally not performed	• N/A
Metrology of measurement and test equipment	• Quality Assurance shall assure gauges and other measuring and testing devices used in the acceptance of design feature are calibrated against certified measurement standards	• Same as Class A	• Same as Class A	• Same as Class A
Personnel qualification and certification for key manufacturing processes	• Quality shall oversee a training program that assures adequate skill levels, including formal and on-the-job training. Quality shall assure sufficient formal training to ensure proficiency of persons performing complex or critical operations	• Same as Class A	• Same as Class A	• Per company policy

Hardware Quality Tasks	Class A	Class B	Class C	Class D
Non-conformance handling including corrective action	• Quality shall assure deviation from design and/or contact requirements are documented and evaluated for impact on product performance. The quality organization shall manage and participate in a system for determination of action necessary to eliminate reoccurrence of nonconformance. Customers are fully involved in the nonconformance handling	• Same as Class A	• Similar to Class A minus customer involvement. Customers are notified of significant nonconformance handling. MRB could be delegated to contractors or subcontractors	• Informal log (Squawk Log) to record non-conformance resolution. Reviewed according to company best practice
Product verification; compliance, inspection verifications necessary to ensure product compliance including: - Receiving, in-process, and final inspections of products - Verification of test set-ups and test output data - Verification of critical features and key characteristics - Material receiving and dimensional/ attribute verification	• Products and services produced by outside sources for incorporation in the contract end item shall be subject to quality inspection at the time of receipt. For less critical items in lieu of receiving inspection, quality may use objective quality evidence submitted by the supplier • Beginning at the start of assembly and at progressive levels of assembly and test, the contractor's quality organization shall verify that the contract, drawing, and specification requirements have been met and materials procured or produced. Quality is involved in the management and validation of critical and key characteristics or features • Customer involvement often included validation of key characteristics upon fabrication	• Same as Class A	• Hardware quality performs less or minimal validation of production upon receipt and/or in process. These validations are delegated to the manufacture or internal performing organization. Minimal or no customer involvement in product verification	• Hardware quality organization performs less or minimal validation of production upon receipt and/or in process. These validations are often delegated to the manufacture or other internal performing organizations. No customer involvement in product verification. If the contracts have no QA the customer may provide compliance verifications

Hardware Quality Tasks	Class A	Class B	Class C	Class D
Inspection and documentation of the first article built (FAI)	• Quality shall manage and participate in a 100% verification of design features on the FAI article built. Customer and contractor review evidence of 100% via reports generated from first article inspections	• Same as Class A	• Quality shall manage and participate in a verification of key design features on the first article built. Customers are not normally involved in FAI	• N/A
Product Preservation; - Packaging, handling, preservation, transportation and shipping of products (pre-ship through receipt at customer) - Cleanliness, contamination and corrosion control	• Quality shall assure protection of deliverable hardware at all stages of manufacture and test through delivery. Quality shall assure procedures and processes are employed to: a. Keep deliverable items clean and in a proper environment b. Handled such that the possibility of damage during manufacture or test is minimized c. Packaged to prevent damage during transit d. Transported in such a manner as to minimize any risk to the deliverable item(s) • Customer participates in oversight for key component	• Same as Class A	• Same as Class A with minimal or no customer oversight	• Same as Class A with the potential of delegation of this task to the fabricating organization of another independent organization. Customers are generally not involved

Hardware Quality Tasks	Class A	Class B	Class C	Class D
Environment Controls - Cleanliness and environmental controls including temperature, ESD, and humidity as necessary to assure hardware performance - Audit controls and compliance	• Quality Assurance shall review and participate in identifying controls for cleanliness, contamination, ESD, and corrosion control. Quality assurance on a regular basis shall participle in audits to assure these controls are maintained as required	• Same as Class A	• Identification of environmental controls is delegated to the performing organization for Classes C and D programs	• Same as Class C

B3-4 Summary of Risk Classes

Class A. For high risk programs (Class A), the HQP will take all actions to ensure that hardware built for the program meets contractual requirements and ensure mission success. All AS9100 and ISO9000 processes will be followed with few, if any, tailoring.

Class B. The only difference in the HQP between a Class A and Class B program is less potential for full customer involvement in areas such as Design Reviews and Purchasing Documents.

Class C. The reduced risk of Class C programs allows for a HQP with much less customer involvement in the execution of the program. Quality Assurance processes may also be more relaxed in the areas of purchasing, parts and materials identification and traceability, product verification, and environmental controls. Audits are less frequent and less in-depth. Quality's involvement in First Article Inspections is focused on only key design features rather than 100% verification.

Class D. Class D programs allow even more tailoring of the HQP. Audits are not typically performed. Nonconformance handling and product preservation may be done by an organization other than QA. The customer may provide compliance verification in the absence of a contractor QA organization. There is typically no FAI.

B3-5 Effectiveness TIPS (Lessons Learned)

- Early definition of all planned HQA activities in the Program Plan or Quality Plan helps ensure a common understanding for effective HQA execution.
- Judicious identification of critical features during the design phase helps focus HQA activities and resources.
- First article inspection and rigorous process control is effective in managing multi-unit fabrication programs.
- Early evaluation of the strengths and weaknesses with the planned supply base to focus supplied items management.
- Program involvement in the readiness for planned audits helps ensure effective execution.
- Utilization of process FMEAs for new, complex, or critical processes is prudent.

B3-6 References

1. ISO 9001:2008, *Quality Management Systems, Requirements*, 11 November 2008.
2. SAE AS9100C, *Quality Management Systems - Requirements for Aviation, Space and Defense Organizations*, 15 January 2009.
3. Aerospace Report TOR-2005(8583)-3859, *Quality Assurance Requirements for Space and Launch Vehicles*, 1 December 2005.
4. SMC Standard SMC-S-003A, *Quality Systems*.
5. SAE AS9102, *Aerospace First Article Inspection Requirement*.
6. Aerospace Report TOR-2007(8546)-6018 Rev A, *Mission Assurance Guide*, 1 July 2007.

Appendix B4: Software Assurance

David Pinkley, Ball Aerospace

B4-1 Introduction

The primary objective of the software assurance process is to ensure delivered software meets all functional, performance, and interface requirements, including the required dependability, reliability, maintainability, availability, security, supportability, and usability requirements. The Software Quality Assurance (SQA) process provides objective participation in all phases for all types of software development and purchase efforts. The SQA participation includes provided process and product oversight for:

- All software that resides on hardware
- All software that directly controls or processes data for hardware
- All software that resides on ground support equipment and is used to test hardware
- All developmental software used to test and evaluate delivered software
- All safety-critical software and all program subcontracts and customer-furnished software in support of any of the previously listed items.

The SQA maintains oversight to ensure that the software architecture is sufficiently extensible and computer resources have sufficient margins.

Software is defined as computer instructions or data, programs, routines, databases, firmware, and symbolic languages that control the functioning of hardware and direct its operations. Software is anything that can be stored or executed electronically. Firmware is defined as software contained in read only memory (ROM), erasable programmable read-only memory (EPROM), field-programmable gate arrays (FPGAs), flash memory, or other programmable devices.

Software assurance can be further subdivided into software reliability and software safety. The software reliability function assures built-in reliability and maturity for the software for its intended application and measures reliability growth. Built-in reliability is ensured through the Capability Mature Model Integrated software development (CMMI-DEV) process, which emphasizes detailed peer reviews, thorough testing, and defect management.

Software safety function identifies critical software elements that represent hazards to both the mission systems and development personnel. Once safety-critical software functions are identified by performing appropriate hazard analyses, design safety features and procedures are implemented to mitigate risk to acceptable levels. Software safety typically includes:

- Identification of safety critical functions
- Identification of system and subsystem hazards/risks
- Determines the effects of risk occurrence
- Analyze the risk to determine all contribution factors
- Categorize the risk in terms of severity and likelihood of occurrence
- Determine mitigation requirements for each hazard commensurate with the identified risks
- Determine test requirements to prove the successful implementation
- Determine and communicate any residual safety risks
- Determine software product is sufficiently robust to gracefully degrade in the presence of anomalous events.

This appendix provides guidelines for applying effective software assurance to space systems. The methods of software assurance may be tailored to meet the needs of the program; however, a software assurance process is either required or recommended for any space system development activity to ensure clarification of users' needs. The process may be applied to all space flight systems; to include deliverable payloads, space vehicles, or other associated products. Formal software assurance may be dictated by the acquisition authority per the contract or developed in accordance with the contractor's best practices commensurate with the level of risk associated with the specific mission. Ultimately, the developer is responsible for implementing an organized, systematic software assurance process to increase the likelihood of achieving mission success.

B4-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which risk profile can be developed and are not intended as general standalone industry standard definitions.

Software Quality Assurance. Software quality is exhibited when the delivered software meets all functional, performance, and interface requirements including required dependability, reliability, maintainability, availability, security, supportability, and usability. Software Quality Assurance follows a set of established processes and procedures to independently determine the quality of the software products and processes developed and used on a program through objective participation in all phases of the software development process.

Support to Program Reviews. Participation in formal and informal program level reviews (SRR, PDR, CDR, TRR, etc.) reporting on compliance to standards and conventions, timely action item disposition and tracking, adequate technical review, and on-going requirements traceability. SQA reviews and audits the product review process to ensure reviews occur in compliance to standards, plans, and requirements.

Audit/Review Software/Firmware Reviews. SQA reviews program software development plan (SDP) for completeness of activities required for the risk posture of the program. In addition an on-going assessment is made of the SDP to ensure software development engineering compliance including software processes releases for program applicability.

Peer Review and Audit Software/Firmware Requirements. SQA in concert with development team ensuring the design and development of all customer technical, operational, quality, reliability, and safety requirements in a consistent, reliable, and repeatable manner. Software Requirements Specifications (SRSs) are reviewed to ensure requirements are unambiguous, consistent, traceable, implementable, testable, and adequately reviewed.

Audit and Review Software/Firmware Trade Studies. SQA review of trade studies to ensure they follow a documented and consistent process for completeness, consistency, reliability, and safety.

Software Safety Assurance. Integrated into the overall SQA process and jointly performed with system safety. Evaluate software safety critical functions or data via a safety analysis performed by the system safety. Software safety identifies safety requirements and performs analysis to assure safety-critical events are identified, evaluated, and eliminated or reduced to an acceptable level. All changes to requirements, design, and code are evaluated for safety implications and to maintain an acceptable risk level.

Audit and Review Software Design. Participation in development level peer design reviews to ensure compliance to approved requirements and standards. Periodic audits of the design are conducted ensuring product compliance, quality, reliability, and safety. The review criteria includes designing in of all relevant requirements, compliance with any approved top level designs, adequate review by technical personnel, control of the product under review, handling of action items, verifying the implement ability of the design, verifying the testability of the design, verifying the results and concurrence of any lower level prototype testing, ensuring the design includes adequate fault handling, and verifying review of all relevant reliability and safety design issues.

Code Review and Audit. Participation in formal and informal (peer) code review to ensure compliance to approved design and standards. Periodic audits of the code are conducted to ensure product compliance, quality, reliability, and safety. The review criteria includes implementation of all relevant requirements, compliance with design, adequate review by technical personnel, control of the product under review, handling of action items, verifying the testability of the implementation, verifying the results and concurrence of lower level testing, verifying appropriate low level path and stress testing, ensuring adequate fault handling, and verifying review of all relevant reliability and safety issues.

Audit and Participate in SCCB. The SQA serves as an active member of the Software Change Control Board (SCCB) verifying the need for requested changes and ensures proper review and approval of the changes. SQA ensures correct implementation of the changes and testing results including appropriate management support and resource allocation for each requested change.

Audit and Review Software/Firmware Test Plans and Procedures. Audit and review of test plans, test procedures, test results, and run test records, and by witnessing/monitoring baseline builds and tests. Review criteria includes, the repeatability of tests, applicability of tests, concurrence of test results and execution, verification of requirements, requirements traceability, stress and path testing, adequate pass/fail criteria, and complete and accurate documentation of all test activities and environments.

Software Reliability Assessment. Software reliability growth is measured through the lifecycle using statistical measures to assess the current state of the software and to recommend adjustments to the development and test programs to ensure reliability growth. Software reliability requirements will address the level and manner of fault and failure detection, isolation, fault tolerance, and recovery expected to occur within the software as part of the overall system.

Software/Firmware Test Configuration Audit. The SQA conducts software/firmware test configuration audits in support of final product build and delivery. The audit includes review of test facility, configuration drawings, setup procedures, test facility certification/test records, and review of applicable build documentation. Review criteria includes, the repeatability of the test configuration, applicability of test facility certification, concurrence of certification results, verification of test facility requirements, adequate certification pass/fail criteria, and adequate documentation of all certification activities.

Software/Firmware Test Support. The SQA support of software product through assessments, review of documentation including test plans, test procedures, test results, and “as-run” test records and by witnessing or monitoring of tests. Review criteria includes, the repeatability of tests, applicability of tests, concurrence of test results, verification of requirements, requirements traceability, stress and path testing, adequate pass/fail criteria, and complete and accurate documentation of all test activities.

Software Supplier Support. The SQA activities include supplier-related activities to mitigate program risk and help ensure delivered products meet the needs of the program. The program SQE reviews software supplier documentation from the SOW, requirements allocated to the subcontract, and any supplier produced software documentation required by the contract. This review may include Software Development Plans, requirement documents, design documents, code, test plans, procedures, and test results. Program SQA participates in periodic performance monitoring, acceptance of subcontracted product, performs audits and reviews, and support for test, build, and delivery by witnessing and monitoring tests.

B4-3 Matrix - Software Assurance

SA Requirement	Class A	Class B	Class C	Class D
Plan and Establish SQA on the Program	• CSCI software/firmware process instantiation; S/W process tailoring • Contractor performs ongoing independent evaluations of software development process, products, work product, and software services • Documents evaluation records and resolutions for all software QA activities and non-compliance issues are made available to customer for review	• CSCI software/firmware process instantiation; S/W process tailoring • Same as Class A	• CSCI software/firmware process instantiation; S/W process tailoring • Contractor determines the applicability of software quality assurance product and process evaluations	• CSCI software/firmware process instantiation; S/W process tailoring • Up to developer. Typically not performed
Program Reviews	• Milestone review participation. Joint (customer, contractor) technical reviews performed for evolving software products and project status. Joint management reviews conducted for approvals, commitments, and to resolve management issues. Risk mitigation strategies are presented at reviews	• Milestone review participation • Customer and contractor participation is dependent on specific program needs, and customer leadership	• Milestone review participation • Less formal technical interchange meetings with customer may be conducted for the review of design and test	• Milestone review participation. Technical interchange meetings not required, informal status may be reported
Audit and Review and Software/Firmware Plans	• S/W Process Tailoring Request (PTR) Rigor implementation audits; S/W CM baseline/Audits	• S/W Process Tailoring Request (PTR) Rigor implementation audits; S/W CM baseline/Audits	• S/W Process Tailoring Request (PTR) Rigor implementation audits; S/W CM baseline/Audits	• S/W Process Tailoring Request (PTR) Rigor implementation audits; S/W CM baseline/Audits

SA Requirement	Class A	Class B	Class C	Class D
Peer Review and Audit Software/Firmware Requirements	• Requirement Compliance, SRS Review/Audit • Peer review prep, materials, reviews, follow-up and data analysis performed by contractor. Meeting records maintained with evaluations and resolutions documented. Status with metrics and corrective actions provided to customer for review	• Requirement Compliance, SRS Review/Audit • Same as Class A	• Contractor determines the applicability of peer reviews and product evaluations	• Contractor determines the applicability of peer reviews and product evaluations
Audit and Review Software/Firmware Trade Studies	• Software/Firmware Trade studies (***Likely***) quality, completeness, consistency, reliability, safety	• Software/Firmware Trade studies (***Potential***) quality, completeness, consistency, reliability, safety	• Software/Firmware Trade studies (***non-heritage deltas***) quality, completeness, consistency, reliability, safety	• Software/Firmware Trade studies (***unlikely***) quality, completeness, consistency, reliability, safety
Software Safety Assurance	• Software Safety completeness, correctness of execution and artifacts • Identification of all critical software hazards to the mission system and development personnel	• Software Safety completeness, correctness of execution and artifacts • Hazard assessment the same as Class A	• Software Safety (***heritage baselined***) completeness, correctness of execution and artifacts • Hazard assessment the same as Class A	• Software Safety • Hazard assessment the same as Class A to ensure no detrimental effects in ridesharing situation or to personnel
Audit and Review Software Design	• Peer Design Reviews for requirement and standard compliance (group/one-on-one) tailored per PTR	• Peer Design Reviews for requirement and standard compliance (group/one-on-one) tailored per PTR	• Peer Design Reviews for requirement and standard compliance (group/one-on-one) tailored per PTR	• Peer Design Reviews for requirement and standard compliance (group/one-on-one) tailored per PTR
Code Review and Audit	• Formal/Informal (peer) compliance to design and standards (Group, one-on-one) tailored per PTR	• Formal/Informal (peer) compliance to design and standards (Group, one-on-one) tailored per PTR	• Formal/Informal (peer) compliance to design and standards (Group, one-on-one) tailored per PTR	• Formal/Informal (peer) compliance to design and standards (Group, one-on-one) tailored per PTR
Audit and Participate in SCCB	• SCCB voting member; change need, proper review and approval, implementation, regression testing, documentation; Software baseline configuration audits	• SCCB voting member; change need, proper review and approval, implementation, regression testing, documentation; Software baseline configuration audits	• SCCB voting member; change need, proper review and approval, implementation, regression testing, documentation; Software baseline configuration audits	• SCCB voting member; change need, proper review and approval, implementation, regression testing, documentation; Software baseline configuration audits

SA Requirement	Class A	Class B	Class C	Class D
Audit and Review Software/Firmware Test Plans and Procedures	• Adequate control, review, and traceability, appropriate witnessing/monitoring tailored per PTR	• Adequate control, review, and traceability, appropriate witnessing/monitoring tailored per PTR	• Adequate control, review, and traceability, appropriate witnessing/monitoring tailored per PTR	• Adequate control, review, and traceability, appropriate witnessing/monitoring tailored per PTR
Conduct Software Reliability Assessment	• Planning: Emphasis on error prevention, fault detection, and removal, actions to increase reliability; Software Engineering defect classification process, SQA metric collection, and Reliability Engineering Statistical Analysis of Reliability with feedback for growth	• Planning: Emphasis on error prevention, fault detection, and removal, actions to increase reliability; Software Engineering defect classification process, SQA metric collection, and Reliability Engineering Statistical Analysis of Reliability with feedback for growth. ***(If required)***	• Focus is on maximizing reliability through the use of heritage software with controlled and gradual modifications	• Not Performed
Software/Firmware Test Configuration Audit	• Test Configuration Audits supporting final build and delivery	• Test Configuration Audits supporting final build and delivery	• Test Configuration Audits supporting final build and delivery	• Test Configuration Audits supporting final build and delivery
Software/Firmware Test Support	• Test support via plan, procedure, results, and "as-run" doc. And by witnessing/ monitoring tests as tailored by PTR - Class	• Test support via plan, procedure, results, and "as-run" doc. And by witnessing/ monitoring tests as tailored by PTR - Class	• Test support via plan, procedure, results, and "as-run" doc. And by witnessing/ monitoring tests as tailored by PTR - Class	• Test support via plan, procedure, results, and "as-run" doc. And by witnessing/monitoring tests as tailored by PTR - Class
Software Supplier Support	• Tailored by supplier contract and SOW, contractor manages all subcontractors providing software products or services in accordance with contract requirements flowed to suppliers • Subject to customer oversight and approval	• Tailored by supplier contract and SOW • Same as Class A	• Tailored by supplier contract and SOW. • Same as Class A except no customer oversight or approval	• Tailored by supplier contract and SOW • Not required

B4-4 Summary of Risk Classes

Class A. For Class A Space Systems the full software and firmware software quality assurance process is followed with independent assessments by both internal contactor and government software subject matter experts. Artifacts of all requirements, design, and code reviews are captured with actions formally worked to closure. A full software reliability program and software safety program are conducted. Software reliability will capture both process and product defect knowledge, performs statistical analysis of reliability growth, and provides feedback to software engineering to ensure continual growth. Software safety will work with system safety to develop a hazard analysis identifying safety critical software functions. Hazards will then be assessed against mission and personnel risk and mitigation plans formulated and executed. Software Quality will be a core member of SCCB ensuring the validity of software changes and the successful and timely closeout of those changes. Test support will include audits of configuration, and test witness. Software supplier support is a microcosm of the above process for internally developed software.

Class B. For Class B Space Systems the full software and firmware software quality assurance process is followed with independent assessments principally conducted by the contractor, and software audit process by the customer. Artifacts of core peer and independent reviews are captured with a closed loop action system. Software reliability is focused on product knowledge working to ensure that, as the development proceeds, software reliability growth is maintained. Software safety will identify and mitigate safety critical software hazards. Software Quality is a core member of SCCB orchestrating the acceptance and closeout of software changes. Test support will include configuration audits and support test monitoring.

Class C. For Class C Space Systems the software and firmware software quality assurance process is instantiated as with Class A and B systems but based on contractor internal standards commensurate with the complexity of software development effort. Many Class C efforts will be based on heritage software reuse, which will result in the software quality assurance process being tailored to access the quality impact of heritage. This will include assessment of software technical baseline completeness, software interfaces hardware, firmware, and new software development, impact to product compliance, quality, reliability, and safety. The software quality process will perform selective independent reviews and capture results in a closed loop action system. Software reliability will be focused on ensuring the correct processes are followed to promote reliability growth and software safety focus will be on critical hazards to personnel and hardware. Quality will support SCCB in change acceptance and closeout. Test support will include audits and selective test monitoring.

Class D. For Class D Space Systems the software and firmware quality assurance process is recommended but not mandatory. The program will assess the level of SQA needed based on the level and complexity of software development. Independent assessments will be executed in-line concurrently with peer and functional independent reviews. Artifacts will be captured but only for the major independent reviews conducted. Closed loop action tracking will continued to be followed. Software reliability as in Class C is focused on process assurance of reliable software development and software safety will be limited to those safety hazards of high criticality. A formal software change process is recommended with independent assessment of software changes and closeout. Test support will be limited to and audit process of configuration and monitoring of critical software development milestones.

B4-5 Effectiveness TIPS (Lessons Learned)

An effective software quality functions is based on a triad of development processes. These include:

- A rigorous compliance process that assures that the customer requirements are mapped in to a complete and traceable software development process for the product and the life cycle monitoring of process execution through the requirements, design, and coding process to ensure continued compliance to that process.
- Core membership in the software change management process providing independent assessment of the software change process including assessment of both identified defects, assurance of root cause determination, and the need for software baseline change. Once software change is approved the tracking of that change to ensure that the integrity of the software reliability and safety is not impacted and the change is completed in a timely manner. Core metrics from this process generate by SQA provide visibility into the health of the software development process.
- A process and product focused software reliability and software safety process that ensures continued reliability growth over the development lifecycle and ensures that hazards are appropriately mitigated.

B4-6 References

1. Aerospace Report TOR-2007(8546)-6018, *Mission Assurance Guide*.
2. Aerospace Report TOR-2011(8591)-5, *Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles*.
3. MAIW TOR-2010(8591)-18, *Mission Assurance Program Framework*.

Appendix B5: Supplier Quality Assurance (QA)

Eli Minson, General Dynamics
Brian Shaw, The Aerospace Corporation

B5-1 Introduction

This appendix provides guidelines for ensuring that supplied products used in deliverable systems and ground support equipment meet the highest level of quality for their intended application. Recommended criteria are developed that define sub-tier supplier quality assurance practices as they apply differentially to the four Mission Risk Class profiles.

Supplier Quality Assurance (SQA) processes includes the assessment of supplier capabilities, compliance to processes and flow-down requirements, and the verification of products and services. Development and maintenance of an approved and qualified supply base can reduce the risks associated with receipt of supplied products.

The prime contractor is responsible for ensuring that the developed system conforms to the contract requirements, including all products and services purchased from subcontractors and sub-tier suppliers. The general approach to accomplish this uses the industry-accepted criteria for quality assurance, AS9100, as the baseline.

Certification to AS9100 is typically in place at all Tier 1 and 2 organization developing space systems for mission risk Class A/B programs. Class C/D programs executed by Tier 1 and 2 organizations that also develop space systems for Class A/B programs, have command media built around AS9100 certification requirements reflecting positively on the quality of the end items developed. Below Tier 2, i.e., parts vendors, there is less likelihood of Aerospace specific quality management systems and an even lower likelihood that any buyer will be able to flow QA requirements since they are guided by existing corporate processes. In these cases, a gap assessment between the desired quality management system, i.e., AS9100, and the in effect system, typically ISO related, should be performed to understand the differences.

It should be emphasized that certification in-and-of itself is not sufficient. A properly scoped, funded, and staffed quality program with the proper level of authority must be in place. Objective proof of effectiveness is essential to ensure that a QA program is likely to meet the mission assurance/success objectives.

There are a number of QA-related activities that might not be considered QA, per se, but more logically considered as program management. These are the program management concerns of subcontract management and supplier management. Subcontract management is beyond the scope of this effort. Supplier management as defined in the Supplier Quality Assurance section of the Mission Assurance Program Framework. This appendix addresses those MA program framework supplier quality assurance elements including:

- Pre-contract on-site surveys to assure supplier can produce correctly, on time, the first time; and prevent deflect overflow
- Periodic supplier performance assessments/surveys
- Analyze data and perform objective supplier quality ratings
- Issue and closure of Supplier Corrective Action Requests (SCARs)
- Counterfeit materials avoidance: specifically flow-down, compliance verification, and suspect parts, alert coordination with other functions

- Supplier site inspections of in-process and final products
- Certifications of special processes by third party such as NADAP e.g., heat treatment, prohibited material testing, Non-destructive Test (NDT)

QA and subcontract management practices commonly exist within each Tier 1 and 2 contractor's command media. The government may also levy these requirements contractually using standards. For national security space, the quality system standards may include SAE AS9100 or SMC-S-003 (2008), which is a 9100 clone with additional process: Hardware Acceptance Reviews (HAR) to support the specific needs of high-reliability space systems. Use of compliance standards differs not only between mission risk classes, but as a function of acquisition strategy for specific programs or contracts.

B5-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which risk profile can be developed and are not intended as general standalone industry standard definitions.

Quality Management System (QMS). The systemic process for achieving customer satisfaction through the use of key characteristics identification and control, variation reduction of key characteristics, flow-down of similar process control requirements to subcontractors and suppliers, and other advanced process-oriented control and improvement techniques. QMS includes activities to monitor, measure, analyze, control, and improve processes; reduce product variation; measure/verify product conformity; establish mechanisms for field product performance feedback; and implement effective corrective action.

Documentation. Artifacts comprising written, configuration managed, and maintained statements of policy, objectives, process, procedures, and associated data/information records.

Product Realization. The systematic process to plan, design, acquire, and/or integrate a product (at any level from system to piece-part) meeting the mission, functional, and quality requirements established by the acquiring organization or customer.

Purchasing. The process of procuring product (at any level from system to piece-part) that conforms to the specified purchase requirements from an external supplier.

Production and Service Provision. The processes that creates the hardware or service that is delivered to customers, including assurance that suitable equipment is used, and how the release, delivery and post-delivery activities are controlled.

Monitoring and Measuring Equipment. Equipment used to quantify technical and quality attributes of products being produced, acquired, or delivered.

Measure, Analyze, and Implement Process. The systematic activities that proactively assess and control jobs and processes to ensure that they achieve calculated expectations.

Monitoring and Measurement. The methods used to ensure the effectiveness of the all Quality Management System processes.

B5-3 Matrix – Supplier Quality Assurance

B5-3.1 General Recommended Quality Assurance Approach

The industry consensus approach to effectively manage QA at all levels of application, Tier 1 and lower tier contractors/suppliers, are the requirements specified by SAE AS9100 [ref.]. For DOD high-reliability space, a government standard, SMC-S-003, replicates the AS9100 requirements but adds additional requirements for Hardware Acceptance Review (HAR).

Both documents provide the full range of QA activities that form a comprehensive QA approach. As such, they are sometimes viewed as applicable only to the Tier 1 (Prime) contractor for Class A programs. Failure to flow QA (and many other) requirements to lower tier contractors/suppliers in an applicable, verifiable, and cost conscience way provides an opportunity for unwarranted program risk.

Given that AS9100 and the SMC QA standard clearly are oriented toward Class A systems, this document addresses how those requirements can be differentially applied to the A-D mission risk classes where higher risk acceptance is an acknowledged characteristic. In general, the approach proposed is:

AS 9100 Quality Assurance Practices	
	Class A *Formal verification of all subs and suppliers prior to subcontracting*
	Class B *Formal verification of all subs and major suppliers prior to subcontracting*
	Class C *Formal verification of "major suppliers".* *Self-report (e.g. questionnaire) for all others.*
	Class D *Verification of key QA attributes for safety-critical "parts" suppliers.* *Best judgment of Principal Investigator for all others*

B5-3.2 Specific Recommended Quality Assurance Approach

The following tables show the QA practices as they apply to the four mission risk class profiles:

Quality Assurance Activities	Class A	Class B	Class C	Class D
Quality Management System Implement function + culture Establish criteria and methods - Monitor, measure, analyze - Implement corrective actions - Control outsourced processes	• Certified to ISO/AS9100 • Internal programs for continuous improvement, documented methods and procedures • Monitoring and measuring critical parameters • Monitoring supply base and reviewing incoming material for non-conformance	• Certified to ISO/AS9100 • Methods for monitoring and measuring critical parameters • Monitoring supply base and reviewing incoming material for non-conformance.	• Certified to ISO/AS9100	• Meet the intent of ISO/AS9100
Documentation QA policy + objectives Quality manual Quality procedures Quality records	• Documented and controlled quality system: methods for record retention, controlling effectivity of process changes • Control of quality procedures used during product manufacturing	• Same as Class A	• Documented and controlled quality system including methods for record retention	• Documentation of quality assurance processes
Product Realization Product-specific QA system Project Management Risk + Configuration Management Requirements Management Work transfer control Design Review Verification + Validation Customer interface	• Definition of key product requirements and flow downs from customer through appropriate supplier level • Control and distribution of processes changes impacting the use of the final product • Validation and verification of process or product changes regardless of driver	• Same as Class A	• Proven methods for key product requirements and flow down processes • Known history of successful control and distribution of process changes • Methods for verification and validation	• Documentation of product requirements • Awareness of process changes and impacts • Verification and validation methods per Principal Investigator's judgment

Quality Assurance Activities	Class A	Class B	Class C	Class D
Purchasing Register of approved suppliers Purchasing info + specification Supplier performance evaluation Deal with nonconformance Special process sources Assess supplier + vendor risk issues Purchased product verification	• Control of supplier selection and performance evaluation • Record retention and supplier interface requirements • Assurance of supply continuity • Assurance of purchased product meeting internal and customer requirements	• Same as Class A	• Proven method for control of supplier selection and performance evaluation • Effective record retention and supplier interface processes • Knowledge about supply continuity concerns • Assurance of purchased product meeting internal and customer requirements	• In-house development (e.g., AFRL) • External purchase from known vendors based on prior history or promising new suppliers
Production + Service Provision Plan + control execution Verify production process Production process changes Production equipment, tools + software Post-delivery support Validate processes Identify and trace throughout product realization or lifecycle Protect customer property Product preservation	• Control and validation of process or product changes • Control and verification and validation of process or product changes • Control and retention of critical information related to process or product changes including distribution methods to customers	• Same as Class A	• Proven methods for control of process or product changes • Proven method for control of process or product changes • Have records of critical information related to process or product changes including distribution methods to customers	• In-house development (e.g., AFRL) • External purchase from known vendors based on prior history or promising new suppliers
Control of monitoring + measuring equipment Monitoring + measurement requirements ensure conformity Monitoring + measurement procedures Validity of prior results upon nonconformance.	• Monitoring and measurement of critical parameters related to each main process used during product realization • Casual review of customer failures • Control and monitoring of manufacturing processes and changes to these processes	• Same as Class A	• Proven method for monitoring and measurements of critical parameters • Records indicating control and monitoring of manufacturing processes and changes to these processes	• In-house development (e.g., AFRL) • External purchase from known vendors based on prior history or promising new suppliers

Quality Assurance Activities	Class A	Class B	Class C	Class D
Plan + implement a monitor, measure, analyze, implement process Demonstrate product requirement conformity Ensure QA management system Improve QA effectiveness	• Continuous improvement of all processes and procedures • Implementing changes to the QA system resulting from the monitoring and measuring of key system attributes • Verification and validation of product to customer requirements	• Same as Class A	• Proven improvement method for processes and procedures resulting in nonconforming or unreliable product • Change evidence of the QA system from failed or ineffective system attributes • Verification and validation of product to customer requirements	• In-house development (e.g., AFRL) • External purchase from known vendors based on prior history or promising new suppliers
Monitoring and Measurement **Monitor customer satisfaction** **Conduct internal audit** Monitor + measure quality management processes Correct nonconforming process Identify nonconforming process impact on product Document verification of product characteristics Control nonconforming product - Analyze data - Continual improvement - Corrective action - Preventative action	• Conducting internal audits and addressing resultant identified deficiencies • Control and disposition of nonconforming product from suppliers and of internally generated product	• Same as Class A	• Evidence of internal audits and addressing resultant identified deficiencies • Proven methods for control and disposition of nonconforming product from suppliers and of internally generated product	• In-house development (e.g., AFRL) • External purchase from known vendors based on prior history or promising new suppliers

B5-4 Summary of Risk Classes

Class A. Certification of AS9100 process activities is performed at the prime contractor. Flow down of AS9100 requirement to subs and *all* suppliers with realization that prime contractors will be required to verify intent of AS9100 is met at lower Tier suppliers. Formal verification of all subs and supplier's certification and process/activity artifacts required.

Compliance standards for quality assurance are generally used on contract and are intended to be flowed to subcontractors and suppliers including SAE AS9100 or SMC-S-003 (2008), and SMC-S-019A (2008) for subcontract management practices.

Class B. As with Class A, certification of AS9100 process activities at prime and flow of AS9100 requirement to subs and *major* suppliers with realization that prime contractors will be required to verify intent of AS9100 is met at lower Tier suppliers. Formal verification of all subs and major supplier's certification and process/activity artifacts required. Minor amounts of relief from full requirements can be considered, such as:

- Quality Management System: less focus on internal continuous improvement programs external to the prime contractor.
- Documentation Process: less rigorous control, (oversight) of quality procedures during product manufacture.

Compliance standards for quality assurance are generally used on contract and are intended to be flowed to subcontractors and suppliers including SAE AS9100 or SMC-S-003 (2008), and SMC-S-019A (2008) for subcontract management practices.

Class C. Certification of AS9100 process activities recommended at prime and including verification of AS9100 certification at *major* subs/suppliers. Self-report of certification is allowable for all other subs/suppliers. Significant relief from full AS9100 requirements can be considered, retaining only the "key" practices applicable to the specific acquisition for each QA Process/Activity, as described in the Section 2 Matrix. Standards for quality assurance and subcontract management are often included in contracts, but recommend as reference documents and the contractor is instructed to meet the intent of those standards and flow to subcontractors/suppliers where applicable.

Class D. Meeting the intent of an AS9100-like QA process desirable at the development organization and verification of QA process at subs/suppliers of *safety-critical* parts or components. For all other subs/suppliers, the Principal Investigator's best judgment of acceptable levels of QA in parts/products for the amount of mission assurance that is desired. Significant relief from full AS9100 requirements is acceptable, retaining only the "key" QA practices described in the Section 2 Matrix. Standards for quality assurance and subcontract management are generally not used.

B5-5 Effectiveness TIPS (Lessons Learned)

Certain quality assurance practices, over and above the implementation of AS9100 requirements, were identified by the 2010 MAIW as key issues for successful sub-tier supplier management. These supplier management practices include:

Verify potential subcontractor or supplier QA capabilities by pre-contract on-site surveys.

A supplier survey is a type of subcontractor/supplier QA verification. It is a verification process that accomplishes two goals: verify that the QA processes a sub or supplier claims to do is actually done, and verify that the QA processes a sub or supplier does is effective.

The supplier survey is generally performed during the pre-contract phase. Initial issues to verify include the organization's physical location and ability to meet the business/contractual needs. An on-site supplier audit can often be accomplished in one day but good planning is necessary for the sake of both schedule and effectiveness.

Planning issues include: clear understanding of requirements (such as those discussed in Section 2 of this document); full cooperation of the supplier and their personnel; supplier provision of essential QMS documentation before the actual site visit; and clear identification of personnel to be interviewed and processes to be observed.

During the on-site survey it is important for the auditor to verify processes using objective evidence. Objective evidence may need to be evaluated and measured considering the "spirit" of the evidence as much as the actual evidence verbiage itself. The auditor should ensure that the requirements are being clearly communicated from the prime to the subcontractor or supplier rather than allowing the supplier to control the flow of the audit. Flexibility is important, but it is even more important for an audit to "stay on task" and accomplish all of the stated goals of the supplier survey. Where language or culture may differ, it is often useful to use personnel familiar with the supplier's language/culture to ensure effective communication. After an on-site survey it is recommended to provide the potential subcontractor or supplier with approved results and any recommendations that may be warranted.

The capability information that should be addressed, at a level of detail appropriate for the acquisition class, includes:

1. Engineering
    - 1.1. Processes to integrate all design/development activities to concurrently balance the product design and all associated fabrication, manufacturing, and supportability processes
    - 1.2. Design for manufacturing process that is statistically capable and has adequate capability/capacity to meet expected production rate
    - 1.3. Sub-tier technical capability/capacity
    - 1.4. New technology insertion/qualification
    - 1.5. Risk management program
    - 1.6. Parts and material qualifications
    - 1.7. Parts, materials, and process control plan
    - 1.8. Commercial Off The Shelf (COTS) hardware and software considerations integrated into the risk management process
    - 1.9. Reliability, maintainability, and availability plan
    - 1.10. System safety and product safety plan
    - 1.11. Software engineering processes
    - 1.12. Prohibited parts, materials and process plan
2. Operations
    - 2.1. Manufacturing capability

2.2. Configuration control
2.3. Statistical process control
2.4. Data management plan

3. Supplier Management
   3.1. Financial health assessment
   3.2. Acceptability of accounting system
   3.3. Capability Maturity Model Integration - Acquisition (CMMI-A) assessment
4. Quality Assurance
   4.1. Quality system maturity
   4.2. Definition of space-related requirements beyond industry standards
   4.3. Documented review of special process capability and control
   4.4. Sup-tier supplier control

Conduct periodic supplier performance assessments or resurveys.

Recommendations for periodic re-assessment of suppliers are primarily a function of real or perceived concern that the original assessment has become invalid. Changes over time are inevitable and the cause of the change can be either obvious such as plant damage from earthquake or tsunami, or much more subtle such as evolving alterations to process implementation. Intuitively, the subtle changes are more difficult to detect unless an effective surveillance program is in place and effectively operated.

Proactive surveillance and concurrent risk assessment over-and-above site visits can identify the need for re-assessment or re-survey. This surveillance cannot be limited to the immediate subcontractor or supplier, but must include in-depth knowledge of lower-levels of the supply chain if it is to support an in-depth and realistic understanding of potential problems.

Various tools and systems can be utilized to more efficiently identify critical supply chain areas for assessment. For example, a supply chain value stream map can be used to identify single point failures in the supply chain related to the production of a critical sub-element in a spacecraft. These forms of data mining exercises should be utilized to better inform the re-assessment time frames for suppliers such that the risk posture of the proposed program is appropriately supported.

Ensure consistent and valid analysis of data in the performance of objective supplier quality ratings.

Many systems exist for ranking and scoring suppliers based on objective and subjective performance measures. Based on the need to measure and manage risk profiles for each program class, an appropriate system to capture, rationalize, and manage the risks associated with suppliers needs to be in place at the procurement organization at a minimum with this method being distributed to additional Tiers of suppliers as the program Class shifts from Class D through Class A. At Tier 1 and 2 suppliers it is expected that objective evidence of a system to measure supplier quality may be identified and audited in a manner to show linkages between supplier quality ratings and the risk profile of a program.

Lower Tier suppliers and programs may require support from the procurement agency to perform these tasks and/or the objectivity of the supplier ratings may lean further toward subjective measures based on the ability of the supplier to provide other deliverables that reflect the potential quality of the whole. In the extreme case of a technology demonstration developed by a very small team of individuals the quality of this organization may be up to the opinion of the management arm within the procurement agency.

For all program Classes, a clear mapping of supplier quality to program risk posture should be a goal such that perturbations in the supply chain may be accurately reflected in the risk associated with the specific program.

Effectively manage and flow-down supplier corrective action requests (SCAR).

The Corrective Action Process is fully defined in the Defense Contract Management Agency guidebook [ref]. Support material including a training matrix and a task checklist is included.

As written, one could assume that it only applies to the Tier 1 relationship between the government and prime contractor. Since QA must be appropriately flowed from the Tier 1 to lower tier subcontractors and suppliers, it is appropriate to adapt the DCMA process slightly. Specifically, the role of the government should be adopted by the Tier 1 contractor in order to fulfill their contractual commitment. The Tier 1 contractor must be fully knowledgeable about any corrective actions at subcontractor or sub-tier suppliers that may affect their ability to fulfill their contractual requirements. Given that, the Tier 1 contractor should take an active leadership role such as integrator, if not the arbitrator, of sub-tier corrective actions in support of the overall DCMA (and the like) activities.

Specific tailoring of this process is beyond the scope of the current effort and will need the concurrence/approval of government contracting and legal authorities.

Effectively manage counterfeit material avoidance activities.

Counterfeit material avoidance has become a major issue in the supply chain of U.S. Defense systems and various other industries and organizations. Various Aerospace industry organizations have indicated that the best method for avoidance is to limit procurement of product to Original Equipment Manufacturers (OEMs) or their specific authorized distributors. However, this is sometimes not possible due to the obsolescence of materials required for maintenance or development of new products based on historical designs. All programs, regardless of the class, should be cognizant of the extreme risk taken when materials from unverifiable sources are procured.

If OEM or authorized distributors do not have a product available a cost/benefit analysis should be performed on the procurement of a replacement from a questionable source and the re-design of the system to remove the item in question. This study should take into account the potential for sub-contracting to the OEM for ramping up a closed production line, impact of embedding a counterfeit part into a system, and the potential for the procured parts to flow through to other government systems. With this study in hand the supply chain risk associated with a specified product should become evident and this can be factored into the risk posture of a program.

Utilize on-site inspections of in-process and final products.

Class A/B programs typically flow down requirements for in-process and final product inspections as part of their contractual requirements with DCMA taking part in these activities. If a program chooses not to flow down requirements for these activities the associated risk for embedded un-verified systems or elements within a system should be taken into account during the risk analysis. Class C/D programs may accept deliverables for inspection and the integrators site, but should not integrate the elements into the final system without a sub-system verification. The verification should ensure a system element procured as a Class C/D program does not violate a spacecraft ICD or other requirement that may have been procured as a higher level program class.

The on-site inspection process is intended to shift the costs associated with a sub-system failure as far up the supply chain as possible in order to resolve issues at the lowest level of assembly. This has been shown by various studies and organizations to be the keystone to the reduction in overall system costs. Therefore, the risk associated with integration of an un-inspected element into a high level assembly and the potential incurred risk should be taken into account during the risk analysis of the program.

Effectively manage certification of special processes by third parties.

A clear understanding and mutual agreement must exist between the Tier1 contractor and the contracting agency on the processes considered to be "special". All special processes must be definitively identified, documented, and certified as compliant. Third party survey of special processes can be used as applicable. Industry consensus criteria for "as applicable" do not appear to exist. At a minimum, that consensus must be the contractual agreement between the contracting agency and the Tier 1 contractor. Tier 1 contractor must flow the contractual requirements to Tier 2 and lower subcontractors or suppliers, and manage those subtier entities, as required to fulfill their contractual obligations. Tier 1 contractors may need to support third-party surveys and should (minimally) review third-party survey reports/results as part of their subcontractor management effort.

B5-6 References

1. Aerospace Report TOR-2011(8591)-18, *Mission Assurance Program Framework*, Publication date TBD.
2. Aerospace Report ATR-2011(9369)-4, *Acquisition Risk Planning and Tailoring Guidelines for National Security Space Vehicles*, Publication date TBD.
3. TOR 2007(8546)-6018 Rev A, *Mission Assurance Guide*, 1 July 2007.
4. SAE AS9100C, *Quality Management Systems - Requirements for Aviation, Space and Defense Organizations*, 15 January 2009.
5. SMC-S-003, *Quality Assurance for Space and Launch Vehicles*,.13 June 2008.
6. SMC-S-019A, *Program and Subcontractor Management*, 11 August 2008.
7. Space Quality Improvement Council, *Supplier Capability and Assessments Requirements Document*, Version 10, March 2009.
8. ANSI/PMI 99-001-2008, *A Guide to the Program Managers Book Of Knowledge [PMBOK]*, Fourth edition, 2008.
9. Defense Acquisition University (DAU), *DAU Program Managers Tool Kit,* Fourteenth Ed. 2005.
10. Defense Contract Audit Agency (DCMA), *Corrective Action Process*. http://guidebook.dcma.mil/226/226-1/index.cfm (accessed March 2011).
11. Defense Contract Audit Agency (DCMA), *Pre-award Surveys*, http://guidebook.dcma.mil/42/guidebook_process.htm.
12. Payne, D. *Auditing the PCB fabricator,* Circuits Assembly. February 2005.
13. Texas Instruments QA website, (accessed Feb 2011) http://focus.ti.com/quality/docs/gencontent.tsp?templateId=5909&navigationId=11221&contentId=5022.
14. National Semiconductor Quality policy manual, (accessed Feb 2011) http://www.national.com/kbase/category/Quality.html#46.
15. Microsemi Quality system, (accessed Feb 2011) http://www.microsemi.com/qapolicy.asp.
16. International Rectifier Quality system. (accessed Feb 2011) http://www.irf.com/product-info/reliability.
17. Analog Devices. (accessed Feb 2011) http://www.analog.com/en/quality-and-reliability/total-quality-management/content/index.html.

Appendix C: Triage, Information and Lessons Learned Processes

Appendix C captures the Risk Classes Matrixes for the Triage, Information, and Lessons Learned MA framework processes for mission success. Processes include:

- C1: Failure Review Board
- C2: Corrective/Preventative Action
- C3: Alerts, Information Bulletins

Appendix C1: Failure Review Board

Andy Penner (Lockheed Martin)
Dr. Rudy Enrick (Orbital Sciences Corporation)

C1-1 Introduction

During the development, build, assembly, and test of spaceflight hardware, there will invariably be failures. It is vital to the ultimate success of the hardware that the reasons for the failures be determined and the causes of the identified defects be corrected. This investigation and corrective action process is directed and administered by a Failure Review Board (FRB).

History has shown that poorly performed investigations can and often do result in hardware or mission failures. The primary tasks of the FRB are pursuit of root cause and corrective action for failures or anomalies that occur on their programs. The FRB establishes the structured environment in which failures are identified, oversees and/or directs the investigation tasks, reaches a final conclusion on root cause determination, ensures corrective and preventive actions are taken, and documents the results of these efforts. A properly executed FRB process will reduce the technical risks of any program.

In general, the primary differences between the mission classes for the FRB process are directly associated with the level of risk assumed by that mission class. For example, on Class A programs, where risk is reduced to the lowest practicable level, the FRB will drive to root cause through a highly structured approach that may result in destructive hardware actions, and where corrective actions are rigorously taken and verified effective. By contrast, a Class D program FRB may be an informal gathering of cognizant personnel whose only goal is to return the hardware to functionality and who cannot afford to pursue cause to the level where hardware could be destroyed.

One element of the FRB process warrants further discussion here. When the investigation effort cannot determine the cause of failure, an unverified failure or unknown cause failure is declared (see definitions below for distinction between these two failure types). The response to unverified failures is directly correlated to risk. The lowest risk measure at a component (i.e., box) level is typically to remove and replace all possible causes of the failure (aka, a worst case change out). Of course, other risk factors must be assessed when developing the final disposition, such as collateral damage to adjacent hardware, component test time, and ability to address the consequence of a repeat failure by other means. System level unverified failures are more difficult to address from a risk basis, as it is often unclear what the lowest risk solution to the failure is. Considerations would include (but are not limited to) the consequence of a repeat failure, ability to address the failure through software (e.g., fault protection), collateral damage risks involved with replacing components, and available system redundancy. Due to the risks associated with unverified failures, it is common for these issues to be thoroughly analyzed and briefed to both senior company management and the customer.

The matrix in this section is structured to decompose the various FRB elements, and identify where differences would typically exist between the four mission classes.

C1-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which risk profile can be developed and are not intended as general standalone industry standard definitions.

Failure. A state or condition that occurs during test or pre-operations that indicates a hardware element will fail to meet its performance, qualification, or reliability requirements.

Failure Review Board (FRB). A group, led by senior program personnel, with authority to formally review and direct the course of a root-cause investigation and the associated corrective-action sub-process. The FRB oversees the FRACAS process applicable to the subset of hardware failures that meet program or company thresholds for triggering an FRB.

Failure Reporting, Analysis, and Corrective Action System (FRACAS). The totality of closed-loop processes for detecting, reporting, analyzing, documenting, correcting, trending, preventing, and managing hardware and software failures.

Root Cause. The ultimate cause of a failure that if eliminated would have prevented the occurrence of the failure.

Unknown Cause. A failure that is sufficiently repeatable (verifiable) to be isolated to the unit under test (UUT), but whose root cause cannot be determined for any number of reasons. This includes the spectrum of failures ranging from having only direct cause identified to those having probable cause identified.

Unverified Failure (UVF). A perceived (irrespective of the accuracy of the perception) failure of unknown cause (in the UUT) or ambiguity such that the failure can't be isolated to the UUT or test equipment. Typically a UVF does not repeat itself, preventing verification. This precludes the hypothesis-testing component of a root-cause investigation.

Worst Case Change Out. An anomaly mitigation approach occasionally performed when the exact cause of the anomaly cannot be determined (i.e., an unverified failure). The approach consists of performing an analysis to determine what hardware could possibly have caused the defect. All of the suspect hardware is then replaced.

Note: Definitions 1, 2, 4, 5, and 6 are taken from the 2011 MAIW Failure Review Board Guidance Document TOR-2011(8591)-19. As similar actions are taken for Unknown Cause and Unverified Failures, the term "UVF" is used to describe both of these failure types throughout this Appendix.

C1-3 Matrix – Failure Review Board

Requirement	Class A	Class B	Class C	Class D
Board Members				
Chairman Voting Members Invitees	• Program FRB Chair an experienced technical lead (e.g., Chief Systems Engineer) • Typical Board: Program Manager, Mission Assurance Manager, customer representative • Off-program subject matter experts (SMEs) expected to attend	• Program FRB Chair an experienced technical lead (e.g., Chief Systems Engineer) • Typical Board: Program Manager, Mission Assurance Manager • Customer and off-program subject matter experts (SMEs) invited	• Same as Class B	• FRB Chair assigned on an ad-hoc basis • Typical Board: Program Manager, Mission Assurance • Program SMEs limited to immediate supervision
FRB Plan				
Detail Level Approvals	• Detailed Program FRB Plan generated (delineate when FRBs held, identify roles and responsibilities, documentation requirements) • FRB Plan could require customer approval	• FRB performed to company command media requirements	• Same as Class B	• Same as Class B
Documentation				
Meeting Notices Presentations Meeting Minutes Action Items	• Formal FRB meeting notices used (including time, location, telephone/computer links for off-site personnel) • Presentation packages provided using a format defined in the FRB Plan • Meeting minutes written, distributed, and stored • Action items captured and tracked using a closed-loop system	• Formal FRB meeting notices used (including time, location, telephone/computer links for off-site personnel) • Presentation packages expected • Meeting minutes written, distributed, and stored • Action items captured and tracked	• FRB meeting notices optional • Presentation packages optional • Meeting minutes and action items documented in the originating non-conformance document	• FRB meeting notices unlikely • Presentation packages optional • Meeting minutes and action items documented in the originating non-conformance document

Requirement	Class A	Class B	Class C	Class D
Meeting Conduct				
Level of Formality Quorum Requirements Communication Needs	• Formal meeting (agenda, attendee list, quorum) • Presentation packages distributed prior to the meeting or on a real-time computer link • Votes taken to approve recommended actions/conclusions • Action items assigned to direct future work	• Same as Class A	• Informal meetings • Presentation material optional • Decisions made by consensus • Action items may be closed based on verbal inputs	• Same as Class C
Investigation Expectations				
Failure Determination Fault Containment Failure Analysis Root Cause Determination	• Structured failure investigation approach • Investigation tool (fishbone, fault tree, K-T analysis) used to guide the investigation • Laboratory support used to perform destructive parts analysis, with formal lab reports provided • Detailed examination of the circumstances around the failure used to identify root cause • FRB participates/directs/ approves steps throughout the process	• Same as Class A	• Lead investigator directs investigation (FRB direction when the failure is extremely complex) • Cause understanding identified to return the hardware to service (may not be root cause) • Lab support expected; formal reports optional	• Investigation approach to find the reason the hardware failed, understand the failure mechanism to determine the means to repair the defect, and return the unit to service • Structured investigation tools optional • Root cause identification often not pursued • Independent failure analysis lab optional (as-needed basis)

Requirement	Class A	Class B	Class C	Class D
Corrective Action				
Failed Hardware Disposition Sibling Hardware Assessment Preventive Action	• Disposition of failed hardware would address root cause and possible overstress concerns • Detailed sibling hardware (i.e., hardware that shares same cause) assessment performed • Preventive actions taken (where possible) to address root cause • FRB would track all corrective measures to closure	• Disposition of failed hardware would address root cause and possible overstress concerns • Detailed sibling hardware (i.e., hardware that shares same cause) assessment performed • Preventive actions taken (where possible) to address root cause • FRB would track hardware disposition and sibling assessment/actions to closure	• Disposition of failed hardware would address failure symptoms and possible overstress concerns • Sibling hardware assessment performed only when root cause was established • Preventive actions taken to comply with company process requirements (not program specific) • FRB would track hardware disposition	• Disposition of failed hardware would focus on return to functionality • Detailed sibling hardware assessment unlikely • Preventive actions taken comply with company process requirements (not program specific) • FRB would track hardware disposition
Unverified Failure Handling				
Disposition Actions Documentation Review Requirements	• Common approach is "worst case change out" of all possible causes performed on component-level UVFs • System-level UVFs would take lowest practical risk approach (e.g., hardware replacement, added fault mitigation) • Formal analysis of the hardware disposition and risks (including risk rating) expected • Extensive program, company (Executive and off-program Subject Matter Experts [SMEs]), and customer reviews required	• Change out of all likely causes of failure on component-level UVFs • System-level UVFs would take low risk approach (e.g., hardware replacement, added fault mitigation) • Formal analysis of hardware disposition and risks reviewed by on-program personnel and the customer • Off-program and Executive reviews would likely be cursory in nature	• • Change out of most likely cause of failure on component-level UVFs • System-level UVFs would take low risk approach (e.g., hardware replacement, added fault mitigation) • Formal analysis of hardware disposition and risks reviewed per company requirements • Customer cognizant of the unverified failure, but not involved in the analysis review • Limited or no off-program and Executive review	• Not uncommon to not replace UVF hardware elements in the cases where a repeat would not lead to mission loss • Formal analysis of hardware disposition and risks reviewed per company requirements • Customer knowledge limited to a summary of the analysis • No off-program and Executive review

Requirement	Class A	Class B	Class C	Class D
Supplier Failures				
	• FRB reviews planned and completed investigation steps, and approves hardware corrective actions • Suppliers provides technical expertise and recommendations • FRB would be the ultimate decision authority	• Same as Class A	• FRB reviews planned and completed investigation steps, and approves hardware corrective actions • Suppliers provides technical expertise and recommendations • FRB would be the ultimate decision authority	• Suppliers expected to complete investigations with minimal guidance • FRB reviews supplier findings to identify any required actions

C1-4 Summary of Risk Classes

Class A. The FRB actions on Class A programs strive to identify root cause, seek to eliminate defects in all sibling hardware that share the identified cause, and take/verify that effective preventive measures are implemented. The FRB meetings tend to be formal in structure, as the customer would routinely attend, and may be a voting FRB member. A program-level FRB plan could be expected, based on contract requirements. The FRB will likely control the investigation closely, whether it is at the contractor's facility or at a supplier. Decisions of the FRB will be well documented, with the results maintained for later review. When the investigation leads to piece parts, destructive parts analysis will be undertaken in support of root cause identification. The disposition for component-level unverified failures would almost exclusively be a worst-case change out. Sibling hardware assessments would be rigorously undertaken, especially for multi-vehicle programs.

Class B. The approach taken for Class B programs will be very similar as for Class A relative to FRB. The pursuit of root cause would still be the top priority, and the FRB meetings would be well structured and would likely include the customer as an invited (but non-voting) participant. It is unlikely that a program-unique FRB plan would be prepared; the company FRB process would be utilized. Some of the control of the investigation would be delegated to the responsible hardware engineer or the supplier, but would be closely monitored by the FRB. The documentation of FRB actions would be maintained, and action worked to closure. Unverified failures would require thorough evaluation, and typically result in worst-case change out. Sibling hardware assessments would be rigorously undertaken, especially for multi-vehicle programs.

Class C. While the pursuit of root cause is still a primary consideration for the FRB on Class C programs, the level of control and rigor are reduced compared to Class A and B programs. The FRB investigations would be led by responsible engineers and suppliers, with the results provided to the FRB. The presentations made would be less formal (perhaps only verbal discussions), and the FRB performed in accordance with company policy. The customer may be invited to participate, but would more likely see just the results of the FRB. Unverified failures would be processed per company policy, but with an eye to cost (and at higher risk) when developing hardware disposition, i.e., a full worst-case change out may not occur.

Class D. The least formal FRB process would be used on Class D programs. The primary goal of the investigation process shifts from root cause (typical on Classes A-C) to the identification of the actions needed to return the hardware to service. The FRB "team" may be limited to the responsible engineer and the program Quality Assurance representative. Documentation expectations would be reduced, with the investigation results recorded only in the associated non-conformance document. Customer involvement would be minimal. Unverified failure disposition would rarely include worst-case change out, as expected for the higher risk program profile.

C1-5 Effectiveness Tips

- A failure investigation or FRB training course can provide a baseline for success when dealing with failures.
- During the initial FRB meeting, a detailed timeline of the events leading up to and including the failure can help bring all meeting participants quickly up to speed with the issue.
- Discuss all investigation steps for the possibility of lost data before executing them; simple actions like de-mating connectors, powering down a test, or loosening a screw can quickly result in unrecoverable information that might have been a clue to the cause of failure.
- Assess any unexpected result identified during an investigation, as it may be a signal to the possible cause.

- Share all data gathered during the investigation, even when the information may not support your conclusions.

C1-6 References

1. MIL-HDBK-2155, Failure Reporting, Analysis, and Corrective Action Taken, 11 Dec 1995.
2. Aerospace Report TOR-2010(8591)-18, Mission Assurance Program Framework (2010 MAIW).
3. Aerospace Report TOR-2011(8591)-19, Failure Review Board Guidance Document (2011 MAIW).

Appendix C2: Corrective/Preventive Action Board

Andy Penner (Lockheed Martin)
Dr. Rudy Emrick (Orbital Sciences Corporation)

C2-1 Introduction

Programs providing spaceflight hardware have to address problems from multiple sources. The issues that are found internal to the program are most readily visible and must be overcome to progress through design, development, build, integration, test, delivery, and ultimately flight. However, problems that occur outside the program can also have a major impact. If another aerospace program (either within the company or at a competitor) identifies an issue whose cause is generic across either the company or the industry, then that problem must be addressed to ensure program success. One mechanism used to identify and address these systemic concerns is the Corrective/Preventive Action Board (C/PAB).

As implied above, the primary purpose of the C/PAB is to identify, act upon, and eliminate systemic problems. The identification step is typically performed through review of non-conformance documents, incident reports, audit findings, customer concerns, test failures, GIDEP (or other) Alerts, and Safety findings. Once a systemic concern is flagged, the C/PAB will direct investigation to identify the root cause of the problem so that actions can be taken to correct or eliminate the issue. Once the corrective and/or preventive measures are enacted, the effectiveness of the actions will be monitored to allow issue closure.

In order to perform all the required actions, the C/PAB must be comprised of representatives from the disciplines where the problems exist and actions are needed, i.e., engineering, manufacturing, quality, supply chain, and management. The representatives must also be of the appropriate level of responsibility and authority to take the actions required to correct the problems. The C/PAB is typically chaired by a senior functional or program representative. Companies may have multiple C/PABs to support either specific program areas (e.g., communication spacecraft, launch vehicles, optical sensing payloads) or to address various manufacturing disciplines (e.g., electronics build and test, propulsion assembly, vibration and thermal testing). While very large programs may have their own C/PAB, it is often the case that programs support the wider area product or manufacturing C/PAB meetings.

The industry references (military handbooks and standards, NASA directives and the like) that are the basis for most Mission Assurance processes are lacking relative to C/PAB direction. Due to this fact, each company must develop their own internal processes to complete this effort. This Appendix is based on the C/PAB process used at one company and was reviewed for applicability across the MAIW members. As stated in the "Future Work" section at the end of this section, development of an industry standard for C/PAB is warranted.

The matrix in this section is structured to decompose the various C/PAB elements, and identify where differences would typically exist between the four mission classes. It should be noted that, since most C/PABs are at a company level, there is little differentiation across the Class A to D missions. All mission classes would be expected to support the various company C/PAB meetings, and only the largest programs would have their own C/PAB. This "leveling" across the classes is reflected in the matrix.

C2-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which risk profile can be developed and are not intended as general standalone industry standard definitions.

Corrective Action. Immediate or short term actions taken to bring hardware or processes into an acceptable condition for known or suspect problems for which root cause may or may not be known. For example, a component failure was determined to have been caused by a manufacturing error due to inadequate technician training. Corrective action is taken to rework all units that have the defect caused by the error, and to implement a process improvement to reduce the errors.

Corrective/Preventive Action Board (C/PAB). A group of individuals typically led by senior quality or engineering personnel, with the responsibility and authority to formally identify, investigate, and take action to correct and eliminate systemic problems. The C/PAB process may be performed at the program, product area, manufacturing area, sub-contracts, and/or company levels.

Preventive Action. Action taken to address the root cause of a problem in order to permanently eliminate the problem. For example, a component failure was determined to have been caused by a manufacturing error due to inadequate technician training. Preventive action is taken to implement a mandatory technician-training program on the process where the defect was created.

Root Cause. The ultimate cause of a failure that if eliminated would have prevented the occurrence of the failure.

Systemic. An issue in which the cause has been determined to impact multiple programs, manufacturing areas, or companies. A systemic problem may be isolated within a specific company (e.g., a soldering process problem affecting multiple programs having boxes built at that location) or industry wide (e.g., a GIDEP Alert documenting fraudulent certifications from a widely used material supplier).

C2-3 Matrix – Corrective/Preventative Action Board

Requirement	Class A	Class B	Class C	Class D
Board Members				
Owner Chairman Membership/Stakeholders Invitees	• CAB owner would likely be the company (or major product business segment) Quality or Engineering Executive • Program-level CAB optional - based on contract or company policy • Senior functional or program representative chairs the program-level CAB • Engineering, Manufacturing, and Subcontracts provide CAB members • Customer would be invited to all program CAB meetings	• CAB owner would likely be the company (or major product business segment) Quality or Engineering Executive • Program-level CAB unlikely • Engineering, Manufacturing, and Subcontracts provide CAB members • Customer would be invited to all program CAB meetings	• CAB owner would likely be the company (or major product business segment) Quality or Engineering Executive • No program-level CAB • Engineering, Manufacturing, and Subcontracts provide CAB members • Customer would be invited to all program CAB meetings	• CAB owner would likely be the company (or major product business segment) Quality or Engineering Executive • No program-level CAB • Engineering, Manufacturing, and Subcontracts provide CAB members • Customer participation unlikely
Documentation				
Agenda Presentations Meeting Minutes Action Items	• Agenda would include data used to identify issues, investigation status of systemic issues, corrective action plans, and status/closure of action items • Formal presentations provided • Meeting minutes (attendees, key discussion points, action item status) produced • Action items tracked to closure, with estimated completion dates	• Same as Class A	• Same as Class A	• Same as Class A

Requirement	Class A	Class B	Class C	Class D
Meeting Conduct				
Meeting Frequency Quorum Requirements Communication Needs	• CAB frequency dependent on contract or company requirements (typically no more that once a month) • Quorum requirements established by the Chair • Representation from all stakeholders expected at each CAB meeting	• Same as Class A	• Same as Class A	• Same as Class A
Issue Identification				
Non-conformance Data Review Escapements Incidents Supplier Issues Rick Review Items Test Failures Audit Findings Customer Findings GIDEP or Other Alerts Safety Findings or Incidents	• List of sources provided at the left provide the basis to identify issues which could trigger CAB action • Action “trigger” for each data source based on program discretion or company policy	• List of sources provided at the left provide the basis to identify issues which could trigger CAB action • Action “trigger” for each data source based on company policy	• Same as Class B	• Same as Class B
Take Action				
Investigation Root Cause Analysis Corrective Action Plan Development Preventive Action Implementation	• Range of investigation actions determined by program discretion and company policy • CAB assigns investigation task and expects the assignee to establish root cause • Corrective action plan to address root cause is established and presented to the CAB • Preventive action plan may also be developed to eliminate the cause	• Range of investigation actions determined by company policy • CAB assigns investigation task and expects the assignee to establish root cause • Corrective action plan to address root cause is established and presented to the CAB • Preventive action plan may also be developed to eliminate the cause	• Same as Class B	• Same as Class B

Requirement	Class A	Class B	Class C	Class D
Verify Action Effectiveness				
Implementation Verification Effectiveness Assessment	• CAB verified the corrective actions were taken (e.g., document changes, training added) • Effectiveness monitored through the same source data that provided the initial issue	• Same as Class A	• Same as Class A	• Same as Class A

C2-4 Summary of Risk Classes

Class A. As Class A programs are typically large in scale, they are the most likely to have a program-specific C/PAB, and is especially true for multi-vehicle programs. The processes used by a program-level C/PAB are the same as for wider area C/PABs, though the majority of the effort would be focused on products and processes used on the program. The results of the program C/PAB would be documented and shared per company requirements, and reported to their customers.

Class B. Unless a Class B program produced multiple flight articles, it would be rare that it would have a program-unique C/PAB (unless required by company policy). In general, Class B programs support wider area (either product or manufacturing area) C/PABs. In this role, the programs would provide the data used to identify systemic issues, and take or support the actions directed by the C/PAB to investigate and correct problems. Any C/PAB issues that impacted the program (i.e., required unplanned action by the program) would be routinely reported to the customer.

Class C. Class C programs rarely have a program-specific C/PAB (unless required by company policy). Class C programs support wider area (either product or manufacturing area) C/PABs. In this role, the programs would provide the data used to identify systemic issues, and take or support the actions directed by the C/PAB to investigate and correct problems. Any C/PAB issues that impacted the program (i.e., required unplanned action by the program) would be reported to the customer.

Class D. Unless company policy dictated otherwise, Class D programs would not have a program-unique C/PAB. Class D programs support wider area (either product or manufacturing area) C/PABs. In this role, the programs would provide the data used to identify systemic issues, and take or support the actions directed by the C/PAB to investigate and correct problems. Any C/PAB issues that impacted the program (i.e., required unplanned action by the program) would be reported to the customer if there were significant cost or schedule implications.

C2-5 Effectiveness Tips

- The C/PAB process works more effectively if there is committed, active participation of area management.
- A structured approach to share information across various C/PABs within a company will make the overall process more effective.
- Maintaining C/PAB records in a common location (such as a server or website) accessible to all interested parties will make the process more useful.

C2-6 References

1. AS9100, Rev. C, *SAE Aerospace Standard*, January 2009.
2. Aerospace Report TOR-2010(8591)-18, *Mission Assurance Program Framework (2010 MAIW)*.

Appendix C3: Alerts/Information Bulletins

Andy Penner (Lockheed Martin Space Systems Company)

C3-1 Introduction

A program will face many problems getting from the proposal phase to product delivery. Most of the issues will occur on program, but there will be other concerns that arise from other programs within the company or from industry at large. These problems will be communicated as Alerts or Information Bulletins.

A partnership between the United States government and industry was established to share information that could impact either party. The sharing arrangement resulted in the Government/Industry Data Exchange Program (GIDEP). The GIDEP system produces many different types of documents, with the Alerts, Agency Action Notices, Problem Advisories, and Safe Alerts being of most interest to the space industry. These documents relate problems encountered during the course of the program life cycle that are suspected or shown to be generic or systemic in nature and thus could impact areas beyond where the original problem was found. Due to a desire to preclude all programs from having to learn of these generic issues themselves, the requirement to be a participant in the GIDEP system (for companies) and respond to GIDEP alerts (for programs) has been a standard for many years.

Numerous government organizations (e.g., Missile Defense Agency, NASA) have developed systems similar to GIDEP to share potentially generic problem information across their programs. These documents, whether termed advisories, bulletins, or alerts, can collectively be called information bulletins. Depending on agency or proprietary restrictions, these government-entity-generated information bulletins can be and often are sent to contractors who do business with the agencies who issue the documents. Another common source is the Space Quality Improvement Council (SQIC), which produces a consistent stream of advisories, many of which become internal bulletins at the companies that identified the issue or GIDEP Alerts. The SQIC advisories do come with third party proprietary restrictions, but are readily exchanged between the SQIC members. At the contractors, the documents are treated the same as GIDEP alerts (if allowed by the distribution restrictions), such that all programs, whether they work for the issuing agency or not, can gain benefit from the information provided.

In a similar vein, contractors often maintain an internal bulletin system to provide information on potentially generic failures or lessons learned across the programs within their company. These documents may be the basis for a later GIDEP alert, but can usually be issued more rapidly within the company than through the GIDEP system. At most companies, these internal information bulletins are treated identically to GIDEP alerts (or external information bulletins), and require program assessment for impact. It is common at many companies to have an internal database into which programs enter their assessments, retain the information for future use, and from which data are pulled to document alert processing status for a variety of internal reviews and meet customer data requirements. All aerospace contractors would maintain internal command media that direct the process for distribution and review of all alerts and bulletins, which would typically be common to all programs within the company.

Due to the nearly universal application of the information, there are few differences across the Class A to D program spectrum. All programs, large or small, can be impacted by a generic part problem, and thus need to have access to the alert and bulletin information. Another factor that tends to reduce differences is that companies use a common alert and bulletin receipt, screening, distribution,

reporting system, and internal reporting requirements for all programs within the company. Finally, all programs are obligated to report potentially generic or systemic issues to a central company function in order to identify possible alert or bulletin topics. Where the differences lie typically is in the customer reporting requirements and how the programs deal with suppliers on alerts. This "leveling" across the classes is reflected in the matrix.

One area where the "general" comments do not apply is in the cases where Class D programs are executed by companies other than the typical aerospace contractors (e.g., universities or similar academic institutes). These groups are typically not part of the GIDEP system, nor are they large enough to require an internal bulletin process or database. In these cases, the customer or spacecraft "host" would provide significant alert issues to the programs for a more informal assessment.

The matrix in this section is structured to decompose the various Alert and bulletin process elements, and identify where four mission classes differences typically exist.

C3-2 Definitions

Definitions are provided to guide the reader in interpreting the mission risk class process matrix, establishing a basis from which risk profile can be developed and are not intended as general standalone industry standard definitions.

Alert. In the context of this document, alert is used to describe one of the Failure Experience Data documents (i.e., Alerts, Safe Alerts, Problem Advisories, or Agency Action Notices) produced by the GIDEP system. Alerts document problems encountered by member companies or government agencies that are generic in nature and pose risks if the issue is not addressed.

Bulletin. In the context of this document, a bulletin is used to describe a government agency or company produced document to identify a generic/systemic issue or lessons learned that the agency or company believes all programs within their sphere need to be aware of and/or take action. Government agency examples would include MDA or NASA advisories, while each company would have various internal bulletins or lessons learned that would be produced in accordance with company policies.

Government/Industry Data Exchange Program (GIDEP). A cooperative effort to exchange research, development, design, testing, acquisition, and logistics information among government and industry participants. GIDEP seeks to reduce or eliminate expenditures of time and money and to improve the total quality and reliability of systems and components during the acquisition and logistics phases of the life cycle. (Note: definition taken from the GIDEP Operations Manual.)

C3-3 Matrix – Alerts, Information Bulletins

Requirement	Class A	Class B	Class C	Class D
Receipt and Distribution				
External Alert (GIDEP, NASA, MDA, Other) Receipt External Alert Screening External Alert Distribution Internal Alert/Bulletin Distribution	• Company receives Alerts from external source (GIDEP, NASA, MDA, SQIC, Other) • Company performs screening to remove non-pertinent Alerts • External Alerts distributed throughout company • Internal Alerts/Bulletins distributed throughout company	• Same as Class A	• Same as Class A	• Same as Class A
Evaluate and Take Action				
Identify Usage (Parts Lists, Procurement Records) Assess In-Line Screen Effectiveness Assess Impact and Risk for Use Initiate Action to Mitigate Risk	• Review of program as-designed or as-built parts lists for suspect parts • Procurement records reviewed to determine whether suspect parts purchased • If use identified, program performs assessment of in-line screens, impact to component/system, and associated risks • Program takes action to mitigate risks (e.g., remove suspect parts, add further screens, add fault protections)	• Same as Class A	• Same as Class A	• Same as Class A

Requirement	Class A	Class B	Class C	Class D
Document and Review Response				
Document Usage and Impact Assessment Independent Review and Approval of Response Close Alert Response	• Document Alert closure rationale in program or company database • Program closure reviewed and approved by independent (non-program) personnel per company process	• Same as Class A	• Same as Class A	• Same as Class A
Report Program Alert Status				
Customer Report (CDRL) Company Report (e.g., CAB, Program Reviews)	• Report Alert review status per contractual requirement • Report Alert review status at various internal reviews per company process	• Same as Class A	• Same as Class A	• Alert review status typically not a customer requirement • Report Alert review status at various internal reviews per company process
Supplier Action				
	• Use suppliers that are GIDEP members to extent possible • Include contractual requirement to respond to any Alert/Bulletin provided to supplier • As-built parts list included at time of component delivery • Require large suppliers to provide Alert/Bulletin formal status reporting as a CDRL (optional)	• Use suppliers that are GIDEP members to extent possible • Include contractual requirement to respond to any Alert/Bulletin provided to supplier • As-built parts list included at time of component delivery	• Use suppliers that are GIDEP members to extent possible • Include contractual requirement to respond to any Alert/Bulletin provided to supplier (optional) • As-built parts list included at time of component delivery	• Same as Class C

Requirement	Class A	Class B	Class C	Class D
Identify New Issues				
FRB Findings MRB Actions Non-conformance Trends	• Assess FRB findings for potential generic/systemic problems that meet internal or GIDEP Alert criteria • Review product MRBs and non-conformance trends for generic/systemic issues that meet internal or GIDEP Alert criteria	• Same as Class A	• Same as Class A	• Same as Class A
Release New Alerts				
Issue Internal Bulletin Issue GIDEP Alert Issue SQIC Advisory or Other External Bulletin	• Internal Bulletin prepared and released per company requirements • GIDEP Alert prepared and released through GIDEP Central • SQIC advisory or other external bulletin released through the required mechanism	• Same as Class A	• Same as Class A	• Same as Class A

C3-4 Summary of Risk Classes

Class A. Alerts and information bulletins on Class A programs would be treated in the same manner – as potential risks that warrant thorough review and a well-documented assessment of impact. The review would include an examination of as-designed and/or as-build parts lists, an evaluation of in-line screens for those parts that were used, and the component and system impact where screens were inadequate. The response for usage would be like most on Class A programs; take the action that produces the least practical risk. Actions would be taken to ensure that hardware provided by suppliers had an assessment equivalent to that on in-house built components. Suppliers that are already on GIDEP Alert distribution would be preferably chosen, contract language would include a requirement to have the supplier response to any alert or bulletin from the contractor, as-built parts lists would be delivered with the hardware, with an option for the supplier to provide a periodic alert response status. The customers for Class A programs levy requirements to perform the alert/bulletin reviews and to provide periodic (typically monthly) status. Company command media also requires periodic status of alert responses. As new issues were identified that met either the GIDEP or internal company requirements, the program would follow the processes to issue alerts or information bulletins.

Class B. The approach taken for Class B programs will be very similar as for Class A relative to alerts and information bulletins. The programs would receive, review, assess, and document their conclusions in the same manner (and likely in the same or similar database) as Class A programs. The data review expectations would be similar, as they would be dictated by company policy. The ultimate response in the event that usage is identified could differ, as the ultimate risk profile could allow for parts use when a Class A program would replace the suspect part. The treatment of suppliers could differ, in that the Class B program could delegate the requirement for alert and bulletin processing to the supplier without receiving full feedback (i.e., only be informed if an impact exists). The Class B program customer will levy a requirement to perform GIDEP alert review, but may not mandate periodic responses. Company status reporting rules would still apply. The process for alert/bulletin-worthy issues identified on the program would be identical to that of Class A programs, as all programs would have an obligation to process new concerns through the company/GIDEP procedures.

Class C. Unlike most of the other sub-processes, there is not a significant breaking point between Class C programs and those that mandate lower risk profiles when it comes to alerts and bulletins. Since the requirements to perform and document the assessments flow from company policy, Class C programs would execute the task in a similar manner the Class A and B programs. Reviews would occur and be documented in the company database. Suppliers would be supported either by being made responsible for all alert/bulletin reviews, or (more often) providing parts lists so that the program could perform the assessments. The actions taken where usage was identified would be consistent with the overall mission risk profile. The contract from the customer would include a requirement for GIDEP review, but a formal status report would be unlikely. New issues that warrant an alert or bulletin would be expected per GIDEP/company requirements.

Class D. Even though Class D programs are performed to a higher risk profile, it is unlikely that relief would be given to alleviate alert/bulletin processing. The primary reason for this is that a mission failure caused by a known, documented condition is an unacceptable result to nearly all companies regardless of the risk profile. Therefore, Class D programs would process alerts and bulletins to the company's requirements. The customer, however, may not mandate GIDEP requirements on the program, and even if levied, would not expect or require a documented response or status update. The program would perform the alert review response for supplied hardware in the most cost effective manner (likely receiving parts lists and performing the assessment themselves).

However, as with any program, is a new generic/systemic issue is identified that warrants an alert or bulletin, the program would be responsible to process the document in accordance with GIDEP or company standards.

C3-5 Effectiveness Tips

- Including people who must respond to Internal Bulletins in the draft Bulletin review process will lead to documents, which are more readily "action-able".
- The earlier a program can complete its "as-built" parts list, the better it is for Alert responses.
- By establishing, communicating, and enforcing a minimum expectation for Alert closure rationale, the usefulness of the Alert data will extend into the mission operations phase.
- A program should consider establishing clear roles and responsibilities for Alert response early in the program life cycle (preferably prior to processing the first document).
- Clearly communicating Alert/Bulletin review requirements with suppliers at contract initiation will yield big dividends throughout the program life cycle (even after the supplier delivers the product).
- The Parts, Units, Materials, Process, Subassemblies, and Processes (PUMPS) application provides the user capability to create component, manufacturing, or process advisories and notification of key personnel regarding new content and changes pertaining to spacecraft parts defects or failures. This application helps users to maintain awareness of issues that impact project scope and performance and email is used for notification of new or updated advisories.

C3-6 References

1. MIL-STD-1556B, Government/Industry Data Exchange Program (GIDEP), 24 Feb 1986.
2. Contractor Participation Requirements
3. SO300-BT-PRO-010, GIDEP Operations Manual, September 2009.
4. SO300-BU-GYD-010, GIDEP Program Requirements Guide, April 2008.
5. Aerospace Report TOR-2010(8591)-18, Mission Assurance Program Framework, (2010 MAIW).

Appendix D: Risk Balance Critical Evaluation Methodology

David Pinkley (Ball Aerospace)

Performing a critical evaluation for a given acquisition requires detailed programmatic, funding, and mission requirements discussions between the acquisition agency and the contractor(s). The objective of the evaluation is to achieve the optimal development architecture given programmatic constraints and mission needs. Figure D-1 identifies key drivers in this risk balancing evaluation. Acquisition planning will capture the type of mission, whether operational or experimental for NSS or flagship, discovery or technology demonstrator for NASA. In support of this mission type other procurement documents will capture specific mission requirements, mission environments, and other programmatic objectives. This acquisition baseline must be aligned with the funding strategy and assignment of buyer and seller risk. Buyer risk is often associated with missions involving new development, a malleable requirements baseline, and minimum practical risk in a cost plus contract. Seller risk is often associated with firm baseline requirements, heritage development, and low to moderate risks in a fixed price contract.

Both the programmatic baseline and its funding strategy must be in alignment with an achievable development baseline that effectively manages risks to mission success including performance, robustness, implementation, and operations risks. The mission class process execution matrices presented in the first three appendixes of this document serve as the foundation for developing an optimal risk strategy given programmatic constraints. Figure D-1 highlights how the acquisition baseline, including the funding strategy, together with the mission class matrices of typical process execution is the input data for management of risk uncertainty and achieving an optimal risk balance. The risk surface at the bottom of D-1 is examined in detail in Figure D-2 in development of this risk balance methodology.

The focus of this section is on “Risk Balance”. That is, coming up with the optimal set of process execution to maximize the probability of mission success given the program constraints in a given risk profile. Figure D-2 shows a visualization of a risk surface for balancing the key factors for mission success. In this figure various factors that affect risk are depicted as “spokes” arising from a central area termed the minimum practical risk area.

Each spoke has the lowest possible risk near its point of origin, so the innermost surface, (Class A), as the lowest risk exposure to mission success. As resource tradeoffs are made, i.e., as one moves out a radial spoke, risk increases and the risk surface expands. The diagram can be used to visualize various tradeoffs that are possible for a given mission class profile.

Table D-1 provides a legend for the risk surface listing each of the radial spokes chosen for this risk surface and the vector characteristics of each spoke from minimal practical to higher risk profiles with typical A-D mission class profiles capturing characteristics typical for that profile. The risk spokes chosen are representative of both MA framework mission success processes and key development characteristics for a given mission. It should be noted, much as the MA framework mission success processes are significantly interrelated, these spokes and development characteristics are also interrelated and not independent. For example, if an unproven team represented on one vector worked on a low TRL, another vector, the probability of success will likely suffer. However, if a proven team works on a less complex system, the MA focus can be reduced. This is typically the case for heritage-based missions in which many MA products are a priori integrated into the development effort.

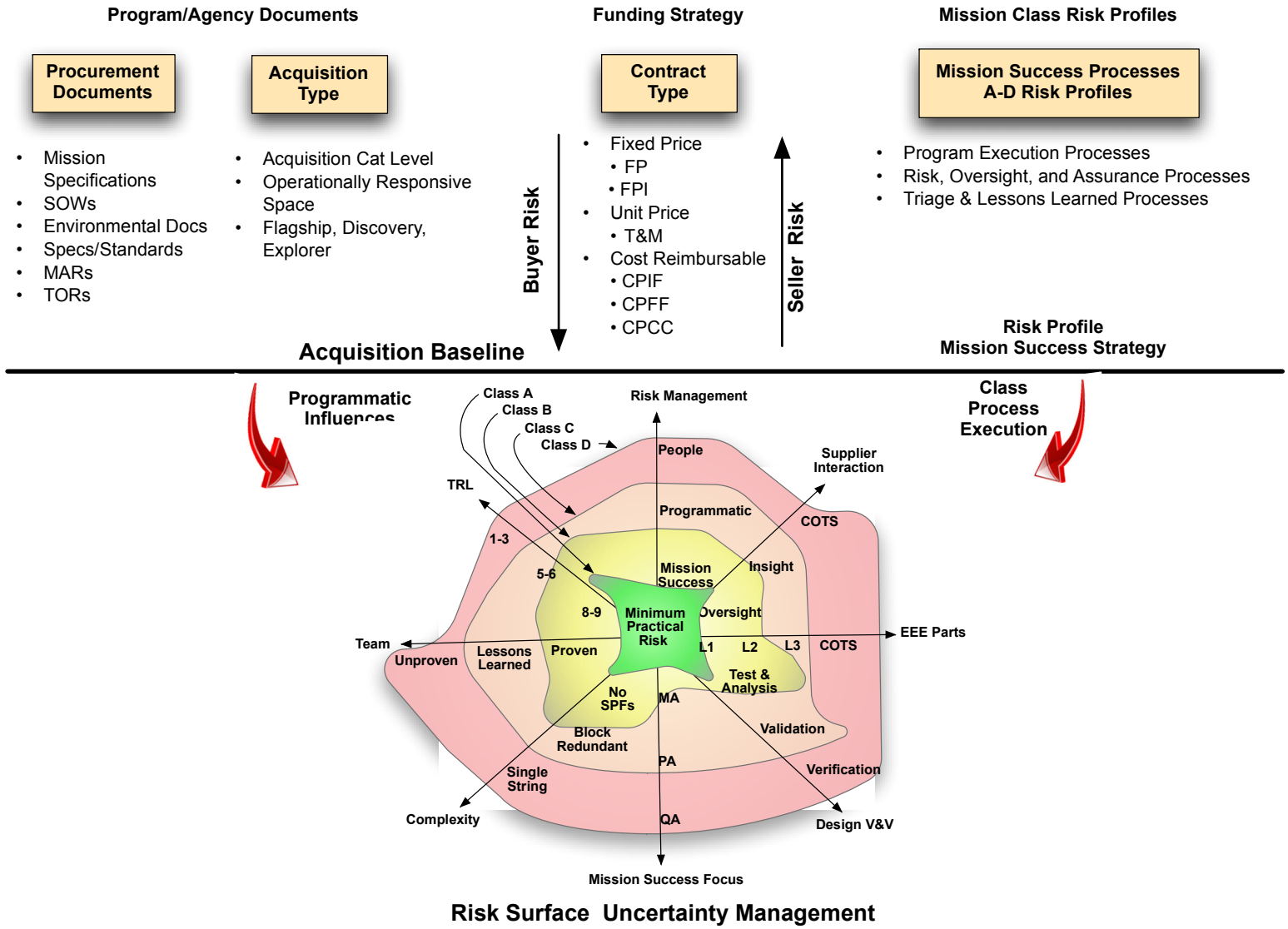


Figure D-1. Drivers for risk balance critical evaluation.

The legend spokes generally cover 8 of the 16 mission success processes addressed in the appendixes *as products of that processes application*. Moving clockwise from 12 noon the risk surface includes Risk Management; Supplier Interaction; the EEE parts element of PM&P; the Design V&V process performed during Integration and Test; Mission Success as a higher-level abstract of the Design Assurance and Hardware/Software Quality Assurance functions; and Reliability evaluation of redundancy versus Design for Minimum Risk (DFMR) as a complexity measure. These process application risk products complement the team and TRL spokes which are givens due to programmatic and technical constraints that must be balanced in the design.

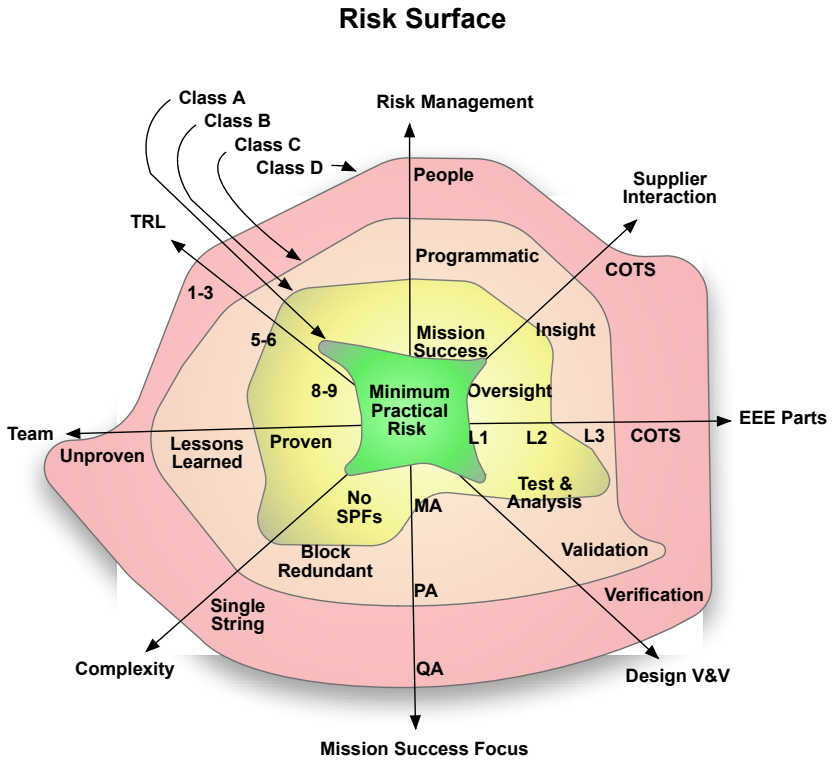


Figure D-2. Mission risk class surface.

Table D-1. Mission Risk Class Surface Legend

Mission Risk Class Surface Legend	
Radical Spokes	**Vector Characteristic**
Risk Management	• **People**: Risk Process Informal, Sparse documentation • **Programmatic**: Risk Process cost/schedule/technical focus • **Mission Success**: Programmatic Plus Residual Risk Management
Supplier Interaction	• **COTS**: Buying product as catalog item with little data • **Insight**: Formal Data available throughout development • **Oversight**: Customer/Supplier interactive development
EEE Parts	• **COTS**: Consumer commercial and Industrial Grade • **L3**: Hi-Rel parts with screening but little qualification data • **L2**: Military grade parts will full screening and Qual program • **L1**: Space grade parts with delta screening and qualification
Design V&V	• **Verification**: Ensuring compliance to requirements • **Validation**: Additionally ensuring product meets mission needs • **Test and Analysis**: Life-cycle build-up of V&V artifacts
Mission Success Focus	• **QA**: Verification of process and product integrity • **PA**: Reliability and Quality built into the product • **MA**: Systems management of processes supporting mission success
Complexity	• **Single String**: Simplex assemblies performing mission • **Block Redundant**: Parallel active and standby assemblies • **No SPFs**: No simplex assemblies beyond DFMR items
Team	• **Unproven**: New team without mission class experience • **Lessons Learned**: Promulgation of lessons throughout • **Proven**: Experienced team with mission class in development
TRL	• **1-3**: Basic principles to proof of concept • **5-6**: Environmental Breadboard to Prototype • **8-9**: Flight Qualified to Mission Operations

Risk balance trades that can be visualized using the risk surface include:

1. **Risk Management.** Management of cumulative residual risk in addition to programmatic risk.
2. **Supplier Interaction.** Supplier dynamic review through continual risk evaluation versus heavy oversight.
3. **EEE Parts.** Class C and D, L3 and COTS parts respectively risk controlled via rigorous assembly level qualification.
4. **Design V&V.** Scenario, Stress, confidence verification to validation.
5. **Mission Success Focus.** Upfront process qualification versus 100% inspection.
6. **Complexity.** (a) Design for minimum risk versus redundancy tradeoffs; (b) Cross-strapping complexity vs. block redundancy.
7. **Team.** Lessons learned promulgation seasoning of developmental team.
8. **TRL.** Heritage design enveloping of the requirements baseline.

The point of this figure is that a broader system view of risk is needed to choose the best risk mitigation options for a given program with its programmatic and mission constraints. In essence risk balancing follows the governing principle of conservation of energy (program resources), to achieve the optimal balance for mission success.

Figure D-1 identifies some of the key vectors that can be dialed up or down within a given risk profile in order to achieve a balanced and optimal risk strategy for given program constraints. Risk balance

decisions should be based on the management of uncertainties. Uncertainties can lead to both mission success risks and given how those uncertainties are managed opportunities. These risk and opportunities require risk mitigation or opportunity exploitations. Given an optimal mitigation or exploitation the outcomes will be increased reliability, robustness, versatility, flexibility, resolvability and interoperability.

Figure D-3 shows this chain of events in management of uncertainties in the achievement of mission objectives. The figure shows the well-known stages of risk and opportunity management from the typical progression of uncertainties (i.e., the initial mission development environment), to the identification of mission risks, followed by risk handling (mitigation, acceptance, transfer), and then followed by an improved environment of end state from a risk perspective. This diagram represents the classic flow of risk management. The questions is "Does this risk balance focus on uncertainty management change how the classic process is executed?" and the answer is no. It's just that the emphasis is on management of residual risk, which is an element of the classical process. For instance the classical 5X5 risk cube ratings for likelihood and consequence should remain constant over the Mission Risk Class profiles. For the higher risk profiles there will potentially be yellow and even red risks at launch. The key is risk understanding and eliminating the uncertainties as much as possible within the constraints of the program. The yellow and red risks in the higher risk profiles should still get the same attention but the burn-down mitigations may be limited since more residual risk is left on the table.

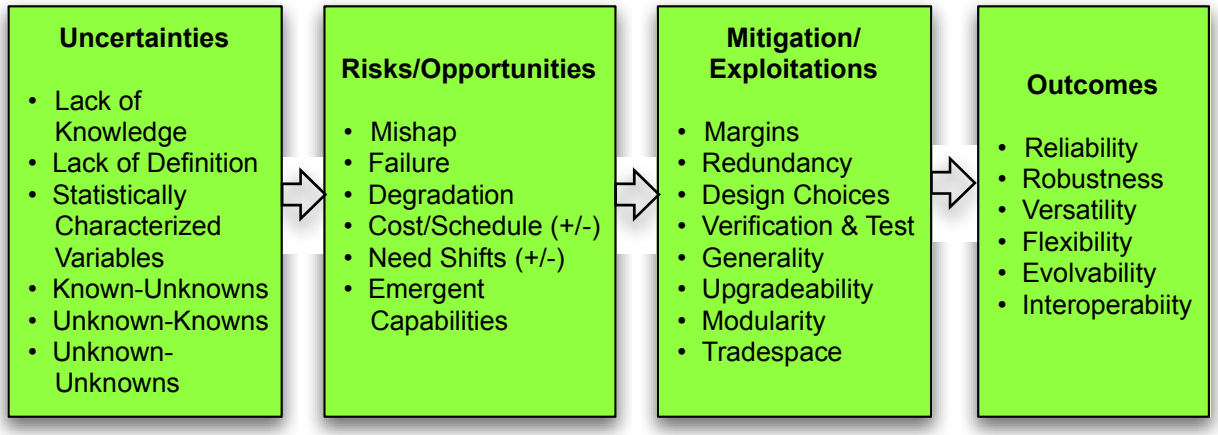


Figure D-3. Uncertainty management achieving optimal outcomes.

The risk identification and opportunity identification, risk/opportunity handling, risk management outcomes, blocks two through four in the figure are well defined elsewhere and will not be covered in more detail here. The focus is on the first block, uncertainties, which must be managed properly, in order to develop an effective risk balance strategy.

The first three uncertainties in the D-3 Uncertainties figure are well known common developmental items. Lack of knowledge represents the uncertainty that is systematically reduced with developmental analysis and test activities. Lack of definition represents open item uncertainty managed through program planning to layout. Throughout the life cycle these uncertainty types can be defined to build up and support a balanced design and development. Statistically Characterized Variable uncertainty represents uncertainty in the precise value of variables that can be either statistically characterized or at least bounded.

The last three uncertainties in the D-3 figure are much more insidious, lack of knowledge special case items that lead to the range of failures in space systems that we see. These are *Known-Unknowns, Unknown-Knowns, and Unknown-Unknowns*. These three types of uncertainty types must be dealt with adequately during the design and development of a space system to ensure achievement of mission success beyond being lucky.

Table D-2 lists these three uncertainty types along with ***known-knowns***, which represents the optimal risk management objective of retiring risks through adequate operational data, scenario validation, demonstrated performance across all key TPMs, and the build-up of verification and validation artifacts.

Table D-2. Special Case Lack of Knowledge Uncertainty Risks and Mitigations

Retired Risks	No Residual Risk	Artifacts
Known-Knowns *Risk Artifacts*	• Operational Flight Data • Test-As-You-Fly Validation • Demonstrated TPM Performance • Flight or test-validated analysis, simulations, and models • Operation within validated limits	Life Cycle program build up of incremental knowledge with full verification and validation
Open Risks	**Open Residual Risks**	**Risk Handling**
Known-Unknowns *Accepted Risk*	• Analysis/test limitations • Unverified predictions from models/simulations • Envelope expansion and operations without validation • Unverified failure modes and hazards	Evaluate technical baseline limitations; margin gaps in enveloping requirements; incomplete verification and validation; insufficient analysis thoroughness. Perform delta assessments to fill in knowledge gaps.
Unknown-Knowns *Execution Risk*	• Miscommunicate test/analysis results • Uneven understanding of data/environment • Poor documentation combined with loss of corporate memory	Establish good program communications/data sharing; Incremental build-up of program knowledge with trending
Unknown-Unknowns *Unknown Risk*	• Bad assumptions • Unfinished foundation research • Untested new environments • Inadvertent operations outside of limits	Demonstration of TRL level 6 by PDR; Rigor in environmental analysis and testing supported by appropriate fidelity simulators and test-beds and TLYF with appropriate redundancy and margins verified and mission validated

Known-Unknowns are uncertainties that are *known not to be known*. They are at best bounded or may have entirely unknown values. The objective of this risk balance effort is to characterize risk in this category statistically with time and/or effort using, at a minimum, semi-analytical or qualitative methods. Risks that fall in this category become manifest in Class C and Class D risk profiles when the program execution standards are lowered including reduction of analysis and test, unjustified predictions, use of heritage technical baseline beyond their qualification envelope, and undemonstrated or analyzed failure modes and hazards. Critical evaluation must be performed to understand gaps due to these limitations and delta assessments to achieve a balanced risk profile with sufficient knowledge of the accepted residual risks.

Unknown-Knowns are uncertainties that are *unknown due to poor execution but for which data exists to mitigate the risk*. The objective of the risk balance effort is to ensure that minimum standards are adhered to ensure all input products - mission requirements and environmental knowledge, and

output products - analysis and test results, are communicated to all owners and properly documented to ensure traceability. This is reflected in mission classes with the roll-off of risk management, customer and internal oversight/insight, and assurance processes which are responsible for assuring that all available data is used to surface and bound risks to mission success.

Unknown-Unknowns are *uncertainties that by definition are not known*. This is reflected in space vehicle design in which redundancy and design margins are used to handle random failure rates and uncertainty in margins or their corresponding environments. This may result in continuous long-term exceptions, intermittents, or periodic anomalies as the case of solar mass ejections, which are dependent on the correspondence of the mission within the solar cycle. Mission classes, especially Class D, are very susceptible to unknown-unknowns due to their minimum assurance standards. Assurance planning should focus on contingencies whether on the ground or on-orbit to mitigate the largest classes of unknowns; for instance, lack of knowledge about commercial-off-the-shelf part behavior in the natural space environment.

In summary, a risk balance methodology should be followed in the application of any of the appendix process matrices that provide typical process execution for a given mission class. The matrices should be used as a starting point of typical process execution as an input to a critical evaluation of mission and programmatic constraints with the resulting output of an optimal process execution and risk strategy for the design and development effort. This balance will be a recursive effort looking at risk exposure throughout the design and development activities and using available knowledge to refine the risk balance strategy. The product of this risk balance effort will provide a program and mission risk signature that should be communicated both internally and outside the program to demonstrate how risk is being managed as a resource.