AEROSPACE REPORT NO.
ATR-2023-01889

Mission Assurance Guidelines for Mission Risk Classes and Do No Harm (DNH) for Space Vehicles

December 15, 2023

Jeff B. Juranek
Enterprise Systems Engineering
Corporate Chief Engineer's Office

and

Lisa J. McMurray and Ryan P. Rairigh, Lockheed Martin Space
Tara M. Abou Assi and Steven J. Bullock, The Boeing Company
Mark L. Baldwin, Raytheon
Jesse A. Leitner, NASA Goddard Space Flight Center

Prepared for:

General Manager, Corporate Chief Engineer's Office

Authorized by: Corporate Chief Engineer's Office

Developed in conjunction with Government and Industry contributors as part of the U.S. Space Programs Mission Success Improvement Workshop.

Foreword

This document was produced under the auspices of the Mission Success Improvement Workshop (MSIW) in 2023. A multidisciplinary team representative of government, industry, and partners of The Aerospace Corporation was assembled in order to provide a needed update to the mission risk class body of knowledge. Since the publication of *Mission Assurance Guidelines for A-D Mission Risk Classes* (Aerospace Report No. TOR-2011(8591)-21) [1], many lessons learned have been collected from tailoring mission assurance on new acquisitions. A number of technological changes have shifted the desired architectures towards proliferated systems that support increased resiliency while leveraging the reduced cost to launch. Significant knowledge and experience have been acquired since the release of TOR-2011(8591)-21, and it was the intent of this team to capture these learnings and provide a meaningful revision to it.

This report (Aerospace Report No. ATR-2023-01889) represents a thoughtful update to the technical content of TOR-2011(8591)-21 [1]. While the original team identified 16 mission assurance framework processes, this MSIW team has:

- Redefined the mission risk class profile key characteristics based on technical criteria instead of programmatic criteria
- Updated the MA framework category names
- Prioritized the framework processes based on technical importance
- Updated five of the original framework processes (contained in the appendices)
- Eliminated the design assurance process from the list of 16 framework processes, resulting in 15 framework processes
- Added guidance for the management of a sub-Class D mission risk profile, defined primarily by the requirements in *Rideshare Mission Assurance and Do No Harm Process* (Aerospace Report No. TOR-2016-02946-Rev A) [25], for “Do No Harm” instead of the process practices of the specific mission risk profiles defined herein.

The original mission risk class profiles in TOR-2011(8591)-21 [1] contained a matrix with 11 key characteristics that contained a “patchwork” of mostly programmatic elements. While the matrix was important from a “big picture perspective,” this MSIW team sought to focus on more “mission-related” characteristics that are more impactful for early tailoring discussions. Five new key characteristics have been defined with greater details to guide an acquisition team in making mission tradeoffs that have more technical impact.

When TOR-2011(8591)-21 [1] was released, it contained 3 mission assurance categories with 16 framework processes. After considerable review and discussion by the MSIW team and a look back at how this information has been utilized (in industry and by the government) since its release, it was decided to create four categories and update the top-five most important framework processes, which would be the focus for the scope of this update. The other chapters and appendices for the remaining framework processes were not updated as part of this workshop but could become part of a future MSIW. For the five framework processes selected, they were substantially updated with new information in the appendices. It should be noted that the updated criteria in the appendices are provided as guidance and are not requirements.

Acknowledgments

This document has been produced as a collaborative effort of the MSIW. The MSIW forum was organized to enhance mission success processes and support disciplines through collaboration between industry and government across the U.S. space program community, utilizing an issue-based approach. The process is to engage the appropriate subject matter experts to share best practices across the community in order to produce value-added mission assurance guidance documentation.

This document was created by multiple authors throughout the government and the space industry. For their content contributions, the following team members are acknowledged for making this collaborative effort possible:

Tara M. Abou Assi	The Boeing Company
Chahriar Assad	The Boeing Company
Steven J. Bullock	The Boeing Company
Lisa J. McMurray	Lockheed Martin Space
Ryan P. Rairigh	Lockheed Martin Space
Kevin T. Boyle	The Boeing Company
Eli Minson	Maxar
Ron Langlais	Maxar
Harold J. Martinez	Northrop Grumman Space Systems
Mark L. Baldwin	Raytheon
Jesse A. Leitner	NASA Goddard Space Flight Center
Michael S. Marlow	Space Systems Command
Vinay Goyal	The Aerospace Corporation
Mark J. Mueller	The Aerospace Corporation

The team would like to thank the steering team champions for their assistance, direction, and insight:

Ryan W. White	Lockheed Martin Space
Dan K. White	Northrop Grumman Space Systems
Barbara M. Braun	The Aerospace Corporation
Mark J. Silverman	The Aerospace Corporation

Finally, this team would like to acknowledge the original authors from the 2010 Mission Assurance Improvement Workshop (MAIW) that created TOR-2011(8591)-21 [1], which is the basis for ATR-2023-01889.

Document History

Revision No.	Title and Description of Change	Effective Date
TOR-2011(8591)-21	Aerospace Report TOR-2011(8591)-21, *Mission Assurance Guidelines for A-D Mission Risk Classes* • Initial release (original document)	June 3, 2011
ATR-2023-01889 draft Stakeholder review	Aerospace Report ATR-2023-01889, *Mission Assurance Guidelines for Mission Risk Classes and Do No Harm (DNH) for Space Vehicles* • Updated base document TOR-2011(8591)-21 to ATR-2023-01889 to reflect more than 12 years of lessons learned and technology changes with respect to mission risk classes experience • Changed title to make focus on space vehicles • Clarified document revision letter references • Added rationale for removing design assurance MA process (duplicative and inconsistent) • Made appendix headings more specific to MA process • Added definition for failure modes and effects analysis (FMEA) in Appendix A, System Safety • Added definition for "Maintainability and Operational Reliability" in Appendix B, Reliability • Added section to address implementation or use of document • Updated references throughout document with latest revisions • "Requirement and shall" statements have been removed since the intent of this document is for guidance only • Added document history summary • Minor formatting and grammatical fixes throughout	October 15, 2023
ATR-2023-01889 (this document)	Aerospace Report ATR-2023-01889, *Mission Assurance Guidelines for Mission Risk Classes and Do No Harm (DNH) for Space Vehicles* • Initial release (new document)	December 15, 2023

Disclaimer

Note: ATR-2023-01889 is for guidance only and should not be cited as compliance. This document will aid in the development of the program risk profile based on mission needs.

Executive Summary

This document is a team product from the 2023 Mission Success Improvement Workshop (MSIW) 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, D, and Do No Harm [DNH]) to serve as a recommended technical baseline suitable to meet program objectives based on programmatic constraints and mission needs. This document leverages the 2010 Mission Assurance Improvement Workshop (MAIW) product, *Mission Assurance Program Framework* (Aerospace Report No. TOR-2010(8591)-18) [4], 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, often without sufficient guidance on the characteristics and requirements for those different classes. The early lifecycle establishment of a 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 and DNH for U.S. space programs, considering factors that include criticality to a specific government agency's strategic plan, national significance, availability of alternative opportunities, success criteria, investment, and mission life. Mission risk class profiles are based on NPR 8705.4, "Risk Classification for NASA Payloads"; DOD-HDBK-343, "Design, Construction, and Testing Requirements for One of a Kind Space Equipment"; and the mission risk posture assessment (MRPA) criteria found in *Mission Risk Posture Assessment Process Description* (Aerospace Report No. ATR-2015-03151), outlining requirements for 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. The mission risk Class D represents the **highest risk** profile, typically for experimental missions of one year or less and more fully shifts development to contractor best practices with no government oversight. This revision offers guidance for the management of a sub-Class D mission risk profile, defined primarily by the requirements in *Rideshare Mission Assurance and the Do No Harm Process* (Aerospace Report No. TOR-2016-02946-Rev A) [25], for "Do No Harm" instead of the process practices of the specific mission risk profiles defined herein. This category harmonizes with the NASA philosophy of a sub-Class D DNH category for which mission failure is not considered a formal mishap.

These guidelines define 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, D, and DNH) 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 original document, *Mission Assurance Guidelines for A-D Mission Risk Classes* (Aerospace Report No. TOR-2011(8591)-21) [1], was established to define typical practices to ensure mission success across the mission risk classes (A, B, C, or D) that align with the programmatic and technical constraints combined with the stakeholder desire for government involvement in development. Mission risk class profiles are aligned with technical and quality attributes and approaches that impact mission success. Execution risk associated with acquisition program cost and schedule is only indirectly addressed in this document. This updated 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.

Mission assurance (MA) as adopted by these guidelines is defined in *Third United States Space Program Mission Assurance Summit Overview* (Aerospace Report No. TOR-2011(8591)-9) [2], which contains the Mission Assurance Strategic Intent approved by National Aeronautics and Space Administration (NASA), Missile Defense Agency (MDA), and Space and Missile Systems Center (SMC) (now Space Systems Command), and other U.S. government agencies. 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 15 of the 16 processes defined by the 2010 Mission Assurance Improvement Workshop (MAIW) product, *Mission Assurance Program Framework* (Aerospace Report No. TOR-2010(8591)-18) [4], for their support in achieving mission success. The appendices of this updated document provide tables and summaries of typical execution of the MA framework processes supporting mission success, with updates to five of the most critical MA framework processes. The material presented should not be a standalone reference but a starting point for developing the program's risk strategy given mission needs and programmatic constraints. The 15 processes included both core (key drivers to mission success, independent of organizational construct) and supporting (verification processes/activities executed within the performing discipline to verify work product or process integrity prior to completion). The core and supporting processes together form 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.

The mission risk classes A through D and Do No Harm (DNH) establish a hierarchy for the U.S. space programs considering factors such as criticality to a specific government agency's or other customer's mission objectives, mission risk mitigation priority, mission significance of individual asset, mission life of individual asset, and customer engagement level.

NPR 8705.4, "Risk Classification for NASA Payloads"; DOD-HDBK-343, "Design, Construction, and Testing Requirements for One-of-a-Kind Space Equipment"; and GPR 8705.4, "Risk Classification Guidelines and Risk-Based SMA Practices for GSFC Payloads and Systems" have been leveraged to define basic risk mission classes and success criteria. In addition, this document is a companion document to *Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles* (Aerospace Report No. TOR-2011(8591)-5) [5]. The intended audience for the Aerospace document is government program offices and the contractor community who 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 assurance 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 and how many options there are within the overall project or program to achieve associated objectives. When applying requirements across mission assurance risk classes, it is key to realize that mission assurance may not be uniform across subsystems, elements, segments, or mission events. It is critical to select the appropriate mission assurance risk class that most suitably balances the risk for the system design and program execution approach. For example, a mission assurance Class C or D program may accept higher residual risk for many program aspects. However, there are typical areas that warrant a lower residual risk (more Class A) position. These may include:

- Where required by government or regulatory requirements (e.g., disposal, launch safety, etc.)
- Where failure would prevent achieving fundamental mission goals
- Where DNH requirements establish a lower risk posture (see TOR-2016-02946-Rev A for more details [25])

It is important to note that while, in general, the tolerance for risk goes down while stepping from DNH and Class D up to Class A where the volume and stringency of practices recommended are increased, the managing organization should not assume a monotonic reduction in risk (or consequential increase in system reliability) simply by employing the higher practices. The practices are designed based on risk trades that are aligned with the particular classification, rather than absolute reduction of risk, and if practices are inconsistent with the programmatic or technical constraints, the result might be an overall increase in risk that occurs with a much higher use in resources. Furthermore, the classifications A and B tend to be more oversight driven (government controlled), while those below B are more insight driven (developer standard practices). The stakeholder should take these into consideration when classifying a 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 a risk class to specific mission category, such as flagship, discovery, and explorer missions.

Table 1. Existing Risk Classification Guidelines

Document	Scope
TOR-2010(8591)-18, *Mission Assurance Program Framework*, June 30. 2010	The Mission Assurance Program Framework was developed for the 2010 MAIW activity and resulted in the development of 16 common mission assurance processes across multiple contractors and Aerospace. These 16 common mission assurance processes were recommended as an essential set necessary for guidelines to provide effective mission assurance for U.S. space programs.
TOR-2011(8591)-5, *Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles*, September 13, 2010	These guidelines establish mission class tailoring of compliance documents and provide specific tailoring guidance to those documents in order to better map requirements to the spectrum of NSS acquisitions. TOR-2011(8591)-5 defines four mission risk classes consistent with this document.
TOR-2011(8591)-21, *Mission Assurance Guidelines for A-D Mission Risk Classes*, June 3, 2011	Contractors are required to respond to acquisitions specifying different mission risk classes with sufficient guidance on the characteristics and requirements for those different classes. Early in program lifecycle, the risk tolerance level is established and provides the basis for government and contractors to effectively communicate acquisition strategies and relevant requirements. TOR-2011(8591)-21 provides mission risk class profiles for A through D for U.S. space programs and considers critical factors based on the government's strategic plans.
DOD-HBDK-343, *Design, Construction, and Testing Requirements for One of a Kind Space Equipment*, February 1, 1986	DOD-HBDK-343 describes technical and program requirements for the design, construction, and testing of various classes of space equipment. It defines four payload classes (A through D). The requirements are a composite of those that have been found to be cost effective for one-of-a-kind space programs.
NASA Goddard Space Flight Center (GSFC) GPR8705.4A, *Risk Classification Guidelines and Risk-Based SMA Practices for GSFC Payloads and Systems*, June 13, 2022	GPR8705.4A establishes common assurance practices for GSFC-managed spaceflight projects based on the risk classification level determined by the stakeholder. The establishment of practices commensurate with the specified risk posture early in the project lifecycle provides the basis for program and project managers to develop and implement appropriate requirements, mission assurance practices, and risk management strategies to effectively communicate the acceptable level of risk to mission success.
NASA NPR 8705.4A, *Risk Classification for NASA Payloads*, April 29, 2021	NPR 8705.4A defines the criteria for NASA's mission directorates to define the risk tolerance classes for robotic NASA missions and instruments and the corresponding Agency-level assurance expectations that drive design and analysis, test philosophy, and common assurance.
ATR-2015-13151, *Mission Risk Posture Assessment Process Description*, September 29, 2015	ATR-2015-13151 establishes the risk posture assessment (RPA) process to characterize and document the space program's technical baseline utilizing best practices in 50 technical focus areas.
TOR-2016-02946-Rev A, *Rideshare Mission Assurance and Do No Harm Process*, February 28, 2019	The objective of the rideshare mission assurance (RMA) process is to provide all mission partners with a degree of certainty that all payloads included on a mission will DNH to each other or to any operational aspect of the launch.

1.3 Recommended Implementation of This Document

The intent of this document is to serve as a work product that government and industry partners could utilize and use individually and collectively with their new business/proposal teams to layout a framework for developing a risk profile understanding based on mission needs and risk posture. The document outlines the common expectations and language used to define the MA guidelines for mission risk classes and DNH for space vehicles.

This document was developed by industry and government personnel committed to finding solutions to new acquisitions that use the mission risk classes and DNH guidance criteria as a means of *achieving alignment* and creating a "win-win" approach to defining mission needs. This stands in comparison to the traditional approach of "throwing a bunch of specifications and standards over the wall" to see what resonates with industry contractors. New approaches and cooperation are needed to successfully navigate different mission risk profiles and more constrained cost and schedule needs.

Much has been learned in the more than 12 years since TOR-2011(8591)-21 [1] was published. The accumulated wisdom and acknowledgment that mission risk profiles are useful holds true more than ever as the government's approach to new acquisitions is changing. In turn, industry contractors are working hard to adapt these approaches and earnestly want to better anticipate these mission needs. Additionally, TOR-2016-02946-Rev A [25] on the DNH process has also added to the understanding of the mission risk classes as part of this accumulated wisdom.

All parties, whether industry or government, are challenged when defining a new mission. This document identifies guidance to aid in the risk posture development early in the program lifecycle and provides the basis for new acquisitions to develop appropriate requirements, mission assurance practices, and risk management strategies to help effectively communicate the acceptable level of risk to mission success.

The risk classification of any particular space vehicle, payload, subsystem, or unit is set by the program, so it is not a "one-size fits all" but rather can and should be adapted appropriately based on mission needs. There is flexibility in applying the mission risk profile approaches to various hardware levels. It is with this flexibility that the following logical uses for this document (ATR-2023-01889) are recommended:

- Prospective customers should use this document on new acquisitions as guidance only to better understand mission needs and not impose contractual compliance.

- Contractors should use this document to review their command media against the latest mission risk classes and DNH criteria to better understand expectations.

- All parties should use this document early in the program lifecycle to establish a common language between customer and contractor program teams for risk trade opportunities.

Ultimately, the expectations across the spectrum of classes serve the following purposes:

- Provide a starting point for MA requirements for each risk classification

- Provide a means for a program or developer to demonstrate that they are producing a product aligned with a given classification

- Help a customer convey to a developer what is meant by a given classification.

Implementation of this document can come in various forms, but a common flow could be as follows:

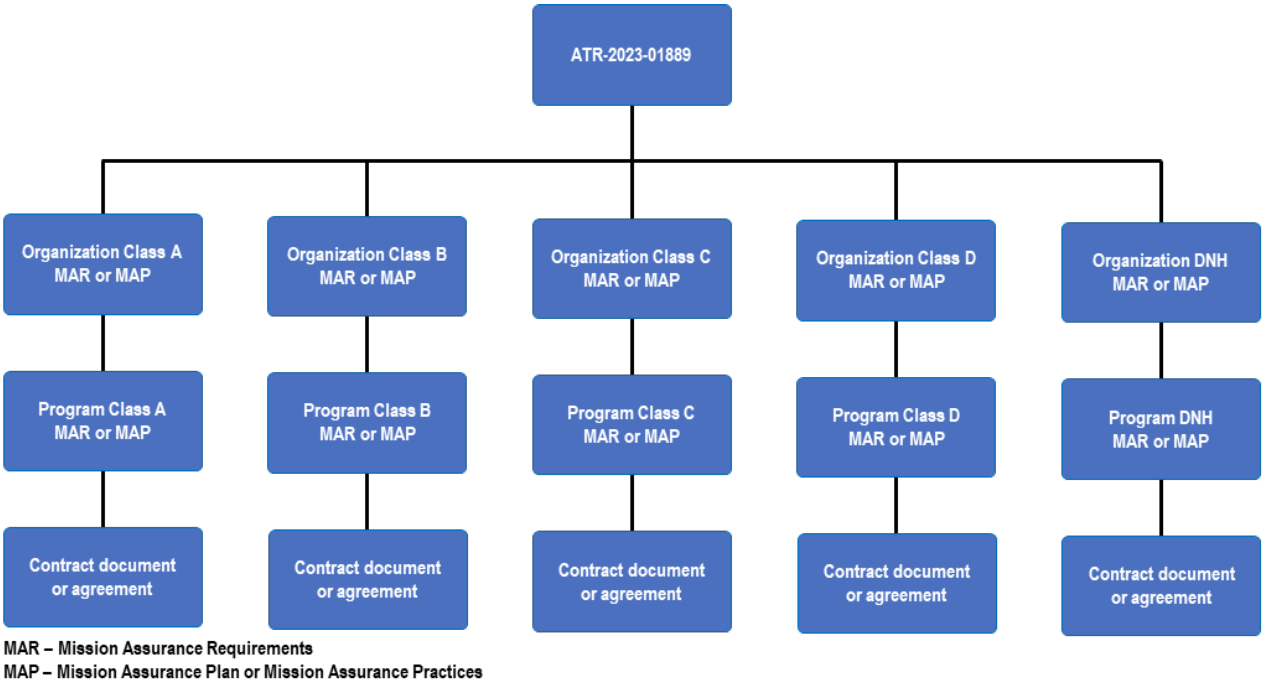
ATR-2023-01889
Organization Class A MAR or MAP
Organization Class B MAR or MAP
Organization Class C MAR or MAP
Organization Class D MAR or MAP
Organization DNH MAR or MAP
Program Class A MAR or MAP
Program Class B MAR or MAP
Program Class C MAR or MAP
Program Class D MAR or MAP
Program DNH MAR or MAP
Contract document or agreement
Contract document or agreement
Contract document or agreement
Contract document or agreement
Contract document or agreement
MAR – Mission Assurance Requirements
MAP – Mission Assurance Plan or Mission Assurance Practices

Figure 1. Recommended implementation approach for ATR-2023-01889.

This document could be used to create organizational templates for MA requirements, which would be the starting point for program-level requirements documents. Paragraphs from these requirements documents, or even the entire text, could then be copied into contracts.

2. Mission Risk Class Profile Key Characteristics

This chapter examines key characteristics of mission risk classes A through D and includes a sub-Class D mission risk profile, defined primarily by the requirements of TOR-2016-02946 [25] for DNH instead of the process practices of a specific mission risk class. This category harmonizes with the NASA philosophy of a sub-Class D DNH category for which mission failure is not considered a formal mishap.

The mission class profiles lay out a structural approach for defining a hierarchy of risk combinations for the U.S. space systems enterprise. Characteristic categories in Table 2 examine key programmatic and mission indicators with corresponding mission class considerations. Note that none of these characteristics are absolute. Each portrays representative characteristics exhibited by the risk class profiles.

The characteristics shown in Table 2 represent "new thinking" for the mission risk class profiles and place a deeper technical emphasis on "the mission" when compared with TOR-2011(8591)-21 [1], which contained a more general listing of programmatic attributes. The following paragraphs give further definition and explanation of each technical characteristic.

2.1 Mission Objective/Minimum Viable Mission Functionality (Availability/Performance)

This characteristic is determined by the customer's required availability and performance criteria and is the most important characteristic for determining the mission risk category. This characteristic defines what you are trying to accomplish for this mission to be considered successful.

2.2 Mission Risk Mitigation Priority (Failure Tolerance)

The mission risk mitigation priority is determined by the relative importance of three attributes of risk mitigation: cost, schedule, and technical impacts. Table 2 scores the most important attribute as 1 and the least important as 3. For example, a Class A mission risk profile identifies the mitigation of technical risk as being of primary importance to the customer, with mitigation of schedule and cost risks being of less importance to the customer, whereas a Class C mission risk profile prioritizes mitigation of schedule risk over cost and technical risk. This characteristic defines how much you can actually achieve out of what you're trying to do and still be considered successful.

2.3 Mission Significance of Individual Asset

This characteristic considers the effect of a constellation mission for which the customer is willing to accept degradation or loss of one or more individual assets provided that the overall mission goals are met. This does not insinuate that all constellation missions accept higher mission risk—the customer may determine that every asset in the constellation is critical to the overall mission. This also does not insinuate that every Class C or D mission consists of a constellation. For a Class D mission, the entire mission may be considered expendable.

2.4 Mission Life of Individual Asset

Mission life is a characteristic that must consider the mission environment, including expected radiation exposure and expected thermal environment/cycles for LEO, MEO, GEO, or interplanetary missions. Other environmental attributes, such as micrometeoroid/object detection (MMOD) or atomic oxygen (AO) exposure, may need to be considered. The mission life in these operational environments are major drivers to the design of individual assets, including electrical, electronic and electromechanical (EEE) component selection; thermal control systems and materials; and radiation survivability.

The individual asset’s life in years overlaps significantly between mission risk classes, especially for the middle categories. A mission sending a single asset to explore a planet for which the specific environmental attributes are not well known may have a two-year mission life and be identified as mission class B, while a GEO satellite might have a required mission life of 10 years for an individual asset and also be identified as mission risk Class B. In some cases, the mission life may be gated by a specific payload’s life limitations.

2.5 Customer Engagement

The customer engagement characteristic takes into consideration three elements of customer engagement with the contractor:

1. Contract data requirements lists (CDRLs)
2. Compliance standards
3. Customer approval on program control boards (engineering review board [ERB], change control board [CCB], PMPCB, failure review board [FRB], material review board [MRB], qualification review board [QRB], etc.)

Class A missions with significant customer oversight would expect to have a large number of data deliverables (plans and reports) all requiring customer approval, with a correspondingly large number of contractual compliance standards and customer approval required on a majority of program control boards. In contrast, a Class D mission would expect few to no compliance standards and no customer oversight of any control boards, and the only data requirement might be a final report. Customer engagement should be defined up front and negotiated, including consideration of contract type.

Table 2. Mission Risk Class Profiles

Characteristic	Class A	Class B	Class C	Class D	DNH
1. Mission objective/ minimum viable mission functionality (availability/ performance)	Mission of highest customer importance, unable to withstand degradation or loss of mission	Customer mission that can withstand some degradation or loss of mission capability provided overall mission goal(s) met	Customer missions that can withstand major degradation but not mission loss	Customer missions that can withstand mission loss. Missions that demonstrate new technology or capability	Only mission constraint is do no harm to launch vehicle (LV) or host (safety of flight)
2. Mission risk mitigation priority (failure tolerance) (1 = first priority, etc.)	Cost: 3 Schedule: 2 Technical: 1	Cost: 2 Schedule: 2 Technical: 2	Cost: 2 Schedule: 1 Technical: 3	Cost: 1 Schedule: 2 Technical: 3	Cost: 1 Schedule: 1 Technical: N/A except as it applies to DNH
3. Mission significance of individual asset	Individual essential mission asset	Individual major mission asset	Individual asset not essential if overall mission is met	Individual asset/mission is expendable	N/A
4. Mission life of individual asset	More than 5 yrs, may be 15+ yrs	2–10 yrs	1–5 yrs	Typically less than 2 yrs	Not specified
5. Customer engagement	Customer oversight of most program activities	Customer oversight of major program activities with remainder insight	Customer insight into all program activities, oversight of few key activities	No customer oversight, limited insight	None, except as dictated by DNH requirements of LV or host

3. Mission Success Processes

The list of 15 processes shown in Table 3 is taken from the 16 listed in the 2010 MAIW MA program framework, which was captured in TOR-2010(8591)-18 [4]. The MA framework guideline provides an industry and government matrix of processes that support achieving mission success. The 15 processes are organized into 4 categories. This ordering is changed from TOR-2011(8591)-21 [1] and purposely removes design assurance from the list of processes.

Table 3. MA Framework Mission Success Processes

Mission Success Framework Category	Process	
1. Policy, compliance, and safety	(1) **System safety**	
2. Mission design and qualification	(2) **Reliability engineering**	
	(3) **Parts, materials and processes**	
	(4) **Environmental compatibility analysis**	
	(5) **Integration, test, and evaluation**	
3. Oversight and assurance	(6) Independent reviews	**Future MSIW Work**
	(7) Failure review board	
	(8) Corrective/preventative action board	
	(9) Configuration/change management	
	(10) Requirements analysis and validation	
	(11) Risk assessment and management	
4. Quality management	(12) Hardware quality assurance	
	(13) Software assurance	
	(14) Supplier quality assurance	
	(15) Alerts and information bulletins	

The processes can be characterized by the following categories:

- Category 1: System safety processes include comprehensive safety management of potential hazards to personnel, equipment, systems, the environment, and facilities. The baseline comprising the minimum requirements is customarily defined by Range Safety, the launch site, and safety policies and regulations cited on contracts or otherwise imposed by the launch services provider. The only variation across mission assurance risk classification is the degree of external oversight and deliverables to verify adequate safety management, which falls under category 3 (oversight and assurance).

- Category 2: Mission design and qualification processes include the technical processes that drive program execution and mission success.

- Category 3: Oversight and assurance processes include oversight/insight parallel processes for identification of potential risks to mission success. In the application of these processes, oversight and insight are defined as follows:

  - Oversight is defined as the act of overseeing a program to actuarially characterize risk. Oversight implies certain separateness between the customer and contractor with 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 4: Quality management processes ensure the quality of products and services. There is a high degree of overlap between these processes and those governed by AS9100, which is to say that key quality processes are applied where AS9100 or ISO9001 is placed on contract.

The 4 categories break the 15 processes into: (1) universal processes regardless of mission assurance risk classification (safety), (2) technical processes that drive program execution and mission success, (3) non-technical processes that influence cost and schedule, and (4) processes that standardize quality expectations across industry. The figure below illustrates the consequence of selection relative to mission assurance risk classification. The y-axis shows the mission success categories and indicates the relative level of effort devoted to each category by risk class. The graphic is conceptual in nature, and the categories are separated to make them visually distinguishable. System safety remains constant across all mission risk classes, while the level of effort decreases for the other framework categories. Likewise, the DNH classification represents the minimum licensing, regulatory, and safety requirements.

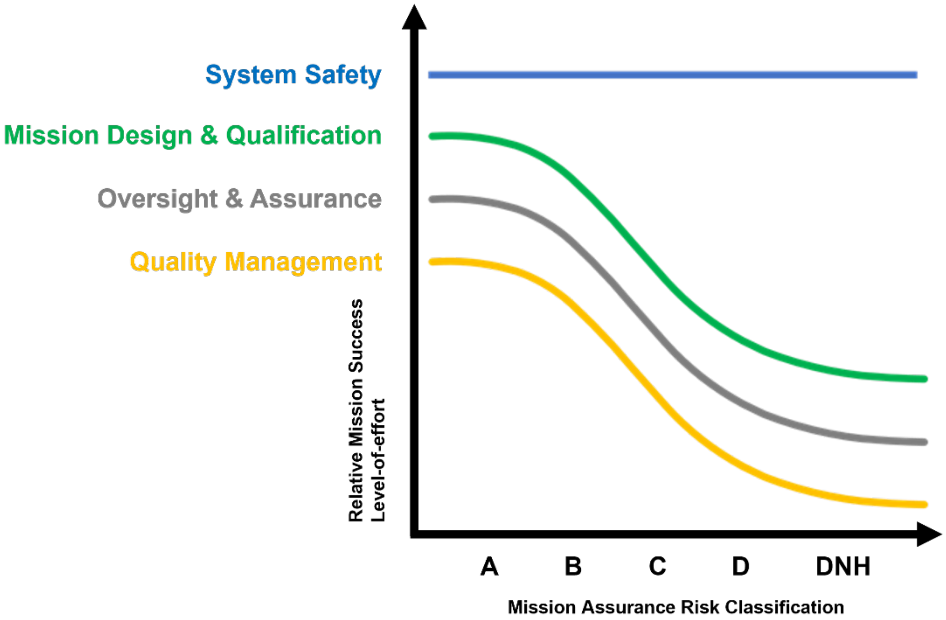

Figure 2. MA processes relative to mission assurance risk classification.

When considering tailoring for risk classification, the processes identified in the mission design and qualification category should be defined early. For example, understanding the balance between reliability performance and part quality will affect assumptions for program cost and schedule. Assuming lower-quality parts to save cost and schedule but expecting a high-reliability and high-availability mission is contradictory without doing sufficient system definition upfront. Understanding the relationship between qualification approach, mission functionality, and failure tolerance is also critical for adequately estimating program cost and schedule. As failure tolerance increases and minimum viable mission functionality decreases, qualification margin can be reduced. Pushing a greater degree of system definition upfront in the proposal and bid phase is recommended for more risk-tolerant missions because a one-size-fits-all approach is unlikely to be adequate. It also encourages dialogue with the customer, creating earlier opportunity to define critical and foundational characteristics.

It is important to note that the oversight and assurance processes do not drive technical risk but do have a significant consequence on influencing cost and schedule. Having a high degree of oversight on a more risk-tolerant mission impacts the ability for programs to execute on schedule and within budget. The mission success of programs with greater risk tolerance is defined by cost, schedule, and achieving the desired performance objectives—with varying influence across those three variables relative to risk class. Having a high degree of oversight on a more risk-tolerant mission may drive the risk classification to a less tolerant profile (e.g., Class A).

The top 5 of the 15 processes are defined with greater detail in their respective appendices and include general recommendations on tailoring relative to mission assurance risk classification. However, none of the original appendices have been comprehensively updated to reflect the current mission assurance risk classifications, and all are slated for future revisions. For the appendices that have not been updated in this revision, it is expected that the items that are discussed for Class D programs would be tailored for a Class DNH program. Keeping this in mind, the recommendations in the appendices are provided as guidance but are not requirements.

4. Acronyms

A_o	Operational availability
AEC	Automotive Electronics Council
AFSCN	Air Force Satellite Control Network
AO	Atomic oxygen
BOC	Break of configuration
CCB	Change control board
CDRL	Contract data requirements list
CIL	Critical items list
CoC	Certificate of conformance
COLA	Collision avoidance
COTS	Commercial off the shelf
DITL	Day in the life
DNH	Do No Harm
DOD	Department of Defense
DPA	Destructive physical analysis
DSN	Defense Switch Network
EEE	Electrical, electronic and electromechanical
EH&S	Environmental Health and Safety
EM	Engineering model
EOLP	End-of-life plan
EPA	Environmental Protection Agency
ERB	Engineering review board
ESOH	Environment, safety, and occupational health
ECA	Environmental compatibility analysis
EMC	Electromagnetic compatibility
EMI	Electromagnetic interference
FFMEA	Functional FMEA
FFP	Firm fixed price
FME	Failure modes and effect
FMEA	Failure modes and effects analysis
FMECA	Failure modes and effects criticality analysis
FPGA	Field-programmable gate array
FRB	Failure review board

FT	Fault tree
FTA	Fault tree analysis
GEO	Geosynchronous Earth orbit
GIDEP	Government-Industry Data Exchange Program
GSE	Ground support equipment
GSFC	Goddard Space Flight Center
HW	Hardware
IFMEA	Interface FMEA
IPC	Institute of Printed Circuits
IRR	Integration readiness review
I&T	Integration and test
IT&E	Integration, test, and evaluation
IUT	Instrument under test
KPP	Key performance parameter
LDC	Lot date code
LEO	Low Earth orbit
LV	Launch vehicle
MA	Mission assurance
MAIW	Mission Assurance Improvement Workshop
MDA	Missile Defense Agency
MEO	Medium Earth orbit
MMOD	Micrometeoroid/object detection
MRAR	Mishap risk assessment report
MRB	Material review board
MRPA	Mission risk posture assessment
MSIW	Mission Success Improvement Workshop
MSPSP	Missile system pre-launch safety package
MTTR	Mean time to repair or mean time to recover
N/A	Not applicable
NASA	National Aeronautics and Space Administration
NEPA	National Environmental Policy Act
NSS	National security space
OOHA	On-orbit hazard analysis
O&SHA	Operating and support hazard analysis

OSHA	Occupational Safety and Health Administration
PESHE	Programmatic environmental, safety, and occupational health evaluation
PHA	Preliminary hazard analysis
PHL	Preliminary hazard list
PMP	Parts, Materials, and Processes
PMPCB	PMP control board
PRA	Probabilistic risk assessment
PSA	Part stress analysis
QA	Quality assurance
QRB	Qualification review board
RAC	Reliability Analysis Center
RBD	Reliability block diagram
RCCA	Root cause corrective action
R&D	Research and development
RDM	Radiation design margin
RF	Radio frequency
RMA	Rideshare mission assurance
RPA	Risk posture assessment
SAR	Safety assessment report
SDAR	Space debris assessment report
SEE	Single-event effect
SEL	Single-event latch-up
SHA	System hazard analysis
SMC	Space and Missile Systems Center
SME	Subject matter expert
SOW	Statement of work
SPC	Statistical process control
SPF	Single-point failure
SRCA	Safety requirements/criteria analysis
SSA	Software safety analysis
SSC	Space Systems Command
SSHA	Subsystem hazard analysis
SSMP	System safety management plan
SSPP	System safety program plan

STE	Special test equipment
SW	Software
SWaP	Size, weight, and power
T&C	Telemetry and command or terms and conditions
TID	Total intensity dose
TLYF	Test like you fly
TOR	Technical operating report
TRR	Test readiness review
U.S.	United States
V&V	Verification and validation
WCCA	Worst-case circuit analysis

5. References

5.1 System Safety

[1] Johnson-Roth, G. A., *Mission Assurance Guidelines for A-D Mission Risk Classes*, Aerospace Report No. TOR-2011(8591)-21. The Aerospace Corporation, El Segundo, CA.

[2] States, M. K., Third United States Space Program Mission Assurance Summit Overview, Aerospace Report No. TOR-2011(8591)-9. The Aerospace Corporation, El Segundo, CA. March 15, 2011.

[3] Guarro, S. B.; G. A. Johnson-Roth; and W. F. Tosney (Eds.), *Mission Assurance Guide*, Aerospace Report No. TOR 2007(8546)-6018, Rev B. The Aerospace Corporation, El Segundo, CA. June 1, 2012.

[4] Bjorndahl, W. D., *Mission Assurance Program Framework,* Aerospace Report No. TOR-2010(8591)-18. The Aerospace Corporation, El Segundo, CA. June 30, 2010.

[5] Johnson-Roth, G., and W. Tosney, *Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles*, Aerospace Report No. TOR-2011(8591)-5, 1 The Aerospace Corporation, El Segundo, CA. September 13, 2010.

[6] SMCI 63-1201, *Assurance of Operational Safety, Suitability, and Effectiveness for Space and Missile Systems Center*. January 16, 2004.

[7] SMCI 63-1205, *Space System Safety Policy, Process, and Techniques*. June 28, 2011.

[8] AFI 91-202, *USAG Mishap Prevention Program*. August 1, 1998.

[9] AFSPCMAN 91-710, *Range Safety User Requirements Manual*. July 1, 2004.

[10] *Programmatic Environmental, Safety, and Health Evaluation Guide*, Space and Missile Systems Center.

[11] MIL-STD-882E, *Department of Defense Standard Practice for System Safety*. May 11, 2012.

[12] ANSI/GEIA-STD-0010, Rev. A, *Standard Best Practices for System Safety Program Development and Execution*, 18 October 2018.

[13] Englehart, W. C. (Ed.), *Space Vehicle Systems Engineering Handbook,* Aerospace Report No. TOR-2006(8506)-4494. The Aerospace Corporation, El Segundo, CA. January 31, 2006.

[14] Read, A.; P. S. Chang; B. M. Braun; and D. D. Voelkel, *Rideshare Mission Assurance and Do No Harm Process*, Aerospace Report No. TOR-2016-02946-Rev A. The Aerospace Corporation, El Segundo, CA.

5.2 Reliability

[15] Johnson-Roth, G. A., *Mission Assurance Guidelines for A-D Mission Risk Classes*, Aerospace Report No. TOR-2011(8591)-21. The Aerospace Corporation, El Segundo, CA.

[16] States, M. K., Third United States Space Program Mission Assurance Summit Overview, Aerospace Report No. TOR-2011(8591)-9. The Aerospace Corporation, El Segundo, CA. March 15, 2011.

[17] Guarro, S. B.; G. A. Johnson-Roth; and W. F. Tosney (Eds.), *Mission Assurance Guide,* Aerospace Report No. TOR 2007(8546)-6018, Rev B. The Aerospace Corporation, El Segundo, CA. June 1, 2012.

[18] Bjorndahl, W. D., *Mission Assurance Program Framework,* Aerospace Report No. TOR-2010(8591)-18. The Aerospace Corporation, El Segundo, CA. June 30, 2010.

[19] Johnson-Roth, G., and W. Tosney, *Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles,* Aerospace Report No. TOR-2011(8591)-5. The Aerospace Corporation, El Segundo, CA. September 3, 2010.

[20] Ingram-Cotton, J. B.; M. J. Hecht; R. J. Duphily; M. Zambrana; T Hiramoto; and C. O'Connor, *Reliability Program Requirements for Space Systems,* Aerospace Report No. TOR-2007(8583)-6889. The Aerospace Corporation, El Segundo, CA. July 10, 2007.

[21] Englehart, W. C. (Ed.), *Space Vehicle Systems Engineering Handbook,* Aerospace Report No. TOR-2006(8506)-4494. The Aerospace Corporation, El Segundo, CA. January 31, 2006.

[22] Duphily, R. J., *Space Vehicle Failure Modes, Effects, and Criticality Analysis (FEMCA) Guide*, Aerospace Report No. TOR-2009(8591)-13. The Aerospace Corporation, El Segundo, CA. June 15, 2009.

[23] Robertson, S. R.; L. I. Harzstark; J. P. Siplon; D. M. Peters; P. H. Hesse; M. J. Engler; R. J. Ferro; W. A. Martin; G. G. Cuevas; M. H. Cohen; J. H. Sokol; K. N. Feistel; S. R. Nuccio; and G. J. Ewell, *Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles*, Aerospace Report No. TOR-2006(8583)-5236 Rev B, (also published as SMC-S-10). The Aerospace Corporation, El Segundo, CA. March 6, 2013.

[24] Duphily, R. J., *Space Vehicle End-of-Life (EOL) Disposal Reliability Overview*, Aerospace Report No. TOR-2021-02404 Rev. B. The Aerospace Corporation, El Segundo, CA. December 15, 2021.

[25] Read, A.; P. S. Chang; B. M. Braun; and D. D. Voelkel, *Rideshare Mission Assurance and Do No Harm Process*, Aerospace Report No. TOR-2016-02946-Rev A. The Aerospace Corporation, El Segundo, CA.

5.3 Parts, Materials and Processes

[26] Johnson-Roth, G. A., *Mission Assurance Guidelines for A-D Mission Risk Classes*, Aerospace Report No. TOR-2011(8591)-21. The Aerospace Corporation, El Segundo, CA.

[27] States, M. K., Third United States Space Program Mission Assurance Summit Overview, Aerospace Report No. TOR-2011(8591)-9. The Aerospace Corporation, El Segundo, CA. March 15, 2011.

[28] Robertson, S. R.; L. I. Harzstark; J. P. Siplon; D. M. Peters; P. H. Hesse; M. J. Engler; G. G. Cuevas; and D. C. Meshel, *Parts, Materials and Processes Control Program for Space and Launch*

Vehicles (also published as SMC-S-009-2009), Aerospace Report No. TOR-2006(8583)-5235 Rev. B. The Aerospace Corporation, El Segundo, CA. March 6, 2013.

[29] Robertson, S. R.; L. I. Harzstark; J. P. Siplon; D. M. Peters; P. H. Hesse; M. J. Engler; R. J. Ferro; W. A. Martin; G. G. Cuevas; M. H. Cohen; J. H. Sokol; K. N. Feistel; S. R. Nuccio; and G. J. Ewell, *Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles,* Aerospace Report No. TOR-2006(8583)-5236 Rev. B, (also published as SMC-S-10). The Aerospace Corporation, El Segundo, CA. March 6, 2013.

[30] EEE-INST-002 *Instructions for EEE Parts Selection, Screening, Qualification and Derating.*

[31] *(NASA/TP-2003-212242), Addendum 1,* April 2008.

[32] NASA-STD-6061C, *Standard Materials and Processes Requirements for Spacecraft*, September 30, 2021.

[33] Speece, D. J., *Objective Criteria for Heritage Hardware Reuse,* Aerospace Report No. TOR-2010(8591)-19. The Aerospace Corporation, El Segundo, CA. June 30, 2010.

[34] Lewis, R., and D. J. Speece, *Reuse of Hardware and Software Products,* Aerospace Report No. TOR-2009(8546)-8604, Rev. A. The Aerospace Corporation, El Segundo, CA. January 27, 2010.

[35] Lenertz, B. A., *Electrical Design Worst Case Circuit Analysis Guidelines and Draft Standard,* Aerospace Report No. TOR-2013-00297. The Aerospace Corporation, El Segundo, CA. June 3, 2013.

[36] Hogan, S. L., *Expanding Space Design Options Using COTS*, Aerospace Report No. ATR-2023-01935. The Aerospace Corporation, El Segundo, CA. September 6, 2023.

[37] Read, A.; P. S. Chang; B. M. Braun; and D. D. Voelkel, *Rideshare Mission Assurance and Do No Harm Process*, Aerospace Report No. TOR-2016-02946-Rev A. The Aerospace Corporation, El Segundo, CA.

5.4 Environmental Compatibility

[38] Johnson-Roth, G. A., *Mission Assurance Guidelines for A-D Mission Risk Classes*, Aerospace Report No. TOR-2011(8591)-21. The Aerospace Corporation, El Segundo, CA.

[39] States, M. K., Third United States Space Program Mission Assurance Summit Overview, Aerospace Report No. TOR-2011(8591)-9. The Aerospace Corporation, El Segundo, CA. March 15, 2011.

[40] Perl, E.; A. J. Peterson; J. M. Snyder; C. P. Wright; and J. W. Welch, *Test Requirements for Launch, Upper-Stage, and Space Vehicles,* Aerospace Report No. TR-RS-2014-00016. The Aerospace Corporation, El Segundo, CA. June 15, 2014 (also published as SMC-S-016), June 25, 2014.

[41] MIL-STD-461F, *Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,* December 10, 2007.

[42] MIL-STD-461G, *Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment,* December 11, 2015.

[43] Dunbar, M. W., *Electromagnetic Compatibility Requirements for Space Equipment and Systems,* Aerospace Report No. TOR-2005 (8583)-1 Rev. A (MIL-STD-1541A). The Aerospace Corporation, El Segundo, CA. January 1, 2008.

[44] MIL-STD-1542B, *EMC and Grounding Requirements for Space Systems Facilities,* November 15, 1991.

[45] DOD-W-83575A, Notice 1, *General Specifications for Space Vehicle Wiring Harness Design and Testing,* September 4, 2002.

[46] ASTM E1548-09, *Standard Practice for Preparation of Aerospace Contamination Control Plans,* October 5, 2017.

[47] Goldstein, S., *Criteria for Explosive Systems and Devices Used of Space Vehicles,* Aerospace Report No. TOR-2004 (8583)-3291. The Aerospace Corporation, El Segundo, CA. August 9, 2004.

[48] Chang, J. B., and N. R. Patel, *Space Systems Structures Design and Test Requirements,* Aerospace Report No. TOR-2003 (8583)-2894. The Aerospace Corporation, El Segundo, CA. August 2, 2004.

[49] Gore, B. W., *Critical Clearances in Space Vehicles,* Aerospace Report No. ATR-2009(9369)-1. The Aerospace Corporation, El Segundo, CA. October 31, 2008.

[50] Conely. P. L. (Ed.), *Space Vehicle Mechanisms-Elements of Successful Design,* Wiley and Sons, 1998.

[51] Wertz, J. R., and W. J. Larson (Eds.), *Space Mission Analysis and Design Third Edition,* Kulwer Academic Publishers, 1999.

[52] Pisacane, V. L. and R. C. Moore, R.C. (Eds.), *Fundamental of Space Systems,* Oxford University Press, 1994.

[53] PD-EC-1101, *NASA Preferred Reliability Practices Environmental Factors, NASA Lewis Research Center.*

[54] NASA NPR 8705.4A, *Risk Classification for NASA Payloads,* April 29, 2021.

[55] DOD-HBDK-343, *Design, Construction, and Testing Requirements for One of a Kind Space Equipment,* February 1, 1986.

[56] NASA NSS 1740.14, *Guidelines and Assessment Procedures for Limiting Orbital Debris,* August 1995.

[57] Scialdone, J. J., *Spacecraft Compartment Venting,* Proc. SPIE 3427, 23 (1998); doi:10.1117/12.328500.

[58] Bedingfield, K. L.; R. D. Leach, and M. B. Alexander (Eds.), NASA Reference Publication 1390, *Spacecraft System Failures and Anomalies Attributed to the Natural Space Environment*, August 1996.

[59] Johnson-Roth, G., and W. Tosney, *Mission Risk Planning and Acquisition Tailoring Guidelines for National Security Space Vehicles,* Aerospace Report No. TOR-2011(8591)-5. The Aerospace Corporation, El Segundo, CA. September 13, 2010.

[60] Read, A.; P. S. Chang; B. M. Braun; and D. D. Voelkel, *Rideshare Mission Assurance and Do No Harm Process*, Aerospace Report No. TOR-2016-02946-Rev A. The Aerospace Corporation, El Segundo, CA.

5.5 Integration, Test and Evaluation

[61] Johnson-Roth, G. A., *Mission Assurance Guidelines for A-D Mission Risk Classes*, Aerospace Report No. TOR-2011(8591)-21. The Aerospace Corporation, El Segundo, CA.

[62] States, M. K., Third United States Space Program Mission Assurance Summit Overview, Aerospace Report No. TOR-2011(8591)-9. The Aerospace Corporation, El Segundo, CA. March 15, 2011.

[63] Johnson-Roth, G., and W. Tosney, *Mission Risk Planning and Tailoring Guidelines for National Security Space Vehicles*, Aerospace Report No. TOR-2011(8591)-5. The Aerospace Corporation, El Segundo, CA. September 13, 2010.

[64] Hanifen, D. W.; A. J. Peterson; and W. F. Tosney (Eds.), *Space Vehicle Test and Evaluation Handbook*, Aerospace Report No. TOR-2006(8546)-4591. The Aerospace Corporation, El Segundo, CA. November 6, 2006.

[65] Perl, E.; A. J. Peterson; J. M. Snyder; C. P. Wright; and J. W. Welch, *Test Requirements for Launch, Upper-Stage, and Space Vehicles*, Aerospace Report No. TR-RS-2014-00016. The Aerospace Corporation, El Segundo, CA. June 15, 2014 (also published as SMC-S-016), June 25, 2014.

[66] MIL-HDBK-340A (USAF), Military Handbook, *Test Requirements for Launch, Upper-stage, and Space Vehicles*. April 1, 1999.

[67] Gore, B. W., *Critical Clearances in Space Vehicles*, Aerospace Report No. ATR-2009(9369)-1. The Aerospace Corporation, El Segundo, CA. October 31, 2008.

[68] Cantrell, J. C.; D. Gianetto; R. Atkinson; M. Edwards, and M. McKeown, *Suggested Checklist to Improve Test Performance in the System Test Equipment Area*, Aerospace Report No. TOR-2009(8591)-12. The Aerospace Corporation, El Segundo, CA. May 21, 2009.

[69] Knight, F. L., *Space Vehicle Checklist for Assuring Adherence to Test-Like-You-Fly Principles*, Aerospace Report No. TOR-2009(8591)-15. The Aerospace Corporation, El Segundo, CA. June 30, 2009.

[70] Dunbar, M. W., *Electromagnetic Compatibility Requirements for Space Equipment and Systems*, Aerospace Report No. TOR-2005 (8583)-1 Rev A (MIL-STD-1541A). The Aerospace Corporation, El Segundo, CA. January 2008.

[71] GSFC-STD-7000 (NASA document), *General Environmental Verification Specification*, April 2005.

[72] Welch, J. W., *Flight Unit Qualification Guidelines*, Aerospace Report No. TOR-2010(8591)-20. The Aerospace Corporation, El Segundo, CA. June 30, 2010.

[73] Read, A.; P. S. Chang; B. M. Braun; and D. D. Voelkel, *Rideshare Mission Assurance and Do No Harm Process*, Aerospace Report No. TOR-2016-02946-Rev A. The Aerospace Corporation, El Segundo, CA.

Appendix A. System Safety

A.1 Introduction

The primary objective of the system safety discipline and process is to ensure potential hazards to personnel, equipment, systems, the environment, and facilities are identified, tracked, evaluated, and eliminated and associated residual risks are 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:

1. Providing safety requirements, safety design, safety testing, safety operations, and disposal checklists for programs and users

2. Identifying and tailoring contract system safety requirements consistent with mission requirements

3. Performing 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. Inputting 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. Investigating and formally reporting 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 overarching 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. System safety differs from the traditional Environmental Health and Safety (EH&S) discipline in that the focus is placed on the design, build and test, and operational aspects of the product, with engineering subject matter experts (SMEs) integrated with the product design and development and end-user teams.

This appendix provides guidelines for applying system safety to space systems. System safety processes and work products are generally applicable to all space missions owing their origin in government policies and standards as discussed in the introduction to section 3. For example, a system safety program is required for all NSS space system development programs, with commercial activities at non-traditional launch sites coming under the purview of the FAA and Range Safety AFSPCMAN 91-70. The MIL-STD-882E 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 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 elimination/control/mitigation recommended by MIL-STD-882E:

1. Design to eliminate hazard
2. Reduce hazard risk (likelihood or severity)
3. Incorporate engineering features or safety devices
4. Provide warning devices or notifications
5. Develop procedures and training

System safety is applicable across the entire lifecycle and to all system levels.

A.2 Definitions for System Safety

Definitions are provided to guide the reader in interpreting the mission risk class process matrix below, establishing a basis from which the risk profile can be developed. They 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 by systems engineering personnel to responsible design, test, and operations personnel. Safety compliance checklists and hazards analysis are used to track implementation and verification of allocated requirements.

Safety analyses: There are various tools available to assist in implementing a system safety program to identify hazards. The analyses below identify hazards in particular settings or at particular times in the system lifecycle, 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 later evaluation. 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 focus initial assessment of hazards and to identify requisite hazard controls and follow-on actions. Hazards associated with the proposed design or function are 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)** identifies hazards in subsystems of a major larger system. The analysis identifies 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 the software's interaction with other aspects of the system. Actions are identified to eliminate or control hazards from the 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 (OOHA): Other analyses may be performed that incorporate one or more of the analytical tools described above. Of particular importance is the OOHA that must be performed to address the safety of a system that includes an orbiting asset. An on-orbit hazard analysis includes orbital safety considerations, such as collision avoidance (COLA), directed energy, orbital debris minimization, end-of-life safing, and the space environment. An OOHA 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 OOHA supports development of documents such as the programmatic environmental, safety, and occupational health evaluation (PESHE), space debris assessment report (SDAR), or end-of-life plan (EOLP).

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, including the following:

- **Fault tree analysis (FTA)** is a logic-tree method of analyzing catastrophic events 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 (ETA)/Event Sequence Diagram (ESD)** 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 several stepwise, mutually exclusive loss levels. The system challenge may be a failure or fault, an undesirable event, or a normal system operating command.

- **Failure modes and effects analysis (FMEA)** is a bottom-up process that assesses components, assemblies, and subsystems to identify potential failure modes in a system and their causes and effects on the system hazards. It is a design tool used to systematically analyze postulated component failures and identify the resultant effects on system operations.

Safety risk documentation: The acquisition authority may require formal safety documentation and other documentation may be 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 a record of safety features. The documentation is also useful for supporting potential legal/liability activities, such as accident investigation, indemnification reviews, or the government contractor legal defense.

- **A system safety management plan (SSMP)** provides guidance on how the program office 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.

An SSPP establishes a system safety organization to execute 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 lifecycle phases of the program and to establish a formal, disciplined program to achieve the system safety objectives.

- The **MSPSP and MRAR** capture 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 lifecycle of a system will ensure that system safety is properly addressed during system reviews, meetings with Range Safety and other regulating organizations, and MSPSP/MRAR preparation. For programs involved with the 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 contents for the MRAR. Other MRAR contents might typically include analyses from parts of the lifecycle outside the purview of the Range, such as prelaunch 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 need to be submitted to the program office.

- The **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, and document residual risk acceptance and ongoing assessment of the effectiveness of mitigation efforts.

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

- The **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.

- **EOLP** programs 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 their useful life where they 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.

- The **SAR** 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 (see ANSI/GEIA-STD-0010, *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.

- The **OOHA report** documents the OOHA that 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 and 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.

A.3 Matrix—System Safety

Recommended system safety activities vary widely by inherent system hazards and risks 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 about the loss of the 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-882E. Provided below is a summary of risk class profile support from the System Safety Mission Class Matrix.

Category	Class A	Class B	Class C	Class D	Do No Harm
System Safety					
Requirements Identification, Allocation, and Verification	Identify and define applicable safety requirements from government/industry regulations, policies, and standards.Tailor with appropriate stakeholder(s) and allocate program integration and launch site safety requirements as appropriate throughout the product and mission lifecycle spanning contractor (i.e., design, integration and test [I&T], and delivery) and external (prelaunch, launch, postlaunch on-orbit and disposal) operations.	Same as Class A.	Same as Class A, with expectation that MIL-STD-882E requirements for work product depth and customer approval are tailored. Minimum Range Safety requirements must be satisfied.	Same as Class C, except contractor proposes tailored requirements that will meet customer approval. Minimum Range Ground, and Safety and Licensing requirements must be satisfied.	Minimum range, ground, and safety and licensing requirements must be satisfied.
Safety Analysis and Support	Contractor performs all analyses defined in tailored system safety and Range Safety standards. Typical work products include: SSPP, PHL, PHA, SSHA, SHA, software safety analysis. Typical support effort include OOHA, space debris assessment, EOLP, and COLA; O&SHA for contractor operations performed outside of contractor facility; health hazard assessment. Perform safety assessment of engineering change proposals, specification change notices, software problem reports, and requests for deviation/waiver.	Same as Class A with reduction of scope for support efforts and assessments.	Same as Class A, with reduction of scope for MIL-STD-882E, support efforts, and assessments. Prioritize support and data necessary to satisfy primary mission. Minimum Range Safety analyses, work products, and support must be performed.	Same as Class C, with scope aligned per contractor-proposed requirements. Minimum Range, Ground, and Safety and Licensing requirements must be satisfied.	Minimum Range, Ground, and Safety and Licensing requirements must be satisfied.

Category	Class A	Class B	Class C	Class D	Do No Harm
Safety Risk Assessment	Contractor assesses hazard probability of occurrence and severity.	Same as Class A.	Same as Class A.	Same as Class A.	Minimum Range, Ground, and Safety and Licensing requirements must be satisfied.
System Safety Program Plan and Documentation	Formal system safety program plan is expected as a deliverable. MSPSP/MRAR, safety analysis/hazard reports or input to prime if subcontractor effort is on contract.	Same as Class A.	MSPSP/MRAR and hazard reports expected 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 expected but less detailed. System safety plan may be required. As a minimum, developer must ensure payload is safe to integrate and launch.	Not expected—developer's choice.
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.	Minimum Range, Ground, and Safety and Licensing requirements must be satisfied.
Mishap Reporting and Investigation	Contractor describes incident-reporting process in SSPP. Includes direction for formal mishaps safety investigation boards in case of mission loss or major mission impact.	Same as Class A.	Formal mishap board usually not expected (dependent on mission value and mishap severity). Contractor performs root cause analysis and provides results.	Same as Class C.	Not expected—developer's choice.
Integration Site and Launch Site Safety Support	Coordination, hazardous procedures submittal.	Same as Class A.	Same as Class A.	Same as Class A.	Minimum Range, Ground, and Safety and Licensing requirements must be satisfied.

A.4 Summary of Risk Classes for 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 about the loss of the 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-882E. Provided below is a summary of risk class profile support from the System Safety Mission Class Matrix.

Class A: System safety process applies assessment and analyses throughout the lifecycle 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 program plan and a safety analysis/hazard tracking report are required as a deliverable. The plan would include 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 firm-fixed-price (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.

DNH: Typically, the minimum range, ground, and safety and licensing requirements must be satisfied.

A.5 Effectiveness Tips—System Safety 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 ensuring the proper level of management acceptance for residual hazard risks.

Appendix B. Reliability

B.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. Reliability engineering is the process that provides independent insight, planning, and validation for reliability; end-of-life capability, including asset disposal; 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. A key tenet of reliability engineering is that the design and associated test activities will ensure components are utilized within their useful life for the mission and that analyses can assume random failure rates. These analyses include, but are not limited to:

- Reliability prediction and allocation
- FMEA
- Probabilistic risk assessment
- FTA
- Critical-item assessment analysis
- Trend analysis

Additionally, reliability engineering incorporates and sometimes performs other analyses, including limited-life, part-level electrical, mechanical, and thermal stress analyses and worst-case analyses, as covered in Appendix C. A closed-loop failure and corrective action system is also a key element of the reliability program. The effectiveness of these measures is determined and supported by design analyses, design reviews, hardware tests, and failure data evaluation.

This appendix provides guidelines for applying effective reliability engineering to space systems. The methods of reliability engineering should be selected to meet the needs of the program. However, a reliability engineering process is required for any space system development activity to ensure the system architecture meets mission needs and that, at its most basic level, the products developed for the mission will not negatively impact host or mission partners. This is addressed in more detail in B.3 and B.4. The process may be applied to all space flight systems to include deliverable payloads, space vehicles, or other associated products and may also include ground system elements. 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.

B.2 Definitions for Reliability

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.

Reliability monitoring and control: Reliability monitoring and control captures policies, procedures, and control processes that address the execution of the required reliability engineering scope and effort to meet mission needs and requirements. It includes the creation and implementation of a reliability program plan that delineates the reliability analyses to be executed and delivered (internally to the program or externally to the acquisition authority) for a system across its program lifecycle.

Reliability forecast: The reliability forecast is an analysis that often takes on one of two forms: either a reliability prediction or a probabilistic risk assessment (PRA). A reliability prediction is a mathematical model that is based on a success-space perspective and is often developed using closed-form probability equations but could also be based on a Monte Carlo simulation. Reliability block diagrams (RBDs) are graphical representations of a subsystem's serial, parallel, standby, and complex configurations and often form the foundation of the reliability prediction effort. The inputs to the reliability prediction effort should include the most current and accurate piece-part-level failure rates, part supplier data, or operational data and not depend exclusively on historical sources such as those found in MIL-HDBK-217 FN2 (e.g., ANSI/VITA 51.1 and Reliability Analysis Center (RAC) factors from IITRI: A06830). A PRA is based on a failure-space perspective and can be developed using closed-form Boolean logic (e.g., And gates, Or gates, etc.) but can also be based on algorithms that resolve a system's minimum cut-sets. In addition to an event tree that often characterizes a mission profile, FTA is a logic-tree method of analyzing catastrophic events from the top down and often forms the foundation of the PRA effort.

Maintainability: Maintainability is the measure of a system's, subsystem's, or unit's ability to be maintained to continue providing the required service. It is most often associated with the metrics of mean time to repair or mean time to recover (MTTR), where repair focuses on the average time it takes to replace or fix a failed item from fault discovery and recovery includes that time plus the time it takes for the impacted unit to return to operation.

Operational availability (A_o): A_o is the measure of a system's ability to be utilized as designed or architected in mission as a function of time (uptime) as compared to anticipated downtime. It is often generally expressed as uptime divided by total (up + down) time. For systems comprising constellations of assets, the A_o can be defined and assessed at the constellation level instead of at the individual asset level.

Probability of disposal: The probability of disposal is a prediction of the ability and likelihood that an asset will be removed from a protected orbital region after the end of the mission. The calculation of this probability can include consideration of the reliability of the subsystem(s) necessary to execute disposal, ability to monitor telemetry of those subsystems, and any potential recovery or remediation in the case of subsystem degradation, including failure prior to completion of disposal. Additional guidance is provided in TOR-2021-02404 Rev. B [24].

Serial elements: Serial elements are design features that are in series and require the preceding module, component, or piece-part to function in order for their function to contribute to the mission. A combination of serial elements produces a series system where the ability to employ subsystem B depends on the whether subsystem A is operational regardless of the state of subsystem B. A fully serial design results in what is termed a "single string" design.

B.3 Matrix—Reliability

Category	Class A	Class B	Class C	Class D	Do No Harm
Reliability Monitoring and Control	Comprehensive policies, procedures, monitoring, and control processes supporting minimum practical risk. Formal reliability program plan required by contract as an approved deliverable.	Policies, procedures, monitoring, and control processes supporting low-risk profile. Formal reliability program plan required by contract as an approved deliverable.	Streamlined policies, procedures, monitoring, and control processes assessing compliance in support of moderate risk. Reliability program plan developed.	Policies, procedures, monitoring, and control processes required to ensure hardware and personnel safety. Limited reliability program plan developed.	Policies, procedures, monitoring, and control processes required to ensure host hardware and personnel safety.
Failure Modes and Effects Criticality Analysis (FMECA)	Extensive functional, component, interface, and safety-critical efforts delivered as an approved deliverable. Extensive piece-part level.	Functional, interface efforts often delivered as an approved deliverable. Selective piece-part level FMECA.	Component- or assembly-level FMECA.	Interface FMECA.	Not expected—developer's choice.
Failure Modes and Effects Analysis (FMEA)	Typically secondary to a FMECA.	Typically secondary to a FMECA.	Functional and interface effort.	Interface-level effort.	Interface effort for host interfaces only.
Critical Items List (CIL)	Explicitly delineated within FMECA; often a distinct deliverable.	May be included within FMECA effort; may be a deliverable.	May be included within FMEA effort; often for internal uses only.	May be included within FMEA effort; often for internal uses only.	Not expected—developer's choice.
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 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 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.	Not expected—developer's choice.
Reliability Forecast	System model developed and used to generate a reliability forecast incorporating part-level detail in a reliability prediction or PRA with limited-scope mission end states.	System model developed and used to generate a reliability forecast incorporating part-level detail in a reliability prediction or PRA with limited scope on mission-related end states of program interest.	System model developed and used to generate a reliability forecast incorporating part-level detail (part count) in a reliability prediction.	System model developed and used to generate a reliability forecast incorporating part-level detail (part count) only.	Not expected—developer's choice.
Probability of Asset Disposal	Incorporated as a feature in the system model.	Incorporated as a feature in the system model.	Incorporated as a key feature in the system model.	Incorporated as the key feature (typically) in the system model.	Minimum Range, Ground, and Safety and Licensing requirements must be satisfied.

Category	Class A	Class B	Class C	Class D	Do No Harm
Single-Point Failure (SPF) Policy and Redundancy	Potential risks from serial elements negated. All SPFs are identified and evaluated. An assessment of all credible SPFs that endanger satisfactory completion of the mission or result in a safety hazard that includes: A risk assessment that includes probability and consequence of failure. - Analysis of the individual SPF's impact on asset and system reliability. Non-credible individual SPFs may include any module-level SPF with a $P_s \geq 0.99$ at end of mission life. SPF list explicitly delineated within FMECA.	Potential risks from serial elements minimized. All SPFs are identified and evaluated. An assessment of all credible SPFs that endanger satisfactory completion of the mission or result in a safety hazard that includes: A risk assessment that includes probability and consequence of failure. - Analysis of the SPF's impact on asset and system reliability. Non-credible individual SPFs may include any component-level SPF with a $P_s \geq 0.99$ at end of mission life. SPF List included within FMECA.	Potential risks from serial elements identified and managed. All SPFs are identified and evaluated. An assessment of all credible SPFs that endanger satisfactory completion of the mission or result in a safety hazard that may include: - A risk assessment that includes probability and consequence of failure. - Analysis of the SPF's impact on asset and system reliability. Non-credible individual SPFs may include any piece-part-level SPF with a $P_s \geq 0.99$ at end of mission life. SPF List may be included in FMEA effort.	Potential risks from serial elements identified and accepted. Design critical elements to the greatest extent possible to prevent credible SPFs. All SPFs understood, accommodated and impact accepted. SPF list may be included in FMEA effort.	Potential risks from serial elements accepted by host. Design critical elements to the greatest extent possible to prevent credible SPFs. SPFs acknowledged by host.
Software Reliability	Software reliability growth program recommended for new development of critical software.	Software reliability growth program recommended for new development of critical software.	May be required for new development of critical software.	Not expected—developer's choice.	Not expected—developer's choice.
Mission/System Fault Tree Analysis (FTA) (NASA requirement only)	Mission-/system-level qualification FTA required.	Mission-/system-level qualification FTA required for critical aspects of the mission.	Recommended but not required; performed only to ensure no effect on bus or other payloads.	Performed only to ensure no effect on bus or other payloads.	Not expected—developer's choice.
Ground Support Equipment (GSE) Interface FMEA (IFMEA) **or** **GSE Functional FMEA (FFMEA)**	IFMEA to demonstrate GSE, special test equipment (STE), engineering model (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.	Not expected—developer's choice.

Category	Class A	Class B	Class C	Class D	Do No Harm
Maintainability	Required for development maintenance and mission ground system MTTR, including comprehensive spares philosophy.	Required for development maintenance and mission ground system MTTR, including spares philosophy of critical components.	Recommended for MTTR and A_o management.	Not expected—developer's choice.	Not expected—developer's choice.
Operational Availability (A_o)	System model leveraged to predict A_o. Required A_o aligns with continuous operation. For example, this may equate to an $A_o \geq 0.999$ (~8 hours of downtime per year).	System model leveraged to predict A^o. Required A_o aligns with near continuous operation. For example, this may equate to an $A_o \geq 0.99$ (~87 hours of downtime per year).	System model leveraged to predict A_o. Required A_o aligns with less than continuous operation. For example, this may equate to an $A_o \geq 0.9$ (~877 hours of downtime per year).	Not expected—developer's choice.	Not expected—developer's choice.

B.4 Summary of Risk Classes for Reliability

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 module level (e.g., circuit card assembly). 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 in B.3. Reliability forecasts will typically take the form of system-level reliability predictions based on piece-part-level inputs. In specific instances, where the system has a high degree of complexity and risk aversion compared to other Class A efforts, customers may elect to require a PRA instead of a reliability prediction (e.g., human spaceflight systems developed for NASA).

Reliability requirements will dictate that the potential risks of serial components are negated in an individual asset; exceptions require justification based on risk analysis and mitigation measures. Negation of potential risk from serial components may include redundancy at the unit level, cross-strapping at the card level, functional redundancy between subsystems or units, or other measures. A probability of a disposal metric can be a concern for a Class A program and may be mandated as a separate reliability metric or as a substitute for a nominal mission reliability metric. SPFs are usually not allowed except for structure-like elements and unit-level SPFs with a $P_s \geq 0.99$ at end of mission life. This P_s value corresponds to an individual SPF and is not reflective of an aggregation of multiple SPFs. Occasionally, piece-part FMECAs will be developed for critical SPFs. 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 a Class B system or asset. 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 unit or module 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 in B.3. Reliability forecasts will typically take the form of a system-level reliability prediction based on piece-part-level inputs. In rare instances, where the system has a high degree of complexity and risk aversion compared to other Class B efforts, customers may elect to require a PRA instead of a reliability prediction. However, the PRA is to a lesser degree of detail than what would be expected for Class A, and that detail must be clearly defined as part of the acquisition process by the customer, and where practicable, the contractor.

A Class B reliability analysis effort seeks to minimize the potential risks of serial components and considers common cause failures that could mitigate perceived redundancy. A probability of a disposal metric can be a concern for a Class B program and may be mandated as a separate reliability metric or as a substitute for a nominal mission reliability metric. SPFs exceptions include structure-like elements and card-level (or equivalent) SPFs with a $P_s \geq 0.99$ at end of mission life. 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 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. Specific reliability requirements include all of those listed in the matrix in B.3. A Class C reliability analysis effort seeks to identify and manage the potential risks of serial components. Often this effort will focus on those elements that might impact asset critical functions but not mission functions. A probability of a disposal metric is often a concern for a Class C program and may be mandated as a separate reliability metric or as a substitute for a nominal mission reliability metric. A CIL and/or SPF list may be embedded within the FMEA effort but is often not a distinct deliverable but used to facilitate internal awareness of critical program concerns and mitigations. SPFs exceptions include structure-like elements and piece-part-level SPFs with a $P_s \geq 0.99$ at end of mission life. This P_s value corresponds to an individual SPF and is not reflective of an aggregation of multiple SPFs. It should be noted that a PRA effort and FMECAs of any type, including piece-part, are typically not developed for Class C programs. The contractor's reliability organization and processes will typically define the major reliability tasks as part of the design, development, and verification process.

Class D: Class D may not have formal or specific contractual requirements other than those imparted by applicable safety standards, disposal, or interface requirements. Development of a reliability plan and the reliability assessment is left to the discretion of the experimenter/developer. A Class D reliability analysis effort acknowledges the potential risks of serial components. A probability of a disposal metric is often a concern for a Class D program and may be mandated as a separate reliability metric or as a substitute for a nominal mission reliability metric. A CIL and/or SPF list may be embedded within the FMEA effort but is often not a distinct deliverable but used to facilitate internal awareness of critical program concerns and mitigations. SPFs will likely exist, be understood, and accommodated. Single-string or selective redundant design approaches are often used due to size, weight, and power (SWaP) constraints and the limited life and budgets of the program relative to higher mission classes. It should be noted that a PRA effort and FMECAs of any type, including piece-part, are typically not developed for Class D programs. The contractor's reliability organization and processes will typically define the major reliability tasks as part of the design, development, and verification process.

DNH: DNH missions will develop only those reliability analyses and products necessary to demonstrate to the host that they meet relevant contractual DNH criteria. These will likely be limited to an interface FMEA between the candidate mission and the host, details of relevant SPFs related to that interface, and any other analyses that require reliability inputs to related safety standards.

B.5 Effectiveness Tips—Reliability Lessons Learned

- Ensure the reliability organization is proactive and influences the design throughout the relevant lifecycle phases and does not merely document the design

- Ensure trade studies consider relative reliability as part of system architecture

- 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 corrective action to ensure failure modes or effects are accurately represented in reliability forecasts

- Ensure the scope of the probability of disposal analysis is well understood and agreed to by the acquisition authority early in the program lifecycle, ideally during the acquisition process

Appendix C. Parts, Materials, and Processes (PMP)

C.1 Introduction

The primary objective of the 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 raw materials and the processes used in the manufacturing of deliverable hardware. It also includes a definition of expectations for attributes, such as derating and performance, as well as review of nonstandard or noncompliant items. PMP activities may include:

- Establishment of program requirements for part and material qualification and screening
- Verification of all contractor/subcontractor performance to ensure that delivered products satisfy contractually flowed-down PMP requirements
- Regularly scheduled PMP meetings to resolve issues and adjudicate the usage of nonstandard (per established program requirements) PMP
- Verification of worst-case circuit analysis and degradation limits of critical parameters for worse-case design

This appendix 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 spaceflight 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.

C.2 Definitions for PMP

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. They are not intended as general standalone industry standard definitions.

PMP control board (PMPCB): The responsibility of the PMPCB is to ensure all PMP 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 nonstandard items. The PMPCB reviews and acts on any noncompliance with or deviation from the established PMP requirements.

Program-approved PMP lists/PMP selection lists: The approved PMP list(s) cover the selection, review, and analysis activities for all PMP planned for use of a given program and facilities standardization.

Traceability: PMP traceability provides the capability of identifying parts and materials by lot information in case of problem information received about a specific lot via destructive physical analysis (DPA), Government-Industry Data Exchange Program (GIDEP), or other alert or verified functional failure.

Parts selection: Parts selection establishes the baseline criteria for standard and nonstandard parts, part type specification, and quality level for use on a given program. NASA typically uses EEE-INST-002, *Instructions for EEE Parts Selection, Screening, Qualification and Derating*, as their governing document.

NASA centers can have their own parts management plan. NSS typically uses the following technical operating reports (TORs):

- *Parts, Materials and Processes Control Program for Space and Launch Vehicles* (Aerospace Report No. TOR-2006(8583)-5235 Rev. B [27], also published as SMC-S-009) [26]
- *Technical Requirements for Electronic Parts, Materials and Processes used in Space and Launch Vehicles* (Aerospace Report No. TOR-2006(8583)-5236 Rev. B [27], also published as SMC-S-010), which provides the space quality baseline (SQB) for standard PMP [29]

Expanding Space Design Options Using COTS (Aerospace Report No. ATR-2023-01935 [36]) is a reference for PMPCB adjudication of non-mil-spec parts usage.

Part screening: Part screening establishes the baseline criteria for screening tests for flight parts to remove nonconforming parts, parts with random defects, or parts likely to experience infant mortality from an otherwise acceptable lot, increasing confidence in the reliability of the parts selected for use.

Part qualification: 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.

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.

Part stress analysis (PSA)/worst-case circuit analysis (WCCA): Electrical parts stress analysis is the process of determining a part's ability to withstand induced stresses under given thermal conditions. Induced stresses are taken from the datasheet and circuit analysis and are identified in terms of voltage, current, power, etc. Derating the maximum stresses placed on the component provides safety margins for the design. The objective of a WCCA is to verify that the circuits being analyzed perform their functions throughout their design life after considering the combined effects of expected piece-part parameter degradations caused by initial tolerance, calibration, temperature, aging, and radiation effects. See also TOR-2013-00297 [35].

Part radiation survivability: Part radiation survivability involves part evaluation identifying component risk level and informing design and part selection. Designs should employ semiconductor parts that are radiation hardened by design or have test data with wafer design traceability to demonstrate compliance to mission requirements with appropriate margin. While radiation-hardened parts will not be susceptible to destructive effects, they are still often subject to transients and upsets due to single-event effects (SEEs), which need to be considered in the design usage.

Material and process selection: Material and process selection establishes the baseline criteria for materials and processes that meet the required conditions specified for a given payload and integrated space vehicle. NASA typically uses NASA-STD-6016 *Standard Materials and Processes Requirements for Spacecraft* as their governing document. NSS typically uses *Parts, Materials and Processes Control*

Program for Space and Launch Vehicles (Aerospace Report No. TOR-2006(8583)-5235 Rev. B [27], which was also published as SMC-S-009) and *Technical Requirements for Electronic Parts, Materials and Processes Used in Space and Launch Vehicles* (Aerospace Report No. TOR-2006(8583)-5236 Rev. B, which was also published as SMC-S-010).

Procured materials control: Procured materials control consists of two components: (1) the requirements controlling the properties and source of the materials (traditionally documented in a procurement specification or source control document) and (2) the requirements controlling the receiving inspection of the procured materials, which can range from incoming inspection by the procuring contractor to acceptance of suppliers certificate of conformance (CoC).

Materials and process qualification: Materials and process qualification establishes the qualification criteria for materials and processes used in flight designs. 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.

C.3 Matrix—Parts, Materials, and Processes

Category	Class A	Class B	Class C	Class D	DNH
PMP Program Control					
PMPCB	Customer approval of nonstandard PMP through formal PMPCB.	Nonstandard PMP approved through formal PMPCB with customer participation.	Nonstandard PMP approved through PMPCB or similar forum following contractor's standard practice. Customer participation welcomed but not required.	No requirement for PMPCB or other nonstandard PMP approval forum.	Not expected—developer's choice.
PMP Selection List(s)	Standard PMP list(s) are created and maintained with customer approval.	Standard PMP list(s) are usually created and maintained and may require customer approval.	Standard PMP list(s) are not typically utilized. PMP items are approved for individual design needs.	PMP items are selected based on design need.	Not expected—developer's choice.
Traceability	All PMP items used on flight hardware require traceability to lot date code (LDC) or other production lot identifier.	All PMP items used on flight hardware require traceability to LDC or other production lot identifier.	Traceability to LDC is recommended for complex parts (e.g., microprocessors, FPGAs) and critical raw materials.	Lot traceability is not required.	Not expected—developer's choice.
EEE Parts and Radiation Effect Engineering					
Parts Selection	Highest reliability parts selected, typically Class S/V/K mil-spec parts. NASA EEE-INST-002 Level 1 parts or TOR-2006(8583)-5235 Rev. B [27]/SMC-S-009 and TOR-2006(8583)-5236 Rev. B [29]/SMC-S-010 SQB parts are standard.	Somewhat relaxed reliability-level parts may be used (i.e., Class B/Q/H mil-spec parts). NASA EEE-INST-002 Level 1 or 2 parts are standard.	Automotive Electronics Council (AEC)-qualified parts, vendor hi-rel parts, or other parts with established reliability or proven flight heritage are preferred. NASA EEE-INST-002 Level 1, 2 or 3 parts are standard.	Commercial parts are used.	Not expected—developer's choice.
Parts Screening	Parts show evidence of verification of lot acceptance through statistical process control (SPC), screening, and/or DPA. Typically, parts are screened per NASA EEE-INST-002 Level 1 or TOR-2006(8583)-5235 Rev. B [27]/SMC-S-009 and TOR-2006(8583)-5236 Rev. B [29]/SMC-S-010 SQB requirements.	Parts show evidence of verification of lot acceptance through SPC, screening, and/or DPA. Typically, parts are screened per NASA EEE-INST-002 Level 2 requirements.	Parts show evidence of verification of lot acceptance through SPC (e.g., AEC-qualified parts) or screening. NASA EEE-INST-002 Level 3 requirements when screening is necessary.	Parts are not typically screened by lot.	Not expected—developer's choice.

Category	Class A	Class B	Class C	Class D	DNH
Part Qualification	Parts are qualified at the part level per NASA EEE-INST-002 Level 1 or TOR-2006(8583)-5235 Rev. B [27]/SMC-S-009 and TOR-2006(8583)-5236 Rev. B [29]/SMC-S-010 SQB requirements.	Parts are qualified at the part level per NASA EEE-INST-002 Level 2 requirements.	Parts are rarely qualified at the part level.	Parts are not expected to be qualified at the part level.	Not expected—developer's choice.
Destructive Physical Analysis	Per MIL-STD-1580 for all parts, including those procured to military specifications. Metal surfaces verified for absence of prohibited materials (e.g., pure tin, zinc, or cadmium).	Per MIL-STD-1580 for all parts except those procured to military specifications. Metal surfaces verified for absence of prohibited materials (e.g., pure tin, zinc, or cadmium).	DPA not expected. May be recommended if there are concerns about part quality or as a part of failure investigation. Use of pure tin plating should be mitigated. Use of other heritage prohibited materials adjudicated on part-by-part basis.	DPA not expected. Use of pure tin plating should be mitigated. No requirement on prohibited materials.	Not expected on DPA or prohibited materials.
PSA/WCCA	Formal electrical PSA and WCCA required for all designs. Derating may be per NASA EEE-INST-002 or TOR-2006(8583)-5235 Rev. B [27]/SMC-S-009 requirements unless otherwise approved by the customer.	Formal electrical PSA and WCCA required for all designs. Derating may be per NASA EEE-INST-002 or TOR-2006(8583)-5235 Rev. B [27]/SMC-S-009 requirements unless otherwise approved by the customer. Reduction of scope per TOR-2013-00297 Appendix A.11 [35] may be considered.	Electrical PSA is required for all designs. Derating may be limited to NASA EEE-INST-002 or TOR-2006(8583)-5235 Rev. B [27]/SMC-S-009 criteria, but manufacturer's guard banding may be used. WCCA is recommended for critical circuits.	Electrical PSA is recommended for all designs. Derating per contractor's internal requirements. WCCA is not required.	Not expected—developer's choice.
Radiation Survivability	Testing performed at the part level, typically radiation design margin (RDM) 2X for lot-specific total intensity dose (TID) and displacement damage testing, no single-event latch-up (SEL). SEE hardness levels are identified and verified to meet program requirements.	Testing or analysis at the part level, typically RDM 2X lot-specific and 4X non-lot-specific TID and displacement damage testing, no SEL. SEE hardness levels are identified and verified to meet program requirements with appropriate mitigation strategies.	Part selection preference given to parts with previous SEE hardness testing with heavy ions and with successful TID and displacement damage, testing at RDM 1X. Assembly-level proton test approach may be used to evaluate multiple parts that do not have established radiation performance.	Part selection preference given to parts with previous radiation testing or flight heritage. Radiation testing may be omitted based on environment and operational life requirements.	Not expected—developer's choice.

Category	Class A	Class B	Class C	Class D	DNH
Materials and Processes					
Material and Process Selection	Standard materials and processes meet all applicable requirements of NASA-STD-6016 or are included in TOR-2006(8583)-5235 Rev. B [27]/SMC-S-009 and TOR-2006(8583)-5236 Rev. B [29]/SMC-S-010 SQB materials. Materials and processes with current flight heritage are preferred. Space-level processes are used where available (e.g., Institute of Printed Circuits [IPC] processes).	Standard materials and processes meet the applicable requirements of NASA-STD-6016 or are included in a program PMP requirements document or approved PMP list. Materials and processes with current flight heritage are preferred. Space-level processes should be used where available (e.g., IPC processes).	Materials and processes are selected based on design need and functional/ environmental requirements. Materials and processes selection will focus on utilization of established materials and processes with spacecraft heritage. Industry processes may be used at a lower performance class (e.g., J- STD-001 Class 3 instead of J-STD-001 Space Addendum).	Materials and processes are selected based on design need. Environmental requirements should be considered.	Not expected—developer's choice.
Procured Materials Control	Source and/or specification control and lot acceptance testing is required on each production lot of procured material.	Source and/or specification control and lot acceptance testing should be required on each production lot of procured material, but supplier CoC is acceptable.	Contractor should have a system for material source control. Supplier CoC is expected for procured materials.	Commercial materials are procured off the shelf and a supplier CoC is not required.	Not expected—developer's choice.
Material and Process Qualification	All new or changed materials or processes are qualified by testing to meet the functional and environmental requirements of the program.	All new or changed materials and processes are qualified to meet the functional and environmental requirements, but qualification by similarity is acceptable.	Qualification at the material or process level is not required. Materials and process qualification is accomplished by qualification of the completed hardware. Materials and processes with spacecraft heritage are preferred.	Materials and processes with spacecraft heritage are preferred. Standard industry processes are preferred. Qualification at the material or process level not required.	Not expected—developer's choice.

C.4 Summary of Risk Classes for PMP

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 highest reliability and most rigorously characterized PMP. PMPCB with customer participation is integrated throughout the sub/supplier chain. All new or changed parts, materials, and processes must be qualified. Source controls required on all procured materials and acceptance test for each lot/batch. EEE parts are screened or otherwise verified at lot acceptance, and DPA is performed on all parts. Part and material traceability to LDC is required. Space-level processes are used.

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. Lower-reliability parts may be used. PMPCB with customer participation. New or changed parts and materials should be qualified, but qualification by similarity is acceptable. Source controls and lot acceptance testing should be required on each production lot of procured material, but supplier CoC is acceptable. EEE parts are screened or otherwise verified at lot acceptance, and DPA is performed on all parts, except those procured to military specifications. Part and material traceability to LDC is required. Space-level processes should be used.

Class C: Adherence to a PMP plan that details PMP selection requirements is required. AEC-qualified parts, vendor hi-rel parts, or other parts with established reliability or proven flight heritage are preferred. Materials and processes selection will focus on utilization of established materials and processes with spacecraft heritage. Parts and materials are not required to be qualified at the part/material level. Parts should show evidence of verification of lot acceptance through SPC or screening, but DPA is typically not performed. Supplier CoC should be required for procured materials. Part and material traceability to LDC is recommended. Standard industry processes are used.

Class D: There is no formal PMP approval process. Commercial parts and materials are usually used. Parts and materials are not qualified at the part/material level, and there are no screening or materials acceptance test requirements. DPA is not performed. Part and material traceability to LDC is not required.

DNH: Contract requirements based on safety and contamination standards to not cause harm in the case of rideshares or determined by LV provider.

C.5 Effectiveness Tips—PMP Lessons Learned

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

Appendix D. Environmental Compatibility Analysis (ECA)

D.1 Introduction

The primary objective of an ECA is to ensure that products are designed to withstand all environmental conditions encountered in service. For space systems, especially the integrated spacecraft, risks related to ECA are critical to identify and either be eliminated or reduced to a minimum based on program constraints. For space systems, this is accomplished by:

- Defining environmental requirements
- Considering these requirements in system design and implementation
- Supporting environmental testing and evaluation
- Supporting post-launch environmental response evaluation

The ECA 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 ECA process is implemented in a mission through several paths, such as a specific application of systems engineering (e.g., 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 analyses and test methods are employed to verify the design will withstand the environments encountered in service with margin. Note that the analysis factors of safety need to be consistent with the planned test methods.

Applicable space system environments that should be considered in the ECA process are shown in Figure 3, which was adapted from the NASA Preferred Reliability Practices, Environmental Factors (PD-EC-1101). This figure also illustrates a significant complication for ECA: 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 ECA process must include factors related to the complete lifecycle of the system under development, including the build process, launch conditions, and operations. A well-written system specification addressing ECA will establish requirements for normal (benign) conditions as well as extreme episodic events, such as solar flares and geomagnetic storms. The verification plan should be reviewed by the qualification review board (QRB) as defined in section 3.6 of *Flight Unit Qualification Guidelines* (Aerospace Report No. TOR-2010(8591)-20 [72].

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

🟦	Natural Environment, Earth and Lower Atmosphere
🟩	Natural Environment, Hyper and Space
🟧	Induced Environment

1	Combine to intensify mechanical deterioration
2	Combine to intensify operational deterioration
3	Interdependent (one depends on the other)
4	Coexists with no significant combined effect
5	Weakened effect (one effect weakens the other)
6	Incompatible
7	Unknown (unlikely combination or indetermininate combined effect)
	Independent environments
*	Indicates intensification through combination is weak or doubtful

	Clouds	Fog	Freezing Rain	Frost	Fungus	Geomagnetism	Hail	Humidity	Lightning	Pollution, Air	Rain	Salt Spray	Sand and Dust	Sleet	Snow	Radiation, Solar	Temperature, High	Temperature, Low	Wind	Gravity, Low	Ionized Gases	Meteoroids	Pressure, Low, Vacuum	Radiation, Cosmic, Solar	Radiation, Electromagnetic	Radiation, Van Allen	Acceleration	Explosion	Icing	Nuclear Radiation	Shock, Pyro, Thermal	Temperature, High, Aero. Heating, Fire	Temperature, Low, Aero. Cooling	Turbulence	Vapor Trails	Vibration, Mechanical, Microphonics	Vibration, Acoustic
Clouds																																					
Fog	5																																				
Freezing Rain	3																																				
Frost	5																																				
Fungus																																					
Geomagnetism																																					
Hail	2,1	6																																			
Humidity	3	3	3	3	3																																
Lightning	3	6				2-	2,1																														
Pollution, Air	4	1						1																													
Rain	3	2		6	3	6	1,2	3	4	4																											
Salt Spray		1-	5					5			5																										
Sand and Dust		1-						1-		1-		1-																									
Sleet	3	7					6	3	6																												
Snow	3	7						3	6		2-																										
Radiation, Solar		5		5	5			1-			6	1	1-																								
Temperature, High	5	5	6	6	3			1				1	5	6	6	1																					
Temperature, Low		3	3	3	5			1			1-	5	1-	3	3	5	6																				
Wind	2-	5	7				1,2	7	1,2	3	1,2	1	1,2	1,2	1,2	1	1-	2,1																			
Gravity, Low																4	4	4																			
Ionized Gases					5			1								1	1	5		4																	
Meteoroids																																					
Pressure, Low, Vacuum					7			1								1-	1	1	5	4	3																
Radiation, Cosmic, Solar						3										3				7	1-																
Radiation, Electromagnetic						3														7	1-			3													
Radiation, Van Allen						3										3				4				3													
Acceleration								7								7		1																			
Explosion								1-								7	7	7					1-														
Icing	3	1-	2,1								1-	5				5	6	3	2-																		
Nuclear Radiation																1-	1-				1		7	7	7	7	7	7									
Shock, Pyro, Thermal																		1					1-							7							
Fire																		6											6	7	1						
Temperature, Low, Aero. Cooling																	6													7	1	6					
Turbulence	2-	6					2,1		2,1		2								2,1										2,1			7					
Vapor Trails	5		6				6	3	6	7	6			6	6	4	6	3	5																		
Vibration, Mechanical, Microphonics								1,2				1,2	1,2			1	1	1					1-				1			5		1	1	1			
Vibration, Acoustic																														7		1	1-				

Figure 3. Effects of combined environments.

D.2 Definitions for ECA

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. They are not intended as general standalone industry standard definitions.

ECA: 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: System and mission requirements definition is a process that is used to establish the design, functional, and performance requirements of a space system. The process is used to ensure the system has been validated to perform as expected during its operational lifetime.

Testing requirements: 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 requirement to include the sufficient criteria to address the requirement and its associated risks.

Natural space environment: The 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 human-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: Hardness is an attribute defining the environmental stress level that a space system can survive.

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

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

System/component environment: The 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: Contamination is the presence of minor and unwanted constituents in materials and the development and operating environments.

Outgassing: 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: Radiation is a process in which energetic particles, 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: The thermal environment is encountered by a satellite system, primarily driven by differential temperatures 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 maintain the operating temperature requirements of payloads and systems.

Dynamic environment: The dynamic environment of a spacecraft encompasses the mechanical stresses placed on a system during all phases of the lifecycle. 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.

Micrometeoroids: Micrometeoroids are small meteoroids, usually with a diameter below a few millimeters, that are not detectable with ground observation methods. Natural particles have high velocities relative to Earth or spacecraft.

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

Pressure environment: The pressure environment of a space system generally refers to the operational environment but also includes the 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: The operational environment of spacecraft is the near-perfect vacuum of space. 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.

D.3 Matrix—ECA

Category	Class A	Class B	Class C	Class D	DNH
			Program Characteristics		
ECA	Considers all mission factors, such as proposed orbit, mission life, launch factors, etc. Environmental requirements based on well-defined nominal operation mission and fault scenarios.	Same as Class A.	Considers all mission factors, such as proposed orbit, mission life, launch factors, etc. Environmental requirements based on well-defined nominal operation mission and selected fault scenarios. Fault scenarios are identified and selected by suppliers consistent with risk tolerance level.	Same as Class C.	Not expected—developer's choice.
System/Mission Requirements Definition	Requirements individually addressed in program plans. No waivers allowed on key performance parameters (KPPs) as defined in spec and/or statement of work (SOW).	Critical requirements individually addressed in program plans. Allows limited waivers on non-critical items.	Only critical mission impact requirements addressed in program plans. Waivers allowed on non-critical requirements.	Only requirements to establish minimum mission capability addressed in program plans. Waivers allowed on all requirements.	Not expected—developer's choice.
Testing	Established for each requirement. Tested to meet or exceed most stressing margins over expected lifetime of system. Must meet or exceed all established safety margins.	Same as Class A.	Established for critical requirements. Physical testing usually used to satisfy mission-critical requirements; Analysis may be used to satisfy DNH. Must meet all tailored safety margins.	Established for selected mission capability requirements. Physical testing and/or analysis used to satisfy DNH. Must meet all DNH safety margins.	Physical testing and/or analysis used to satisfy DNH. Must meet all DNH safety margins.

Category	Class A	Class B	Class C	Class D	DNH
Environmental Characteristics					
Operational Environment (Thermal, Radiation, Micrometeoroid, Space Debris, Natural Space Environments)	Fully verified 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 except for: • Tested to meet requirements with reduced margins. • Minimal use of physical testing.	Same as Class A except for: • Tested to meet requirements with reduced margins. • Minimal use of physical testing.	Not expected—developer's choice.
EMI/EMC/Magnetics	Payloads are tested to ensure noninterference with other systems and payloads. Practices follow established standards and guidelines: MIL-STD-461G, TOR-2005(8583)-1 Rev A [43], MIL-STD-1541A, and TOR-2011(8591)-5 [62].	Same as Class A except: • Analysis may replace some testing.	Same as Class B.	Analysis may replace all testing.	Analysis may replace all testing.
Mechanical Environment (Loads, Acceleration, Shock, Vibration, and Acoustics)	Fully verified 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: • 2X life testing of mechanisms recommended.	Verified for the launch and operational environment to ensure no detrimental impact to other systems and payloads. Tested to meet or exceed tailored margins for launch, and analyzed for operating environment over expected lifetime of system. Mechanism life testing not required.	Same as Class C except: • Analyzed and/or tested to meet or exceed tailored margins for launch and for operating environment over expected lifetime of system. • May be tested at space vehicle level.	Same as Class D.
Pressure Environment (Pressure, Vacuum, Venting, Contamination, Out-gassing)	Fully verified for ascent and planned orbit/position. Proof testing expected for all pressure systems.	Same as Class A.	Verified for ascent and operational environments to ensure no detrimental impact to other systems.	Same as Class C, except proof testing expected for all pressure systems.	Same as Class D except: Proof testing expected for all pressure systems.

D.4 Summary of Risk Classes for ECA

The identification and handling of ECA requirements for space systems is critical to success. ECA 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 ECA requirements.

The mission risk classes are defined section 2. Based on the issues such as risk acceptance, service lifecycle profile, and launch constraints, environmental design requirements are established for units, subsystems, vehicles, and systems. Design requirements for each mission class should tailor the design margins to ensure that the space systems and components address the worst-case service-life environments described in TR-RS-2014-00016/SMC-S-016 [65]. TR-RS-2014-00016/SMC-S-016 specifies attention be given to the following ECA 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. 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 ECA 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 ECA that considers all mission factors, such as proposed orbit, mission life, and launch factors, 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 ECA, all requirements must be verified through physical testing, and waivers are not allowed on KPPs. The required environmental design margins for Class A equipment are those specified in TR-2004(8583)-1 and TOR-2011(8591)-5 [61].

Class B: Missions and payloads are defined as high-priority, medium-risk efforts, with cost-saving compromises made primarily in areas other than design and construction. The ECA standards for Class B are similar to those for Class A. They are only somewhat less stringent but can still significantly drive the system risks and the risk mitigation strategy. All Class B missions perform an ECA that considers all mission factors, such as proposed orbit, mission life, and launch factors, 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. All requirements must be verified through physical testing and/or analysis, and limited waivers may be allowed on non-critical requirements. The required environmental design margins for Class B are specified in TR-RS-2014-00016/SMC-S-016 [65] and Aerospace Report TOR-2011(8591)-5 [61].

Class C: Missions and payloads are defined as medium-or-higher-risk efforts that are economical, reflyable, or 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. 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-RS-2014-00016/SMC-S-016 [65].

Class D: Missions and payloads are defined as high-risk, minimum-cost efforts that are economical, reflyable, or repeatable. The loss of a Class D system or payload must not negatively affect the success or mission of the primary payload, does no harm to other payloads on the space vehicle, does no harm to the launch vehicle, and does no harm to the personnel at any stage of manufacturing, integration, test, launch, and landing (if applicable).

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. The mission requirements definition is usually determined by prior experience. Only requirements needed to establish minimum mission capability are addressed in program plans. For Class D, testing is only established for DNH requirements. 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 margins for Class D equipment are similar to those specified in TOR-2011(8591)-5 [62].

DNH: Missions and payloads are defined as high-risk efforts that prioritizes schedule and cost over technical capabilities. The loss of a Class DNH system or payload must not negatively affect the success or mission of the primary payload, does no harm to other payloads on the space vehicle, does no harm to the launch vehicle, and does no harm to the personnel at any stage of manufacturing, integration, test, launch, and landing (if applicable).

D.5 Effectiveness Tips—ECA Lessons Learned

- One of the most effective means of ensuring environmental compatibility is through a well-defined and executed review process. See section 3.7 of *Flight Unit Qualification Guidelines* (TOR-2010(8591)-20 [72]).

- 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 lifecycle environment profile that contains this information should be developed.

Appendix E. Integration, Test, and Evaluation (IT&E)

E.1 Introduction

The primary objectives of IT&E are to (1) integrate space systems in a typically tiered structure comprising 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 that 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 appropriate configuration control has been maintained. Where tailoring is called out in the matrix, it is intended to be consistent with Aerospace Report TOR- 2011(8591)-5 [62]. Note that the MAIW 2010 framework called out lower-tier assemblies down to components. For the purposes of this appendix, these are considered part of hardware quality.

E.2 Definitions for IT&E

The following definitions are intended to be used to build the row entries of the risk matrix A5-3 IT&E.

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

GSE: GSE is any hardware or software required for I&T of a vehicle that is not part of the delivered vehicle.

Interfaces: Interfaces are the meeting of mechanical, electrical, or software boundaries.

Integration functional testing: Integration functional testing is performed to validate successful integration steps, which may or may not demonstrate compliance of the integrated assembly.

In-process screening: In-process screening includes inspection steps inserted during integration to validate mechanical/physical process steps.

Testing requirements compliance and validation: Testing requirements compliance and validation are test activities specifically intended to demonstrate compliance to environmental, functional, or performance requirements.

Software validation testing: Software validation testing is used to demonstrate software requirements and interface compliance and system stability.

Qualification: Qualification is the process of demonstrating that the hardware and software will perform under the required mission environments over the required mission life. See TOR-2010(8591)-20 [72] for additional information.

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

System test/external interfaces: System test/external interfaces demonstrates compliance to vehicle external interfaces, such as ground segments, relays (if applicable), and launch vehicle systems.

End-to-end system test: End-to-end system test is 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: Launch support and compatibility testing is used to validate launch vehicle interfaces as well as launch system compatibility, including command and control and telemetry.

Evaluation: Evaluation involves 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 I&T, includes the activities necessary to assess all the aspects of the I&T 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: Independent reviews are formal or informal reviews performed by SMEs outside the program office chain of command. See TOR-2011(8591)-21, Appendix B2 [61].

GSE hardware (HW) validation: GSE HW validation is the process utilized to validate the readiness of GSE HW as safe and properly configured for use on flight hardware.

GSE software (SW) validation: GSE SW validation is the process utilized to validate the readiness of GSE SW as safe and properly configured for use on flight hardware.

Integration records: Integration records are documentation kept during the integration process.

Data analysis tools: Data analysis tools are tools used to process vehicle test data to trend performance and demonstrate compliance.

Hardware acceptance: Hardware acceptance is the process of buying off hardware delivered for integration as compliant and ready. See TOR-2010(8591)-21, Appendix B3 [61].

Analysis model validation: Analysis model validation is 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: Test evaluation is the process of validating that the conditions of the test and the test results demonstrate compliance.

Test logs: Test logs are test documentation that capture the execution of steps and specific observations, which may have bearing on the system, GSE, or test results.

Test execution: Test execution is the process of demonstrating readiness for, execution of, and close-out steps from planned testing.

Nonconformances: Nonconformances are noted conditions in hardware, software, or GSE data that are outside defined operating conditions. See Appendix C1, Failure Review Board, in TOR-2011(8591)-21 [61].

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

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.

DNH mission assurance risk classification: See section 2 for definitions. Guidance for DNH requirements generation and verification can be found in TOR-2016-02946-Rev A [73].

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 subsystem 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 that, 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.

Space vehicle: 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 that 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 instrument under test (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.

E.3 Matrix—IT&E

Category	Class A	Class B	Class C	Class D	DNH
Integration	Integration follows all quality standards and processes. Reference TOR-2011(8591)-21, Appendix B3 [61].	Integration follows all quality standards and processes. Reference TOR-2011(8591)-21, Appendix B3 [61].	Integration follows all quality standards and processes, with allowances for contractor best practices. Reference TOR-2011(8591)-21, Appendix B3 [61].	Integration uses contractor best practices. Reference TOR-2011(8591)-21, Appendix B3 [61].	Not expected—developer's choice.
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 maintained by I&T team and audited by QA.	Pre-mate connector checks are implemented on all critical flight mates Electrical and mechanical mates are performed to quality standards and signed off. Mate/de-mate and installation logs are maintained.	Best practices are employed. Electrical and mechanical mates follow best practices tailored for program requirements.	Best practices are employed. Electrical and mechanical mates follow best practices tailored for program requirements.
Interface Functional Testing	All functions are tested at each level of integration. Final integration verifies complete functionality, including telemetry and command (T&C). Subsystems utilize GSE high-fidelity simulators to validate interfaces. Box and component tests utilize GSE validated against interface specs.	Final integration verifies critical functionality, including T&C. Subsystems utilize GSE simulators. Box and component tests utilize GSE validated against interface specs. Ability to defer interface functional testing to higher levels of integration.	All mission-critical functions are tested at final integration. Final integration validates critical functionality, including T&C. Ability to defer interface functional testing to higher levels of integration	All mission-critical functions are tested at final integration. Final integration validates functionality and T&C consistent with program risk posture.	Not expected—developer's choice.

Category	Class A	Class B	Class C	Class D	DNH
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	Not expected—developer's choice.
Testing—Requirements Compliance	Test data should demonstrate at least protoqualification margin to expected environments. See Appendix D	Test data should demonstrate at least protoqualification margin to expected environments. See Appendix D	Test data should demonstrate margin to expected environments. Degree of margin is per program risk posture and critical mission functions. See Appendix D	Test data should demonstrate, at minimum, the ability to meet expected environments. See Appendix D	Same as Class D.
SW Validation	SW meets all quality standards. Databases are verified through test and configuration controlled. T&C is verified through test Independent validation performed. See TOR-2011(8591)-21, Appendix B4 [61] .	SW meets standards tailored for program requirements. Databases are validated and configuration controlled. T&C is verified through test Independent validation performed. See TOR-2011(8591)-21, Appendix B4 [61].	SW based on best practices. Databases are validated and configuration controlled. T&C is validated Independent validation of critical algorithms performed. See TOR-2011(8591)-21, Appendix B4 [61].	SW based on best practices. Databases are validated. Mission-critical T&C is validated. See TOR-2011(8591)-21, Appendix B4 [61].	Not expected—developer's choice.

Category	Class A	Class B	Class C	Class D	DNH
Qualification	Qualification method selected is documented with customer approval. Qualification article and levels preferred, use of proto- qualification testing of flight units is acceptable. Subsystems and units functionally tested to relevant environments plus margin at qualification/proto-qualification levels. No unqualified parts, materials, or processes "Standard" analysis and test requirements for low-risk, first-pass quality hardware.	Qualification method selected is documented with customer review. General use of proto-qualification testing of flight units. 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. Comprehensive qualification approach (system through unit) can defer qualification testing to higher levels of integration. No unqualified parts, materials, or processes. "Standard" analysis and test requirements for low-risk, first-pass quality hardware.	Summarized qualification plan provided for customer awareness. Limited customer or other independent review. Overall qualification levels can be tailored for program risk and mission environments. Generally recommend protoqualification or flightproof levels. Contractor command media and industry best practices may be acceptable for defining appropriate qualification approach. Comprehensive qualification approach (system through unit) can defer qualification testing to higher levels of integration. Ability to leverage test data in lieu of analysis where appropriate. Ability to leverage supplier test data to support qualification.	Limited customer insight for qualification plan, with review only for verification of DNH items. Contractor command media and industry best practices are acceptable for defining appropriate qualification approach. Ability to leverage supplier test data to support qualification.	Qualification test is driven by verification of DNH. Safety and compatibility testing required by the launch vehicle provider and/or launch site. Perform minimum characterization to address DNH.

Category	Class A	Class B	Class C	Class D	DNH
Performance Testing	Performance testing verifies operability within environmental requirements. Mission profile test performed for all mission phases (test like you fly [TLYF]). Redundancy tested. Health screening tested pre and post environments.	Performance testing verifies operability within environmental requirements. Mission profile test performed for all mission phases (TLYF). Redundancy tested. Health screening tested pre and post environments	Performance testing verifies mission-critical operability, with best effort for non-mission-critical capabilities, within environmental requirements. TLYF principles applied where critical and feasible. Contractor command media and industry best practices may be used to guide tailoring. Redundancy tested. Health screening tested pre and post environments.	Performance testing verifies mission-critical operability within environmental requirements, with wider test tolerances relative to Class C and fewer mission-critical performance verification requirements than Class C. Limited mission profile test performed. Health screening tested pre and post environments.	Performance testing verifies safety-critical operability within environmental requirements. Any other performance testing is "best effort."

Category	Class A	Class B	Class C	Class D	DNH
Launch Support and Compatibility Tests	Full Compliance to TR-RS-2014-00016/SMC-S-016 [65]. Pre-compatibility test performed generally at contractor factory with Air Force Satellite Control Network (AFSCN)/Defense Switch Network (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 (radio frequency [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 TR-RS-2014-00016/SMC-S-016 [65]. 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 TR-RS-2014-00016/SMC-S-016 [65]. 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.	Not expected—developer's choice.
GSE HW Validation	GSE is configuration controlled and anomaly root cause corrective action (RCCA). GSE is validated as meeting GSE requirements as well as being safe for use on flight HW.	GSE is configuration controlled and anomaly RCCA. GSE interface requirements are verified and are certified as safe to use on flight HW.	GSE is configuration controlled and deemed to be safe to use on flight HW. GSE interface requirements are verified consistent with program risk posture	GSE is deemed as safe to use on flight HW. GSE interface requirements are validated consistent with program risk posture.	Not expected—developer's choice.
GSE SW Validation	GSE SW treated as flight SW.	GSE SW configuration controlled and validated like flight SW.	GSE SW is validated and version control maintained.	GSE SW is validated.	GSE SW is safe to use.

Category	Class A	Class B	Class C	Class D	DNH
Acceptance Testing	Recurring workmanship screening performed on all post-qualification vehicles/hardware.	Recurring workmanship screening performed on all post-qualification vehicles/hardware.	Recurring workmanship screening may be reduced or eliminated.	Recurring workmanship screening may be reduced or eliminated.	Developer's choice.
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 SMEs 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 SMEs review test reports	Test reports are generated and customer reviewed at system and subsystem level consistent with contractor best practices. Review and approval of test reports per contractor best practices.	Test reports are generated and delivered at system level consistent with contractor best practices. Review and approval of test reports per contractor best practices.	Test reports generated for verification of DNH.
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 test logs monitored and audited.	Informal test logs maintained. Limited (if any) independent review.	Informal test logs maintained.
Test Execution	Independent (customer and/or contractor) review of contractor test plans, procedures, setup, execution, and data analysis. Customer approves break of configuration (BOC) reviews and test readiness reviews (TRRs) at system and subsystem levels.	TRRs, post-test reviews and BOC reviews are performed. Independent (customer and/or contractor) review of critical items and survey of processes and procedures.	Limited customer involvement during system and subsystem test activities. Critical test setups, procedures, and data may be reviewed based on program risk posture. Some independent review.	Customer awareness of system test, no independent review.	Only customer involvement for DNH requirements.

E.4 Summary of Risk Classes for IT&E

Class A: 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 TLYF compliance
- Customer and contractor independent reviewer engagement down to subsystem levels and integration readiness reviews (IRRs)
- All telemetry and databases are verified and configuration controlled
- Formal MRB/FRB with customer approval of nonconformances
- Customer attends and approves TRRs and BOCs, independent (customer and/or contractor) review of test setups, data analysis, and test execution
- Customer reviews and approves all test plans, procedures, and test reports

Class B: Key characteristics for IT&E, which differ from Class A include:

- Customer attends TRRs and BOCs, independent (customer and/or contractor) survey of test setups, 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: Key characteristics for IT&E include:

- Minimal independent or customer review throughout, with emphasis on the mission-critical requirements
- Tailoring is performed throughout and may be a combination of contractor command media and industry best practices

- GSE follows contractor best practices
- SW follows contractors best practices
- Limited DITL test, system test performed at launch site, possibly enabled by RF GSE
- GSE SW is validated and version controlled
- Qualification approach shows margin to expected environments, with reduced analysis scope when compared to Classes A and B. Qualification data is a combination of analysis, test, and/or industry test data
- Recurring workmanship screening may be reduced or eliminated, pending QRB approval

Class D: 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 audit processes and mission-critical activities consistent with program risk posture
- Customer reviews plans, procedures, and reports and interacts at established program reporting milestones

DNH: Key characteristics for IT&E include:

- Customer engagement limited to DNH requirements
- Integration uses contractor best practices
- GSE HW and SW comply with safety standards and DNH requirements
- SW follows contractor’s best practices
- Qualification approach driven by program requirements and DNH requirements. Qualification data beyond the aforementioned requirements are “best effort” capabilities, with significant margin for acceptable thresholds

E.5 Effectiveness Tips—IT&E 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 I&T 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.

- The degree of customer and independent SME involvement throughout IT&E heavily influences cost and schedule. A high degree of external oversight may result in a less risk-tolerant risk classification due to the influence on execution. Consideration upfront of external oversight, insight, and awareness is strongly recommended for aligned expectations between the contractor and the customer.

- Model V&V should be started early in the program lifecycle so that deficiencies in available data can be addressed in program planning.

- Determining root cause is essential in resolving I&T issues so that they do not reoccur or are repeated elsewhere in the system. However, for more risk-tolerant missions, it is critical to define the extent to which the root cause is identified. Part of a more risk-tolerant mission assurance posture is also accepting the possibility of not understanding the true root cause.

- Increased reliance on contractor command media and industry best practices should be leveraged as risk tolerance increases. Part of accepting a greater degree of risk (and reducing cost and schedule) is to limit the number of "cooks in the kitchen." At the time of this writing, the number of risk-tolerant missions is rapidly increasing. It is prudent to continuously learn from the industry's collective experiences and recognize where things may need to change—be it technically or non-technically. Maintaining flexibility in risk-class-specific approaches is critical for efficient use of resources and agile execution. Adherence to industry guidelines or white papers should not outrank data-driven decisions—especially on programs that do not have the cost or schedule margin to absorb bureaucracy.

- Integration requires an effective MRB and FRB set of processes with customer and independent reviewers engaged so that issues are resolved expeditiously.

AEROSPACE REPORT NO.
ATR-2023-01889

Mission Assurance Guidelines for Mission Risk Classes and Do No Harm (DNH) for Space Vehicles

Cognizant Program Manager Approval:

Barbara M. Braun, PRINCIPAL DIRECTOR
CORPORATE CHIEF ENGINEERS OFFICE
OFFICE OF EVP

Aerospace Corporate Officer Approval:

Mark J. Silverman, CHIEF ENGINEER/GENERAL MANAGER
OFFICE OF EVP

Content Concurrence Provided Electronically by:

Jeff B. Juranek, SENIOR PROJECT LEADER
ENGAGEMENTS
ENTERPRISE SYSTEMS ENGINEERING
CORPORATE CHIEF ENGINEERS OFFICE

Office of General Counsel Approval Granted Electronically by:

Kien T. Le, ASSISTANT GENERAL COUNSEL
OFFICE OF THE GENERAL COUNSEL
OFFICE OF GENERAL COUNSEL & SECRETARY

SY1265

AEROSPACE REPORT NO.
ATR-2023-01889

Mission Assurance Guidelines for Mission Risk Classes and Do No Harm (DNH) for Space Vehicles

Export Control Office Approval Granted Electronically by:

Angela M. Farmer, SECURITY SUPERVISOR
GOVERNMENT SECURITY
SECURITY OPERATIONS
OFFICE OF THE CHIEF INFORMATION OFFICER

SY1265