NASA/SP-20250002210
Version 1.0
March 2025

GUIDANCE ON THE IMPLEMENTATION OF AN OBJECTIVES-DRIVEN, RISK-INFORMED, AND CASE-ASSURED FRAMEWORK FOR SAFETY AND MISSION SUCCESS

National Aeronautics and Space Administration

NASA/SP-20250002210
Version 1.0

Cover Image: The Earth-orbiting Hubble telescope snapped this picture on June 26, 2001, when Mars was approximately 43 million miles (68 million km) from Earth. Hubble can see details as small as 10 miles (16 km) across. Especially striking is the large amount of seasonal dust storm activity seen in this image. One large storm system is churning high above the northern polar cap (top of image), and a smaller dust storm cloud can be seen nearby. Another large dust storm is spilling out of the giant Hellas impact basin in the Southern Hemisphere (lower right).

Comments, questions, and suggestions regarding this document can be sent to:

Dr. Homayoon Dezfuli
NASA Technical Fellow
Office of Safety and Mission Assurance (OSMA)
NASA Headquarters
hdezfuli@nasa.gov or

Dr. Elaine E. Seasly
Director, Mission Assurance Standards & Capabilities Division
Office of Safety and Mission Assurance
NASA Headquarters
elaine.e.seasly@nasa.gov

National Aeronautics and Space Administration
NASA Headquarters Washington, D.C. 20546
March 2025

ACKNOWLEDGEMENTS

The authors would like to thank the NASA Office of Safety and Mission Assurance (OSMA) for sponsoring the development of this guidance and the development of the objectives-driven, risk-informed, and case-assured framework for S&MS it describes.

Authors:

Homayoon Dezfuli, NASA Headquarters

Chris Everett, Idaho National Laboratory

Frank Groen, NASA Headquarters

Mary Skow, NASA Headquarters

Matthew Forsbacka, NASA Headquarters

This document was developed in stages and benefitted from the valuable input and feedback from the following Reviewers and Contributors:

Alfredo Colón, NASA Headquarters

Anthony DiVenti, NASA Headquarters

Chet Everline, Jet Propulsion Laboratory

Donald Helton, NASA Headquarters

Steven Hirshorn, NASA Headquarters

Chas Hoff, Glenn Research Center

Vicky Hwa, NASA Headquarters

Shandy McMillian, NASA Headquarters

Johnny Nguyen, NASA Headquarters

Tracy Osborne, NASA Headquarters

Jeannette Plante, NASA Headquarters

Robert Youngblood, Idaho National Laboratory

FOREWORD

This NASA guidance document defines an "S&MS assurance framework" for assuring acceptable levels of safety and mission success (S&MS) risk for space flight programs and projects that is consistent with NASA policy directive NPD 8700.1, NASA Policy for Safety and Mission Success, and NPR 8000.4, Agency Risk Management Procedural Requirements. The framework requires the development of program-specific and project-specific S&MS risk postures defining acceptable levels of S&MS risk. It defines a process for incorporating adherence to an S&MS risk posture into S&MS planning throughout the program or project life cycle. It requires the development of an S&MS assurance case that evolves over the program or project life cycle and argues, supported by evidence, that the S&MS risk posture is being adhered to.

This guidance document can be used as a template for incorporating objectives-driven, risk-informed, and case-assured S&MS into the NASA directives structure, e.g., via the development of a NASA Procedural Requirements (NPR) document that directly implements NPD 8700.1 and is inclusive of both crewed and robotic missions.

This guidance document is consistent with the life-cycle management model of NPR 7120.5, NASA Space Flight Program and Project Management Requirements, leveraging the success criteria and life-cycle reviews (LCRs) defined therein to provide ongoing S&MS assurance throughout the duration of the program or project.

This guidance document has been developed to be applicable to NASA space flight programs and projects but can be adapted to non-NASA space flight contexts. It is meant to establish and promote a high level of managerial and technical excellence with respect to S&MS assurance throughout NASA and the space flight industry generally. It is consistent with Space Policy Directive-2, Streamlining Regulations on Commercial Use of Space, which promotes replacing prescriptive requirements in the commercial space flight launch and re-entry licensing process with performance-based criteria.

This guidance document supports NASA's implementation of the philosophy of risk leadership articulated in NPD 1000.0, NASA Governance and Strategic Management Handbook. It is expected to facilitate NASA's evolution away from an approach to acceptable S&MS risk based substantially on compliance with prescribed S&MS-related technical and process requirements, to an objectives-driven, risk-informed, and case-assured approach that allows for flexibility in requirements definition, accommodates diversity in design, management, and acquisition strategy, and fosters innovation in the means by which NASA and its partners safely achieve their space flight goals and objectives.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GUIDANCE ON THE IMPLEMENTATION OF AN OBJECTIVES-DRIVEN, RISK-INFORMED, AND CASE-ASSURED FRAMEWORK FOR SAFETY AND MISSION SUCCESS

1. INTRODUCTION

1.1 Purpose

1.1.1 This guidance document describes an objectives-driven, risk-informed, and case-assured approach to safety and mission success (S&MS)[1] for NASA space flight programs and projects that aligns with the philosophy of risk leadership set forth in NPD 1000.0 [1][2], and which codifies the intent of NPD 8700.1 policy to assure acceptable levels of flight crew safety and mission success risk [2]. This guidance document is consistent with NPR 8000.4 requirements for programmatic decisions to accept S&MS risks within an established risk posture [3]. It is compatible with the program and project management requirements of NPR 7120.5 [4] and NPR 7120.8 [5]; the acquisition policy of NPD 1000.5 [6], and the systems engineering requirements of NPR 7123.1 [7].

1.1.2 The NPD 8700.1 policy to assure acceptable levels of flight crew safety and mission success risk is centered around the establishment of and adherence to a *risk posture* for crew safety and mission success consisting of acceptable levels of risk for their missions and crews, i.e., acceptable levels of crew safety and mission success risk. Because these are emergent properties that are not objectively verifiable in the traditional sense[3], NPD 8700.1 utilizes the concept of the *assurance case* as the vehicle for assuring that crew safety and mission success are within the established risk posture or are on track for being so.

1.1.3 This guidance document defines an *S&MS assurance framework* that can be used to implement NPD 8700.1 policy to assure acceptable levels of flight crew safety and mission success risk. It defines the principal actors in the framework; describes their roles and responsibilities; provides illustrative implementing requirements in the form of **shall**, **should**, and **may** statements; and provides implementation guidance on a number of core framework elements.

1.1.4 The S&MS assurance framework defined in this guidance document builds on existing practices for case-based assurance[4] but is tailored to NASA's governance model and the acquisition, management, and systems engineering practices of its space flight programs and projects. Its intent is to integrate NPD 8700.1 policy to assure acceptable levels of flight crew

[1] See Section 3.2 for a definition and brief discussion of the term "S&MS."

[2] Section 2.2 contains the list of documents referenced in this guidance document.

[3] Because of the probabilistic nature of risk, safety and mission success likelihood are demonstrable in only in the limit of many identical, or at least equivalent, missions.

[4] References to a number of resources relating to case-based assurance can be found in Section 11.

safety and mission success risk into existing NASA process, rather than to establish a separate and/or parallel process.

1.1.5 In the S&MS assurance framework, acceptable S&MS risk is defined in terms of an explicitly established *S&MS risk posture*, and the claim that the S&MS risk posture is being adhered to is made by an *S&MS assurance case* that evolves throughout the program or project life cycle.[5] In general, assurance cases provide a level of structure and formalism that is highly supportive of NASA's ongoing digital transformation initiatives, such as model-based systems engineering and model-based mission assurance.

1.1.6 The S&MS assurance framework is designed to allow substantial flexibility in the specific means by which programs and projects adhere to the S&MS risk postures established for them. Such flexibility is necessary to accommodate the increasingly broad range of acquisition strategies employed by NASA (e.g., commercial transportation services) and the increasingly rapid evolution of space flight-related technologies and practices (e.g., agile mission assurance [8]). This contrasts with traditional approaches to S&MS that largely rely on compliance with predefined and often extensive sets of prescribed S&MS-related technical and process requirements.

1.1.7 The S&MS assurance framework includes provisions by which *Acquirers* and *Providers* come to agreements throughout a space flight program or project life cycle on what counts as sufficient S&MS assurance for the specific program or project in question.[6] This ensures an adequate level of Acquirer insight into Provider activities, while also providing a basis for Acquirer oversight activities designed to keep the Provider on track to adhering to the S&MS risk posture established for the program or project. It enables a graded approach to S&MS assurance, whereby the level of effort dedicated to S&MS assurance is commensurate to the specific assurance needs of the Acquirer for the program or project in question.

1.1.8 The framework as presented herein assumes a single life-cycle review (LCR) at the end of each life-cycle phase, such that the satisfaction of the *S&MS success criteria* established for each LCR is the primary basis for proceeding to the next life-cycle phase insofar as S&MS is concerned.[7,8] It is intended that in actual application, the S&MS assurance framework will be adapted to the life-cycle structure of the implementing program or project, which may have multiple LCRs within a given life-cycle phase, or which may contain major decision points that are not related to life-cycle phase transitions.[9] As such, this guidance document does not advocate for any specific life-cycle phases or LCRs. Instead, it is meant to accommodate the potentially

[5] *S&MS risk posture* and *S&MS assurance case* are central concepts in the S&MS assurance framework. They are used throughout this guidance document and are discussed in Sections 6 and 11 respectively.

[6] *Acquirers* and *Providers* are central actors in the S&MS assurance framework. They are discussed in Section 4. The term *Provider* as used in this guidance document is synonymous with the term *Supplier* as used in NPD 1000.5 [6].

[7] *S&MS success criteria* are central components of the S&MS assurance framework. They are discussed in Section 8.

[8] The full scope of LCR-specific success criteria, of which S&MS success criteria are a part, is discussed in [7].

[9] For example, NPR 8715.24, Planetary Protection Provisions for Robotic Extraterrestrial Missions [9], specifies (as a **should** statement) the development of an assurance case to make informed decisions regarding: (1) Initiation of return activities to the Earth-Mood system; (2) Verification and validation of flight system return reliability; (3) Recommendation to federal authorities for Earth entry and landing of returned samples; (4) Post-landing assessment and verification of sample containment; and (5) Sample release from containment.

wide variety of program and project structures that may be associated with non-traditional acquisition strategies.

1.1.9 The framework as presented herein assumes a single mission concept for each program or project, with a corresponding S&MS risk posture. This is consistent with programs and projects involving a single mission or repeated missions of the same type. It is intended that programs and projects involving multiple missions of different types (e.g., presenting different risks to different at-risk entities and accomplishing different technical objectives) will have multiple S&MS risk postures established for them – one for each mission type.

1.1.10 Additional discussion of the S&MS assurance framework can be found in the paper, "Implementing an Objectives-Driven, Risk-Informed, and Case-Assured Approach to Safety and Mission Success at NASA" [10].

1.2 Scope

1.2.1 The primary focus of this guidance document is *S&MS assurance*, i.e., the means by which a NASA Acquirer can have justified confidence that its space flight missions will be safe and successful. It defines a process by which NASA Acquirers can be assured that the Providers they oversee ensure acceptable S&MS risk, defined in terms of an explicitly established and stated S&MS risk posture. As such, S&MS assurance is predicated on S&MS ensurance.

1.2.2 The scope of this guidance document is space flight. The appropriateness of this guidance document to aeronautics has not been evaluated.

1.2.3 The scope of mission safety addressed by this guidance document includes all entities put at risk of harm by the execution of the mission, including crew, ground personnel, the public, assets, the terrestrial environment, and extra-terrestrial environments. As such, it is somewhat more expansive than NPD 8700.1 policy to assure acceptable levels of flight crew safety and mission success risk, which specifies the establishment, for each mission, of a risk posture for crew safety (and mission success), rather than for the safety of all at-risk entities (e.g., the public).[10] The scope of safety addressed by this guidance document does not include entities put at risk of harm by operations and activities that are distinct from mission execution, such as those associated with manufacturing and training.[11]

1.2.4 This guidance document addresses:

a. The establishment by NASA Acquirers of a program or project S&MS risk posture, comprising: 1) mission-level *S&MS risk tolerances* that define Acquirer expectations for the likelihoods that mission technical objectives will be accomplished and that people, assets, and

[10] This supports a holistic approach to S&MS risk management that addresses all at-risk entities within an integrated risk management framework.

[11] For example, crew safety in the context of this guidance document is not intended to address the safety of the crew during training exercises at the Neutral Buoyancy Laboratory.

environments put at risk by the mission will not be adversely affected; and 2) an expectation that the mission will be as safe as reasonably practicable (ASARP).[12]

b. The planning by Providers, and approval of planning by Acquirers, for adherence to the established S&MS risk posture, including commitments to support Acquirer audit, investigation, and reporting needs.[13]

c. The development and maintenance by Providers of an evolving S&MS assurance case that argues, with evidence, that the program or project is adhering to the established S&MS risk posture.

d. The evaluation by the Acquirer at each LCR of the evolving S&MS assurance case as the primary basis for Acquirer acceptance of the S&MS risk as it is understood at the time. The assurance derived from the S&MS assurance case factors into decisions to grant the Provider the authority to proceed through the program or project life cycle.

1.2.5 Space flight mission S&MS risk depends not only on "hard" factors such as system design and operational procedures, but also on "soft" factors such as safety culture, management practices, adequacy of budgets and schedules, and organizational structure. Providers' S&MS assurance cases are expected to address all factors, both "hard" and "soft," that are relevant to adhering to the established S&MS risk posture.

1.2.6 It is not the intention of this guidance document to promulgate specific strategies for engineering and operating safe and successful space flight systems, performing risk analyses, implementing hazard controls, and the like. Such system safety, systems engineering, and risk management issues are addressed by other NASA directives and guidance documents (e.g., [11], [12], [13], [14]).

1.3 Applicability

1.3.1 This guidance document is applicable to:

a. NASA programs and projects subject to NPR 7120.5 [4] or NPR 7120.8 [5].

b. Any NASA space flight programs and projects that follow life-cycle-based management practices that include the establishment of functionally distinct life-cycle phases, LCRs, and key decision points (KDPs) requiring assurance of acceptable S&MS risk.

[12] Meeting S&MS risk tolerances is *necessary* for adherence to the S&MS risk posture, but not *sufficient* for adherence to it if safer solutions could have been practicably implemented but were not.

[13] This guidance document uses the term "adhering to" to refer to the status of the program or project with respect to the S&MS risk posture in recognition that the achievement and maintenance of acceptable S&MS risk requires a sustained effort throughout the entirety of the program or project life cycle and factors into all program or project decision-making affecting S&MS risk.

c. All NASA space flight acquisition strategies, including in-house system development and mission execution, turnkey system acquisition, and commercial transportation service acquisition.

d. Both crewed and robotic NASA missions.

2. REFERENCED DOCUMENTS

2.1 General

2.1.1 The documents listed in this section are referenced in this guidance document to provide background, context, and/or additional guidance to the material presented herein.

2.2 List of Referenced Documents

2.2.1 The following list indicates the reference number of each document referenced in this guidance document. References are made using square-bracket notation (i.e., [*reference number*]).

1.	NPD 1000.0	NASA Governance and Strategic Management Handbook
2.	NPD 8700.1	NASA Policy for Safety and Mission Success
3.	NPR 8000.4	Agency Risk Management Procedural Requirements
4.	NPR 7120.5	NASA Space Flight Program and Project Management Requirements
5.	NPR 7120.8	NASA Research and Technology Program and Project Management Requirements
6.	NPD 1000.5	Policy for NASA Acquisition
7.	NPR 7123.1	NASA Systems Engineering Processes and Requirements
8.	The Aerospace Corporation	Adaptive Mission Assurance
9.	NPR 8715.24	Planetary Protection Provisions for Robotic Extraterrestrial Missions
10.	PSAM17 Proceedings, Japan	Implementing an Objectives-Driven, Risk-Informed, and Case-Assured Approach to Safety and Mission Success at NASA
11.	NASA/SP-2010-580	NASA System Safety Handbook, Volume 1: System Safety Framework and Concepts for Implementation
12.	NASA/SP-2014-612	NASA System Safety Handbook, Volume 2: System Safety Concepts, Guidelines, and Implementation Examples
13.	NASA/SP-2016-6105	NASA Systems Engineering Handbook, Rev2
14.	NASA/SP-2024-3422	NASA Risk Management Handbook, Version 2
15.	NPR 7120.10	Technical Standards for NASA Programs and Projects
16.	NPR 8705.4	Risk Classification for NASA Payloads
17.	NPR 8705.2	Human-Rating Requirements for Space Systems

18. Decision Memorandum for the Administrator, NASA	Agency's Safety Goals and Thresholds for Crew Transportation Missions to the International Space Station (ISS)
19. NPR 8715.5	Range Flight Safety Program
20. NASA-STD-8719.25	Range Flight Safety Requirements
21. NASA-TM-2005-214062	Exploration Systems Architecture Study (ESAS)
22. NASA/SP-20210010952	Human Systems Integration Handbook
23. NASA/SP-2010-576	NASA Risk-Informed Decision Making Handbook
24. Safety-Critical Systems Symposium, UK	A Methodology for Safety Case Development
25. University of York, UK	The Goal Structuring Notation – A Safety Argument Notation
26. claimsargumentsevidence .org	CAE Framework
27. ISO/IEC 15026	Systems and Software Engineering – Systems and Software Assurance

3. ACRONYMS AND DEFINITIONS

3.1 Acronyms and Abbreviations

Adm	Administrator
AIM	Assurance Implementation Matrix
AoA	Analysis of Alternatives
ASARP	As Safe As Reasonably Practicable
BAT	Best Available Technology
CAE	Claims, Arguments, Evidence
CDR	Critical Design Review
CERR	Critical Event Readiness Review
ConOps	Concept of Operations
DR	Decommissioning Review
DRM	Design Reference Mission
DRR	Disposal Readiness Review
FFRDC	Federally Funded Research and Development Center
FRR	Flight Readiness Review
GSN	Goal Structuring Notation
HSI	Human Systems Integration
ISS	International Space Station
KDP	Key Decision Point
LCR	Life-Cycle Review
LOC	Loss of Crew
LOM	Loss of Mission
MCR	Mission Concept Review
MD	Mission Directorate

MDR	Mission Definition Review
MRR	Mission Readiness Review
NASA	National Aeronautics and Space Administration
NPD	NASA Policy Directive
NPR	NASA Procedural Requirements
ORR	Operational Readiness Review
OSMA	Office of Safety and Mission Assurance
P(LOC)	Probability of Loss of Crew
P(LOM)	Probability of Loss of Mission
PBS	Product Breakdown Structure
PDR	Preliminary Design Review
PFAR	Post-Flight Assessment Review
PLAR	Post-Launch Assessment Review
PRR	Production Readiness Review
PSAM	Probabilistic Safety Assessment and Management
QA	Quality Assurance
RIDM	Risk-Informed Decision Making
RISR	Risk-Informed Selection Report
S&MS	Safety and Mission Success
SAR	System Acceptance Review
SDR	System Definition Review
SE	Systems Engineering
SEMP	Systems Engineering Management Plan
SIR	System Integration Review
SMA	Safety and Mission Assurance

SMAP	Safety and Mission Assurance Plan
SRB	Standing Review Board
SRR	System Requirements Review
TA	Technical Authority
UU	Unknown and/or Underappreciated
V&V	Verification and Validation

3.2 Definitions

Acquirer. A NASA organization that tasks another organization (either within NASA or external to NASA) to produce a system or deliver a service.

As Safe as Reasonably Practicable (ASARP). A mission is ASARP if it employs the safest means of achieving its technical objectives within programmatic constraints (e.g., on cost and schedule). In practice, this entails prioritizing safety in decision-making throughout the program or project life cycle insofar as is practical. The ASARP objective is separate and independent from any safety risk tolerances that may be levied on the mission to define thresholds of acceptable safety.

Assure. See S&MS Assurance.

Assurance Implementation Matrix (AIM). An Assurance Implementation Matrix is used by NASA robotic projects to document their planned implementation consistent with the mission or instrument risk classification defined in NPR 8705.4 [16].

At-Risk Entities. Those persons, assets, and environments put at risk of harm by the execution of the mission.

Ensure. See S&MS Ensurance.

Graded Approach. The application of process at a level of detail and rigor that adds value without unnecessary expenditure of resources, such that the resources and level of effort are commensurate with the stakes and the complexity of the decision situations being addressed. The application of a graded approach to processes reflects NASA's ethical obligation to responsibly steward the resources allocated to it.

Insight. An element of Acquirer surveillance that monitors Provider efforts to successfully conduct program or project activities. Insight is a continuum that can range from low intensity, such as reviewing reports, to high intensity, such as performing surveys and reviews. In the context of the S&MS assurance framework, insight includes reviews of S&MS-related planning, the arguments for the validity of S&MS-related plannning, the (evolving) S&MS assurance case, as well as other reviews, audits, inspections, and evaluations that are negotiated between Acquirer and Provider.

Mission Objective. An explicitly established and stated desired outcome of a mission. Mission objectives include mission technical objectives, which relate to the purpose for which the mission is conducted (e.g., Collect 10 kg of lunar regolith and return it to Earth); mission safety objectives, which relate to the protection of relevant at-risk entities (e.g., Return crew safely to Earth, protect the public from reentry debris); as well as objectives in other mission execution domains such as cost and schedule. Mission objectives are defined at the mission level. Mission objectives are deterministic – they are either achieved or not achieved in any given instance of mission execution.

Mission Safety Objective. See Mission Objective.

Mission Success. A mission outcome in which all mission technical objectives have been met. Mission success can be whole, where all mission objectives are fully met, or partial, where some mission objectives are not met or are only partially met.

Mission Success Risk. The likelihoods that mission technical objectives will not be achieved.

Mission Technical Objective. See Mission Objective.

Objectives-Driven. The character of an operation or activity in which decisions and actions (pertaining to system definition, concept of operations, requirements definition, process execution, performance monitoring, mission execution, etc.) are explicitly derived from the fundamental purposes for which it is conducted. In the context of S&MS, the fundamental purpose is to adhere to the established S&MS risk posture.

Oversight. The scope of authority that the Acquirer has over the Provider's efforts to successfully conduct program or project activities. In the context of the S&MS assurance framework, oversight includes LCR-specific S&MS success criteria approval, S&MS-related planning approval (both initial program-wide or project-wide planning as well as life-cycle-phase-specific planning), approval of S&MS evidence specifications, authority to levy corrective actions as a condition of approval to proceed through KDPs, and approval to proceed through KDPs.

Program Objective. An explicitly established and stated desired outcome of a program. Program objectives typically fall into categories such as safety, technical, cost, and schedule.

Project Objective. An explicitly established and stated desired outcome of a project. Project objectives typically fall into categories such as safety, technical, cost, and schedule.

Provider. A NASA or contractor organization that is tasked by an accountable organization (i.e., the Acquirer) to produce a product or service. Synonymous to the term "Supplier" as used in NPD 1000.5 [6].

Risk Leadership. The application by the leaders, managers, and execution staff of an activity or project of a clear and consistently shared identification and communication of

the activity priority objectives, and of the associated risk posture to be applied in the pursuit and execution of such objectives.

Risk Posture. An expression of the risks an Acquirer is willing to accept in pursuit of mission technical objectives. It is defined up front and in tandem with the development of the mission objectives, and serves as the attitudinal framework for seeking a balance between the benefit of achieving the objectives vs. the potential costs of failure. The risk posture addresses risks to objectives in all relevant mission execution domains (e.g., safety, technical, cost, schedule) and provides the fundamental basis for determinations that the risks are acceptable. (Adapted from [3].)

Risk Tolerance. An expression of the limit of acceptable likelihood of a shortfall with respect to the achievement of an explicitly established and stated mission objective (e.g., ensure that the probability of returning 10 kg of lunar regolith to Earth is at least 90%; ensure that the probability of loss of crew is below 1 in 250; ensure that the probability of cost overrun is below 20%; ensure that the probability of mission success is consistent with that of Mission Type X generally"). Risk tolerances may be expressed quantitatively or qualitatively, and in absolute or relative terms.

S&MS. The union of the domains of *safety* and *mission success*. When used as a compound subject (e.g., as in "this guidance describes an approach to S&MS"), the term "S&MS" refers to the protection of at-risk entities from harm due to mission execution and the accomplishment of mission technical objectives. When used as an adjective modifier (e.g., as in "decisions to accept S&MS risks"), the term "S&MS" narrows the scope of the modified noun to safety and mission success (e.g., "S&MS risks" refers to risks to mission safety objectives and mission technical objectives but not risks to cost objectives or schedule objectives).

S&MS Assurance. Grounds for justified confidence on the part of the Acquirer that the Provider is adhering to the established S&MS risk posture.

S&MS Assurance Case. A compelling, comprehensible, and valid argument, supported by evidence, that a Provider is adhering to the established S&MS risk posture.

S&MS Ensurance. Program or project activities conducted by the Provider for the purpose of adhering to the established S&MS risk posture.

S&MS Evidence. Artifacts that collectively substantiate to the satisfaction of the Acquirer the that the S&MS success criteria have been met and that the Provider is adhering to the S&MS risk posture. S&MS evidence provides the evidentiary basis for the claims of the S&MS assurance case, and as such is an integral part of the S&MS assurance case.

S&MS-Related Planning. That part of the Provider's program or project planning that is conducted for the purpose of adhering to the established S&MS risk posture and complying with externally mandated and/or Acquirer-levied S&MS-related technical and process requirements. This includes the selection of standards (NASA and/or alternate) and derived requirements to which the Provider commits. This guidance document does

not take a position with respect to which particular planning document(s) contains the Provider's S&MS-related planning (e.g., SMA Plan (SMAP), Systems Engineering Management Plan (SEMP), Program Plan, Project Plan). Such decisions are the purview of the individual Providers, subject to any Acquirer requirements that might be levied on them.

S&MS Risk. The likelihoods that mission safety objectives and mission technical objectives will not be achieved.

S&MS Risk Posture. That part of the overall program or project risk posture that establishes the acceptability to the Acquirer of a given S&MS risk. A program's or project's S&MS risk posture comprises the risk tolerances associated with the mission safety and technical objectives, along with the expectation that the mission will be ASARP. The S&MS risk posture may be expressed quantitatively and/or qualitatively, and in absolute or relative terms.

S&MS Success Criteria. Specific accomplishments that need to be satisfactorily demonstrated at each LCRs to assure the Acquirer that the Provider is adhering to the established S&MS risk posture. Satisfaction of an LCR's S&MS success criteria factors into the granting by the Acquirer to the Provider the authority to proceed further in the program or project life cycle. S&MS success criteria are developed by the Provider and approved by the Acquirer during initial S&MS-related planning.

Safety. Freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment.[14]

Safety and Mission Success. See S&MS.

Safety Risk. The likelihoods that mission safety objectives will not be achieved.

Technical Risk. The likelihoods that mission technical objectives will not be achieved.

[14] In the context of space flight, the environment includes orbital and planetary environments. In these environments, safety includes freedom from hazards such as space radiation and micrometeoroid and orbital debris.

4. ESTABLISHING ROLES AND RESPONSIBILITIES

4.1 Introduction

4.1.1 The roles and responsibilities in this guidance document are defined generically in that they refer to the generic organizational entities: Acquirer, Provider, TA, and SRB. This guidance document makes no assumptions about the organizational or management structures within these entities. Guidance for identifying the specific individuals in an organization who are responsible for framework implementation is provided in Section 5.2.

4.1.2 Acquirer and Provider entities reside within NASA's programmatic hierarchy (including commercial providers). TA and SRB entities are part of NASA's system of independent checks and balances and reside outside NASA's programmatic hierarchy. Section 12 provides additional discussion of S&MS assurance within the NASA programmatic hierarchy.

Note: A given organizational entity can be either an Acquirer, a Provider, or both, depending on the context. An organization that provides a system or service to an acquiring organization is a Provider, from the point of view of the acquiring organization. If that same organization meets its obligations to the acquiring organization by contracting out a portion of the effort, it additionally becomes an Acquirer with respect to the supporting contractor organization.

4.2 Acquirer (NASA entity)

4.2.1 An Acquirer is a NASA organization that tasks another organization (either within NASA or external to NASA) to produce a system or deliver a service. Acquirers are responsible for explicitly establishing S&MS risk postures for the programs and projects under their purview, overseeing Provider efforts to adhere to the S&MS risk postures established for them, and accepting or not accepting program or project S&MS risk at KDPs.

4.2.2 Acquirers:

a. Explicitly establish the mission S&MS risk posture, consisting of acceptable levels of S&MS risk, stated as S&MS risk tolerances as well as the expectation that the mission is ASARP.

b. Levy on the Provider any S&MS-related technical and process requirements deemed necessary to ensure and/or assure adherence to the established S&MS risk posture.

c. Approve the Provider's initial planning for adhering to the established S&MS risk posture throughout the program or project life cycle, including the S&MS success criteria for each LCR, informed by the Provider's argument for the validity of their planning.

d. Define, in negotiation with the Provider, S&MS-related audit and S&MS-related reporting requirements for each life-cycle phase.

e. Approve, at the outset of each life-cycle phase, the Provider's planning for adhering to the S&MS risk posture during the phase, informed by the Provider's argument for the validity of their planning for the phase.

f. Evaluate, at each LCR, the Provider's S&MS assurance case and determine if it provides sufficient assurance to the Acquirer that the Provider has met the S&MS success criteria of the LCR and in consequence is adhering to the established S&MS risk posture.

g. Formally accept the S&MS risk associated with decisions to proceed through the life cycle.

h. Conduct S&MS audits, inspections, etc., of the Provider, and evaluate Provider reports, as needed to maintain adequate ongoing insight into Provider performance.

i. Provide oversight in the form of corrective actions, recommendations, etc., based on insights gained via LCRs, audits, reports, etc.

4.3 Provider (NASA or non-NASA entity)

4.3.1 A Provider is a NASA or contractor organization that is tasked by an accountable organization (i.e., the Acquirer) to produce a product or service. Providers are responsible for translating Acquirer objectives into engineered solutions, in the form of systems, services, or other means of Acquirer satisfaction.

4.3.2 Providers:

a. Conduct initial planning for adhering to the established S&MS risk posture throughout the program or project life cycle, including the development of S&MS success criteria for each LCR and compliance with any externally mandated and/or Acquirer-levied S&MS-related technical and process requirements.

b. Develop an argument for the validity of the initial S&MS-related planning with respect to the established S&MS risk posture. [15]

c. Negotiate, with the Acquirer, S&MS-related audit and S&MS-related reporting requirements for each life-cycle phase.

d. Refine, as necessary, at the outset of each life-cycle phase, the initial S&MS-related planning as it pertains to the upcoming phase. The refined planning for the phase includes the specification of the *S&MS evidence*[16] that will be produced to substantiate that the S&MS success criteria of the phase have been met.

e. Develop, at the outset of each life-cycle phase, an argument for the validity of the refined planning for the phase with respect to the S&MS success criteria of the corresponding LCR.

f. Execute the program or project in accordance with the approved S&MS-related planning.

[15] The argument for the validity of the S&MS-related planning may treat externally mandated and/or Acquirer-levied technical and process requirements as constraints. The onus is not on the Provider to argue their validity.

[16] *S&MS evidence* is a central component of the S&MS assurance framework. It is discussed in Section 9.3.3.

g. At each LCR, submit to the Acquirer an S&MS assurance case that argues, supported by the S&MS evidence, that the S&MS success criteria have been met and that the Provider is adhering to the S&MS risk posture.

h. Support Acquirer S&MS audits, inspections, etc., and deliver agreed-upon reports.

4.4 Independent Technical Review Entities (NASA entities)

4.4.1 Independent technical review entities consist of the Technical Authorities (TAs) and Standing Review Boards (SRBs) that are a part of NASA's system of independent checks and balances. They marshal the subject matter expertise required for authoritatively evaluating the technical adequacy of S&MS-related Acquirer and Provider material for which their concurrence decisions are required.

4.4.2 Independent technical review entities:

a. Act as independent, critical, and skeptical elements of NASA's system of checks and balances.

b. Concur or non-concur with the completeness and achievability of the S&MS risk posture. (TAs)

c. Concur or non-concur with the validity of the Provider's initial S&MS-related planning, including the validity of the S&MS success criteria. (TAs)

d. For each life-cycle phase, concur or non-concur with the validity of the Provider's S&MS-related planning for the phase. (TAs)

e. For each life-cycle phase, concur or non-concur with the technical adequacy of the S&MS assurance case prior to submittal to the Acquirer at the corresponding LCR. (TAs)

f. Evaluate the S&MS assurance case at each LCR and present findings and recommendations to the Acquirer. (SRB)

5. DEFINING IMPLEMENTING REQUIREMENTS

5.1 Purpose

5.1.1 Implementation of the S&MS assurance framework defined in this guidance document entails the definition of requirements that are levied on or adopted by both Acquirer and Provider. This section provides illustrative requirements that can be used as a template for defining such organization-specific implementing requirements.

5.1.2 The illustrative requirements in this section are assumed to be defined within an effectively functioning space flight program and project management organizational hierarchy, system of independent checks and balances, phase-based program and project management framework, and Acquirer S&MS management system that includes closed-loop risk management and oversight of Provider activities.

5.1.3 The illustrative requirements in this section constitute an integrated set that establishes a coherent framework for S&MS assurance throughout the program or project life cycle. Care should be taken to ensure that implementation of the framework via organization-specific requirements preserves its coherence.

5.1.4 As discussed in Section 1.1, the life cycle and LCR structure presented in this guidance document is expected to be adapted to the specific life cycle, milestone review, and decision gate structures of the programs and projects to which it is applied.

5.1.5 The guidance provided in this document can be scoped to address all at-risk entities and mission technical objectives or it can be scoped to address a subset of the at-risk entities and mission technical objectives. In either case, the preservation of the Acquirer, Provider, and Independent Technical Review Entity roles and responsibilities is essential to the coherence of the framework.

Note: For example, a human space flight mission might limit application of this guidance document to crew safety and mission success, or a sample return mission might limit application of this guidance document to backward planetary protection. However, although such narrow applications of this guidance document might be appropriate for their specific circumstances, they do not represent a fully integrated approach to S&MS assurance.

5.2 Identifying Responsible Individuals

5.2.1 An organization that defines implementing requirements for the S&MS assurance framework needs to identify the specific individuals within that organization who will be responsible for compliance. Section 13 contains Requirements Compliance Matrices that can be adapted to identify the responsible individuals on a requirement-specific basis.

5.2.2 The Requirements Compliance Matrices in Section 13 accommodate the tailoring of implementing requirements. It is assumed that all tailoring implementing requirements are adjudicated by the levying or adopting organization according to its existing processes for requirements definition and management.

5.2.3 Each illustrative requirement is followed by an italicized *Verification* statement indicating, at a high level, the means by which compliance with the requirement is assumed to be verified. It is assumed that in practice, each defined requirement will be verified by the individual responsible for compliance with that requirement (e.g., as identified in the "Responsible Individual" columns of Table 6 through Table 9).

5.3 Illustrative Requirements for Establishing a Program or Project S&MS Risk Posture and Levying S&MS-related Technical and Process Requirements

5.3.1 The illustrative requirements of this section address the establishment, by the Acquirer, of an S&MS risk posture for a program or project. They also address the levying by the Acquirer of any specific S&MS-related technical and/or process requirements the Acquirer considers necessary for adhering to the S&MS risk posture or necessary for assuring the Acquirer that the S&MS risk posture is being adhered to. Guidance on the establishment of program and project S&MS risk postures is presented in Section 6.

Note: Adherence to the S&MS risk posture is the central focus of Providers' S&MS-related activities, and the claim that the S&MS risk posture is being adhered to is the central claim of the S&MS assurance case.

5.3.2 At program or project initiation, the Acquirer **shall** identify all at-risk entities and associated mission safety objectives.

Note: The set of mission safety objectives collectively define protection from harm caused by mission execution.

Verification: Inspection of configuration-controlled program or project documentation.

5.3.3 At program or project initiation, the Acquirer **shall** establish an S&MS risk posture that includes a set of risk tolerances which:

a. Align with the Agency's risk posture.

b. Address each mission safety objective.

c. Address each mission technical objective.

Note: Constraints on an acceptable S&MS risk posture may flow down to the Acquirer from the Agency level (e.g., for crew safety) or from sources external to NASA (e.g., for safety from orbital debris). An Acquirer-established S&MS risk posture is aligned with the Agency's risk posture if it is at least as constraining as the constraints that flow down to the Acquirer from higher levels of the NASA organizational hierarchy or from sources external to NASA.

Verification: Inspection of configuration-controlled program or project documentation.

5.3.4 The Acquirer **may** define the S&MS risk posture:

a. Quantitatively or qualitatively.

b. In absolute or relative terms.

Note: Defining an S&MS risk posture quantitatively (or even qualitatively) does not imply that analysis results such as those from a probabilistic risk assessment are sufficient on their own to substantiate a claim of adherence to it. Risk analyses are vulnerable to incompleteness and can underestimate S&MS risk, especially for systems in development. Moreover, the assumptions that support risk analyses can imply a host of management commitments. The validity of the assumptions depends on the effectiveness of their management. All such issues are relevant to a claim that the S&MS risk posture is being adhered to.

Verification: Inspection of configuration-controlled program or project documentation.

5.3.5 The Acquirer **shall** include in the S&MS risk posture the specification that the mission is ASARP.

Verification: Inspection of configuration-controlled program or project documentation.

5.3.6 Prior to Provider S&MS-related planning, the Acquirer **shall** obtain a TA concurrence decision, including documented rationale, regarding:

a. The alignment of the S&MS risk posture with the Agency's risk posture.

b. The completeness of the S&MS risk posture, in terms of:

(1) The completeness of the set of at-risk entities.

(2) The establishment of a mission safety objective for each at-risk entity.

(3) The establishment of a risk tolerance for each mission safety objective and each mission technical objective.

c. The feasibility of adhering to the safety-related elements of the mission S&MS risk posture.

Verification: Inspection of configuration-controlled program or project documentation.

5.3.7 Prior to Provider initial S&MS-related planning, the Acquirer **shall** levy any S&MS-related technical and process requirements it deems necessary to ensure and/or assure adherence to the established S&MS risk posture.

Note: This requirement refers only to those requirements imposed by the Acquirer on the Provider. It is expected that the Provider will propose additional, possibly numerous, requirements that derive from the S&MS risk posture and the Provider's particular solution. These Provider-proposed requirements can be technical and/or programmatic.

Verification: Inspection of configuration-controlled program or project documentation.

5.3.8 The Acquirer **should** keep the number of Acquirer-levied S&MS-related technical and process requirements to a minimum.

Note: The over-imposition of requirements by the Acquirer on the Provider runs counter to the intent of NPR 8700.1 to allow flexibility in the selection and acceptance of derived crew safety and mission success objectives, associated strategies, standards and requirements if the associated risks are understood, documented, and consistent with the established risk posture.

Verification: Inspection of configuration-controlled program or project documentation.

5.3.9 Prior to Provider initial S&MS-related planning, the Acquirer **should** obtain a TA concurrence decision, including documented rationale, regarding the necessity of the Acquirer-levied S&MS-related technical and process requirements for ensuring and/or assuring adherence to the S&MS risk posture.

Verification: Inspection of configuration-controlled program or project documentation.

5.3.10 TAs **should** consider treating TA non-concurrences generated by the requirements of this section as formal dissents.

Verification: Inspection of configuration-controlled program or project documentation.

5.4 Illustrative Requirements for Initial S&MS Assurance

5.4.1 The illustrative requirements of this section address the conduct, by the Provider, of initial S&MS-related planning. Initial S&MS-related planning reflects a whole-life-cycle perspective (e.g., addressing concept studies; concept and technology development; preliminary design and technology completion; final design and fabrication; system assembly, integration and test; launch and checkout; operations and sustainment; and closeout).

5.4.2 The Provider's initial S&MS-related planning identifies a baseline set of standards, requirements, and practices to which the Provider commits. This is in addition to any externally mandated and/or Acquirer-levied S&MS-related technical and/or process requirements.

Note: For NASA robotic projects, NPR 8705.4 [16] recommends the development of an Assurance Implementation Matrix (AIM) that documents the Provider's planned implementation consistent with that NPR's mission or instrument risk classification process and SMA objectives.

5.4.3 The scope of the Provider's initial S&MS-related planning goes beyond the technical approach to include programmatic issues such as staffing, resource loading, scheduling, the conduct of internal reviews and audits, issue identification and resolution processes, etc., all of which can affect Provider decision-making and, ultimately, S&MS risk. Guidance on deriving S&MS-related technical and process requirements is presented in Section 6.

5.4.4 The initial S&MS-related planning specifies the Provider's approach to ensuring that the mission is ASARP, addressing analysis of alternatives (AoAs), decision processes, application of accepted/best standards of practice, etc. Guidance on ensuring that a mission is ASARP is presented in Section 7.

5.4.5 The initial S&MS-related planning also specifies the S&MS success criteria to be used by the Acquirer to evaluate program or project status at LCRs. Guidance on the development of S&MS success criteria is presented in Section 8.

5.4.6 At program or project initiation, the Provider **shall** conduct initial S&MS-related planning that:

a. Describes, at a high level, how the Provider intends to adhere to the established S&MS risk posture.

   Note: It might be the case that the Provider considers the established S&MS risk posture to be infeasible or otherwise unable to be confidently adhered to. This is perhaps most probable when the S&MS risk posture is established prior to the selection of a Provider. In such a case, the requirements of Section 5.3 should be revisited, with Provider input, to establish an S&MS risk posture that all parties can agree to.

   Note: Providers that are Acquirers to lower-level Providers should describe how the activities of its lower-level Providers will be coordinated with those of the Provider to ensure adherence to the Provider's established S&MS risk posture, including the protocols for communication between the Provider and its lower-level Providers.

b. Defines the S&MS success criteria that need to be satisfactorily demonstrated at each LCR to show that the Provider is adhering to the established S&MS risk posture.

c. Specifies a baseline set of standards, requirements, and practices the Provider commits to in the service of ensuring and assuring adherence to the established program or project S&MS risk posture, including all externally mandated and/or Acquirer-levied S&MS-related technical and process requirements.

Verification: Inspection of configuration-controlled program or project documentation.

5.4.7 The Provider **should** consult with the Acquirer in the development of S&MS success criteria in order to understand Acquirer S&MS assurance needs and expectations at each LCR.

Verification: Inspection of configuration-controlled program or project documentation.

5.4.8 At program or project initiation, the Provider **shall** develop an argument that establishes the validity of the initial S&MS-related planning with respect to satisfaction of the defined S&MS success criteria, and the validity of the S&MS success criteria with respect to adherence to the established S&MS risk posture.

Note: The argument for the validity of the initial S&MS-related planning forms the basis for the top-level structure of the S&MS assurance case, as discussed in Section 11.

Verification: Analysis of the validation argument for logical coherence and comprehensibility.

5.4.9 At program or project initiation, the Acquirer **shall** obtain a TA concurrence decision, including documented rationale, regarding the validity of the initial S&MS-related planning, including the S&MS success criteria.

Verification: Inspection of configuration-controlled program or project documentation.

5.4.10 At program or project initiation, the Provider **shall** obtain Acquirer approval of the initial S&MS-related planning, including the S&MS success criteria, indicating that the Acquirer considers satisfaction of the defined S&MS success criteria to be adequate grounds for proceeding through the program or project life cycle insofar as S&MS is concerned.

Verification: Inspection of configuration-controlled program or project documentation.

5.4.11 TAs **should** consider treating TA non-concurrences generated by the requirements of this section as formal dissents.

Verification: Inspection of configuration-controlled program or project documentation.

5.5 Illustrative Requirements for S&MS Assurance Within a Life-Cycle Phase

5.5.1 The illustrative requirements of this section address S&MS assurance within each phase of the program or project life cycle. The three primary activities are phase-specific S&MS-related planning, execution of the phase, and evaluation of program or project status at the LCR at the end of the phase. Phase-specific S&MS related planning involves the refinement, as necessary, by the Provider, to an executable level of detail, those aspects of initial S&MS-related planning that pertain to the activities of the phase. Given approved, executable S&MS-related planning for the phase, the Provider conducts the specified activities in concert with other activities of the phase, modifying (and if necessary, rebaselining) the S&MS-related planning along the way as needed to respond to new information or circumstances that may arise, and producing the S&MS evidence that will be used to substantiate successful phase execution. At the end of the phase, the Provider develops an S&MS assurance case (or, equivalently, evolves the S&MS assurance case of the previous LCR) that nominally argues that the S&MS success criteria of the phase have been met, and that the program or project is therefore adhering to the established S&MS risk posture.

5.5.2 The requirements for S&MS assurance within a life-cycle phase are graphically illustrated in the "W-Engine" for S&MS Assurance presented in Section 9. Guidance on the specification of S&MS evidence is presented in Section 9.3.3. Guidance on the development of an S&MS assurance case is presented in Section 11.

5.5.3 Illustrative Requirements for Adjusting the S&MS Success Criteria of the Upcoming Life-Cycle Phase

5.5.3.1 Upon entering a new life-cycle phase, the Provider **may** adjust the S&MS success criteria of that phase as needed to reflect the current status of the program or project.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.3.2 Providers and Acquirers **shall** subject all adjustments made to the S&MS success criteria to the requirements of Section 5.4.

Verification: Per Section 5.4.

5.5.4 Illustrative Requirements for Phase-specific S&MS-Related Planning

5.5.4.1 Prior to life-cycle phase execution, the Provider **shall** conduct detailed S&MS-related planning for the life-cycle phase as needed to:

a. Specify, at an executable level, the S&MS-related activities that will be conducted during the phase.

b. Specify the S&MS evidence the Provider will produce to verify achievement of the S&MS success criteria of the phase.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.4.2 Prior to life-cycle phase execution, the Provider **shall** develop an argument that establishes the validity of the detailed S&MS-related planning for the life-cycle phase, i.e.:

a. That successful execution of the phase according to the S&MS-related planning will result in achieving the S&MS success criteria of the associated LCR.

b. That the S&MS evidence the Provider will produce meet the assurance needs of the Acquirer with respect to achieving the S&MS success criteria.

Verification: Analysis of the validation argument for logical coherence and comprehensibility.

5.5.4.3 Prior to life-cycle phase execution, the Acquirer, in negotiation with the Provider, **may** define S&MS audit and reporting requirements for the phase as needed to:

a. Monitor Provider progress relative to the S&MS-related planning for the phase (e.g., via the tracking and trending of S&MS-related technical metrics).

b. Assess the adequacy of implementation of the phase's S&MS-related process requirements.

c. Understand, analyze, or investigate unplanned events that occur during phase execution.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.4.4 Prior to life-cycle phase execution, the Acquirer **shall** obtain a TA concurrence decision, including documented rationale, regarding:

a. The validity of the detailed S&MS-related planning for the phase with respect to the S&MS success criteria of the associated LCR(s).

b. The validity of the S&MS evidence specifications as verifications that the associated S&MS success criteria have been met.

c. The adequacy of the S&MS audit and reporting requirements for the phase to provide the Acquirer with sufficient and timely insight into the Provider's execution of the phase.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.4.5 Prior to life-cycle phase execution, the Provider **shall** obtain Acquirer approval of its S&MS-related planning for the phase, including provisions for S&MS-related audit and reporting, indicating that the Acquirer:

a. Accepts that the S&MS-related planning is a valid means of achieving the S&MS success criteria.

b. Accepts that the specified S&MS evidence is sufficient to substantiate achievement of the associated S&MS success criteria.

c. Accepts that the S&MS audit and reporting requirements for the phase meet the Acquirer's insight needs.

d. Accepts that the Provider is ready to execute the S&MS-related planning.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.4.6 The Acquirer **shall** treat acceptance of the Provider's S&MS-related planning for the phase as an S&MS risk acceptance decision requiring single-signature risk acceptance.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.4.7 TAs **should** consider treating TA non-concurrences generated by the requirements of this section as formal dissents.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.5 Illustrative Requirements for Life-Cycle Phase Execution

5.5.5.1 The Provider **shall** execute the life cycle phase in accordance with the approved S&MS-related planning for the phase.

Verification: Analysis of program or project execution against the approved S&MS-related planning for the phase.

5.5.5.2 In the event that the Provider determines that a departure from the S&MS-related planning is warranted, the Provider **shall** first replan the S&MS-related activities of the phase to reflect the departure according to the requirements of Section 5.5.4.

Verification: Per Section 5.5.4.

5.5.5.3 The Acquirer and TA **should** review Provider reports and conduct audits of S&MS-related Provider processes as needed to assess the quality and effectiveness of their execution and develop an adequate understanding of any unplanned events.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.5.4 The Acquirer **may** process all Provider reports and Acquirer audits of S&MS-related Provider processes according to existing Acquirer issue management processes.

Verification: Per existing Acquirer issue management process requirements.

5.5.6 Illustrative Requirements for Life-Cycle Reviews

5.5.6.1 Prior to each LCR, the Provider **shall** produce an S&MS assurance case (which **may** be an updating of the S&MS assurance case of the previous LCR), addressing the status of the program or project:

a. With respect to the S&MS success criteria of the LCR.

b. With respect to the S&MS success criteria of previous LCRs.

c. With respect to the established S&MS risk posture.

Note: The status of the program or project with respect to the S&MS success criteria of previous LCRs will have been addressed by prior S&MS assurance case submittals. These submittals remain valid unless conditions have arisen since their submission that invalidate some portion of one or more of them.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.6.2 Prior to each LCR, the Acquirer **shall** obtain a TA concurrence decision, including documented rationale, regarding:

a. The validity of the argument of the S&MS assurance case that S&MS success criteria up to and including those of the pending LCR have been met.

b. The conformance of the S&MS evidence to the S&MS evidence specifications committed to by the Provider in the S&MS-related planning for the phase.

c. The validity of the substantiation of the claims of the S&MS assurance case by the S&MS evidence.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.6.3 In reviewing the Provider's S&MS assurance case prior to each LCR, the TA **should** document as actionable findings, and make available to both the Acquirer and Provider, any instances where:

a. The S&MS assurance case does not provide sufficient assurance that the S&MS success criteria have been met.

b. The S&MS assurance case indicates that the S&MS success criteria have not been met or are no longer met.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.6.4 The Provider **may** address all TA S&MS assurance case review findings according to existing Provider issue management processes.

Verification: Per existing Acquirer issue management process requirements.

5.5.6.5 The Provider **shall** submit the S&MS assurance case to the Acquirer at each LCR.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.6.6 The Provider **may** submit the S&MS assurance case in the form of a summary document, with references to supporting material that is available for Acquirer review.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.6.7 The Acquirer **shall** evaluate the S&MS assurance case submitted by the Provider at each LCR.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.6.8 In reviewing the Provider's S&MS assurance case at each LCR, the Acquirer, possibly supported by an SRB, **shall** document as findings any instances where:

a. The S&MS assurance case does not provide sufficient assurance that an S&MS success criterion has been met.

b. The S&MS assurance case indicates that an S&MS success criterion has not been met or that a previously met S&MS success criterion is no longer met.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.6.9 The Acquirer **shall** render a documented judgement, with supporting rationale, regarding whether or not the Acquirer is adequately assured that the Provider is adhering to the S&MS risk posture and has complied with all applicable externally mandated and/or Acquirer-levied S&MS-related technical or process requirements.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.6.10 The Acquirer's rendered judgement in 5.5.6.9 above **may** be conditional on the satisfactory completion of corrective actions levied by the Acquirer on the Provider.

5.5.6.11 The Acquirer **shall** treat granting the Provider the authority to proceed through the life cycle as an S&MS risk acceptance decision requiring single-signature risk acceptance.

Verification: Inspection of configuration-controlled program or project documentation.

5.5.6.12 TAs **should** consider treating TA non-concurrences generated by the requirements of this section as formal dissents.

Verification: Inspection of configuration-controlled program or project documentation.

6. ESTABLISHING AND USING THE MISSION S&MS RISK POSTURE

6.1 Introduction

6.1.1 The mission S&MS risk posture is that part of the overall program or project risk posture that addresses the willingness of the Acquirer to accept risks to safety and mission success during mission execution.[17] The mission S&MS risk posture recognizes the fact that space flight is inherently risky, and it is impossible to ensure with absolute certainty that a given mission will succeed in meeting its technical objectives without any harm to people, the environment (including orbital and planetary environments), or assets. Consequently, the pursuit of mission technical objectives necessarily entails risks to safety and mission success that must be both acceptable and accepted.

6.1.2 Figure 1 illustrates the relationship between the program or project objectives and the program or project risk posture, including the relationship between the mission safety objectives, the mission technical objectives, and the S&MS risk posture. Every program or project is conducted for the purpose of achieving some set of mission technical objectives, such as to collect certain types of information, retrieve certain materials, or demonstrate some new technology. Additionally, every program or project has an obligation to do so within programmatic constraints that can be expressed in terms of cost objectives, schedule objectives, etc. Every program or project objective carries some risk of shortfall, and the limits of acceptable risk to the objectives collectively constitute the program or project risk posture. The mission S&MS risk posture is the subset of the overall program or project risk posture that addresses the limits of acceptable risk to the mission safety objectives and to the mission technical objectives.

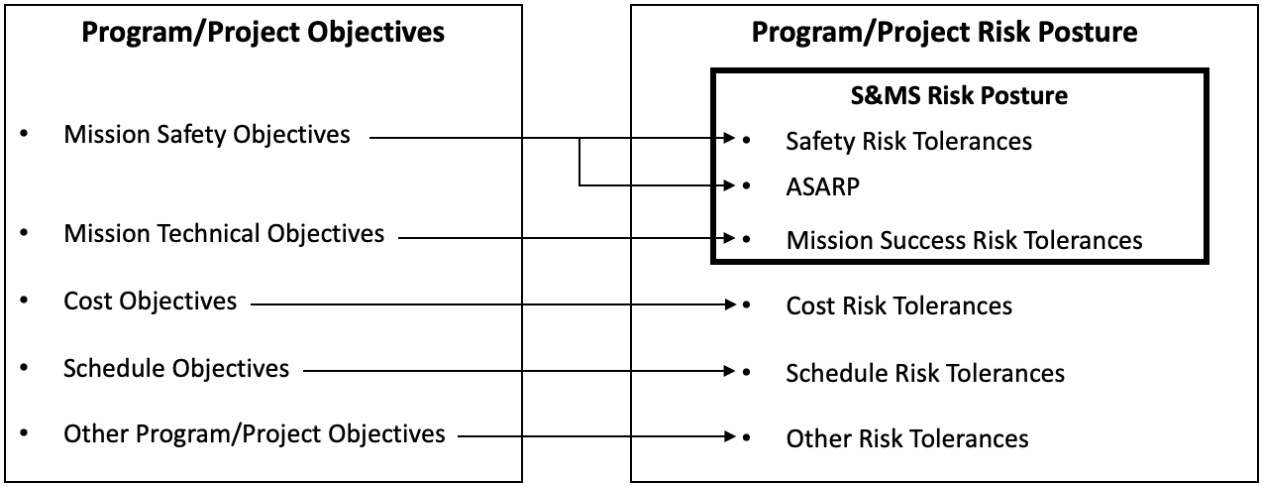

Figure 1. S&MS risk posture in the context of program/project objectives

[17] The establishment of an overall program or project risk posture addressing cost, schedule, and other program/project objectives is beyond the scope of this guidance document. The establishment of a risk posture generally (inclusive of strategic, programmatic, and institutional risks) is addressed briefly in Appendix A.

6.2 The Scope of the S&MS Risk Posture

6.2.1 Figure 2 notionally illustrates the general scope of the S&MS risk posture. It is expressed as an ensemble of individual risk tolerances across the full scope of mission technical objectives and at-risk entities, along with the expectation that the mission will be ASARP.[18]

6.3 Specifying the Character of the S&MS Risk Posture

6.3.1 In this guidance document, adherence to the S&MS risk posture and compliance with any externally mandated and/or Acquirer-levied S&MS-related technical or process requirements drive all Provider SMA activity. The character of the S&MS risk posture therefore largely determines the character of these activities. Adherence to a quantitative, stringent risk posture will, in general, require the application of correspondingly rigorous processes and standards for risk management, safety analysis, quality engineering, software assurance, failure tolerance, accident precursor analysis, human-system integration, etc. Conversely, adherence to a qualitative and more lenient risk posture might be achievable with fewer and/or less rigorous processes and standards.

6.3.2 For crewed missions, NPR 8705.2 [17] requires the specification of Administrator-approved safety goals and safety thresholds that define long-term targeted and maximum tolerable levels of risk to the crew as guidance to developers in evaluating "how safe is safe enough" for a given type of mission. These goals and thresholds are specified at the system-level and are expressed in terms of a quantitative aggregate measure of risk such as P(LOC). This is an example of a quantitative (and presumably stringent) risk posture, and the level of effort dedicated to ensuring and assuring that they are met is correspondingly high.[19,20]

6.3.3 For robotic missions, which can vary widely in their costs and technical objectives, NPR 8705.4 [16] requires the designation of risk tolerance classes for missions and instruments based on factors such as priority, primary mission lifetime, complexity and challenges, and life-cycle cost, which are used to grade the overall SMA effort as captured in an Assurance Implementation Matrix (AIM). Some of these same factors (particularly priority, consisting of relevance to the Agency strategic plan, national significance, and significance to the Agency and its strategic partners) can provide a basis for grading the stringency and specificity of the S&MS risk posture,

[18] See Section 7 for a discussion of ASARP.

[19] Even quantitative and stringent risk tolerances such as those for crew safety can originate from qualitative and relative stakeholder expectations. For example, the Agency's safety threshold for crew transportation to the International Space Station (ISS) began as, "At a minimum, the spaceflight system designed for transport of the crew to the ISS shall be at least as safe for the combined ascent and entry phases as the Space Shuttle was at the end of its operational life." This qualitative, relative expression of risk tolerance was then combined with the results of the existing Space Shuttle probabilistic risk assessment and quantified as, "No worse than 1 in 300 missions" [18].

[20] Defining an S&MS risk posture quantitatively does not imply that analysis results such as those from a probabilistic risk assessment are sufficient on their own to substantiate a claim of adherence to it. Risk analyses are vulnerable to incompleteness and can underestimate S&MS risk, especially for systems in development. Moreover, the assumptions that support risk analyses can imply a host of commitments that should be translated into verifiable technical and process requirements.

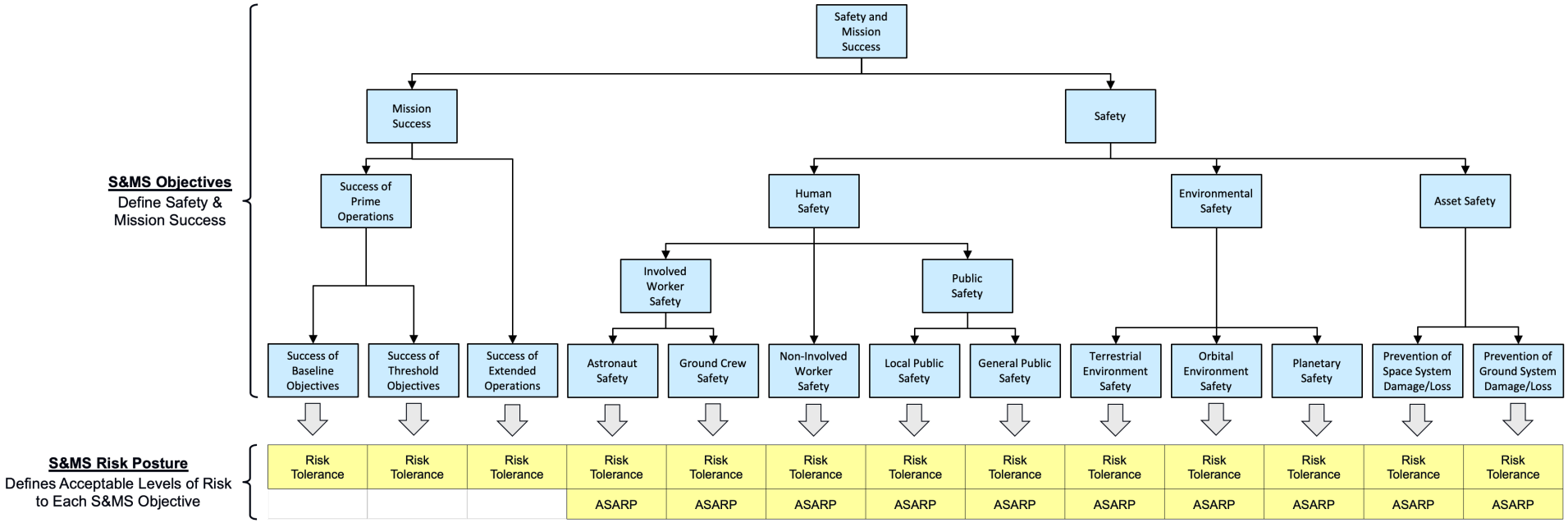

Figure 2. Scope of the S&MS risk posture (notional)

as shown in Table 1, from low-tolerance, quantitatively defined S&MS risk postures for high-priority S&MS objectives, to high(er)-tolerance, qualitatively defined S&MS risk postures for medium-priority S&MS objectives, to ASARP only for low priority or aspirational S&MS objectives.[21]

Table 1. Graded approach to establishing an S&MS risk posture

Priority of S&MS Objective	Recommended Character of the S&MS Risk Posture
High	• Stringent, quantitative S&MS risk posture (e.g., very low mission success risk tolerance: "P(LOM) ≤ 1 in X") • ASARP
Medium	• Less stringent, qualitative S&MS risk posture (e.g., "P(LOM) at least as low as mission M," "P(LOM) consistent with mission type N") • ASARP
Low	• ASARP

6.3.4 The character of the individual risk tolerances can vary within a given S&MS risk posture. For example, for a given mission, the risk tolerance for a threshold objective might be defined quantitatively, whereas the risk tolerance for a baseline objective might be defined qualitatively, and for extended operations not at all.

6.4 Necessary Properties of the S&MS Risk Posture

6.4.1 A valid S&MS risk posture has the following properties:

a. *The S&MS risk posture must reflect stakeholder risk tolerances* – The fundamental purpose of the S&MS risk posture is to ensure that mission S&MS risk is within tolerable limits given the value of the technical objectives being pursued. Therefore, the S&MS risk tolerances within the S&MS risk posture should establish levels of risk above which the Acquirer considers the risk unacceptable.

b. *The S&MS risk posture must be consistent with external and Agency-mandated risk criteria*[22] – NASA space flight programs and projects are required to comply with defined risk criteria in areas such as range safety, orbital debris, nuclear safety, and planetary protection. For example, NPR 8715.5, Range Flight Safety Program [19], and NASA-STD-8719.25, Range Flight Safety Requirements [20], require compliance with range safety risk criteria defined for individual risk, collective risk, and property. Such mandated risk criteria should be

[21] As illustrated in Figure 2, the S&MS risk posture is associated with the mission safety objectives and mission technical objectives, rather than with the mission and instruments.

[22] External and Agency-mandated S&MS-related risk criteria can be thought of as imposed and/or institutionalized stakeholder risk tolerances.

incorporated into the S&MS risk posture, either directly and explicitly or in a manner that bounds and contains them.

c. *The S&MS risk posture must be feasible* – An Acquirer that establishes unachievable S&MS risk tolerances is setting up the program or project for failure. Therefore, it is incumbent on the Acquirer to have confidence that the S&MS risk posture is feasible. For missions that are grounded in heritage there might be a sound actuarial basis for establishing a feasible S&MS risk posture. However, for new systems performing novel missions in novel environments it is incumbent on the Acquirer to conduct risk analyses, tests, etc., as needed to determine levels of S&MS risk that are achievable.

d. *Adherence to the S&MS risk posture must be arguable to relevant oversight entities and decision makers* – In order for the S&MS risk posture to function as the basis for risk acceptance decision-making, it must be possible to make the case that the program/project is adhering to it. Because risk is inherently probabilistic and future-oriented, adherence to an S&MS risk posture cannot be "proven" in the conventional sense, but instead must be convincingly argued using potentially diverse lines of reasoning and pieces of evidence.

e. *The S&MS risk posture must specify that the mission is ASARP* – Being ASARP reflects NASA's ethical obligation to maximize safety insofar as is practicable in the execution of its space flight missions.

f. *The safety risk tolerances of the S&MS risk posture should be as stringent as practicable* – In keeping with the expectation that the mission is ASARP, Acquirers should set the safety risk tolerances of the S&MS risk posture as low as reasonably achievable. This is what would be expected from the prioritization of safety as it applies to S&MS risk posture decision-making. The implication of ASARP with respect to the establishment of an S&MS risk posture is that the Acquirer should conduct a high-level AoA (e.g., at the mission concept/architecture level) in order to understand what constitutes achievable safety risk. This is consistent with the risk-informed decision-making (RIDM) process of NPR 8000.4 [3], which stresses AoA in decision-making, particularly as it applies to the formulation of achievable objectives.

6.5 A Process for Establishing a Mission S&MS Risk Posture

6.5.1 Figure 3 illustrates a process for establishing a mission S&MS risk posture that ensures that the resulting S&MS risk posture has the necessary properties of consistency with stakeholder risk tolerances, consistency with external and Agency safety mandates, feasibility, arguability, and being ASARP. At the core of the process is the conduct of a high-level, risk-informed AoA to develop a set of contending alternatives whose risks with respect to mission objectives across all domains (e.g., safety, technical, cost, schedule) has been analyzed. From this set of alternatives, the one with the lowest safety risk is the ASARP alternative, as long as the risks to the remaining objectives (including programmatic constraints) are tolerable. If not, then the alternative is discarded and the next-safest alternative is considered. If no alternatives have risks that are tolerable across all objectives, then the trade space is expanded and/or the objectives are relaxed, and a new set of alternatives is developed.

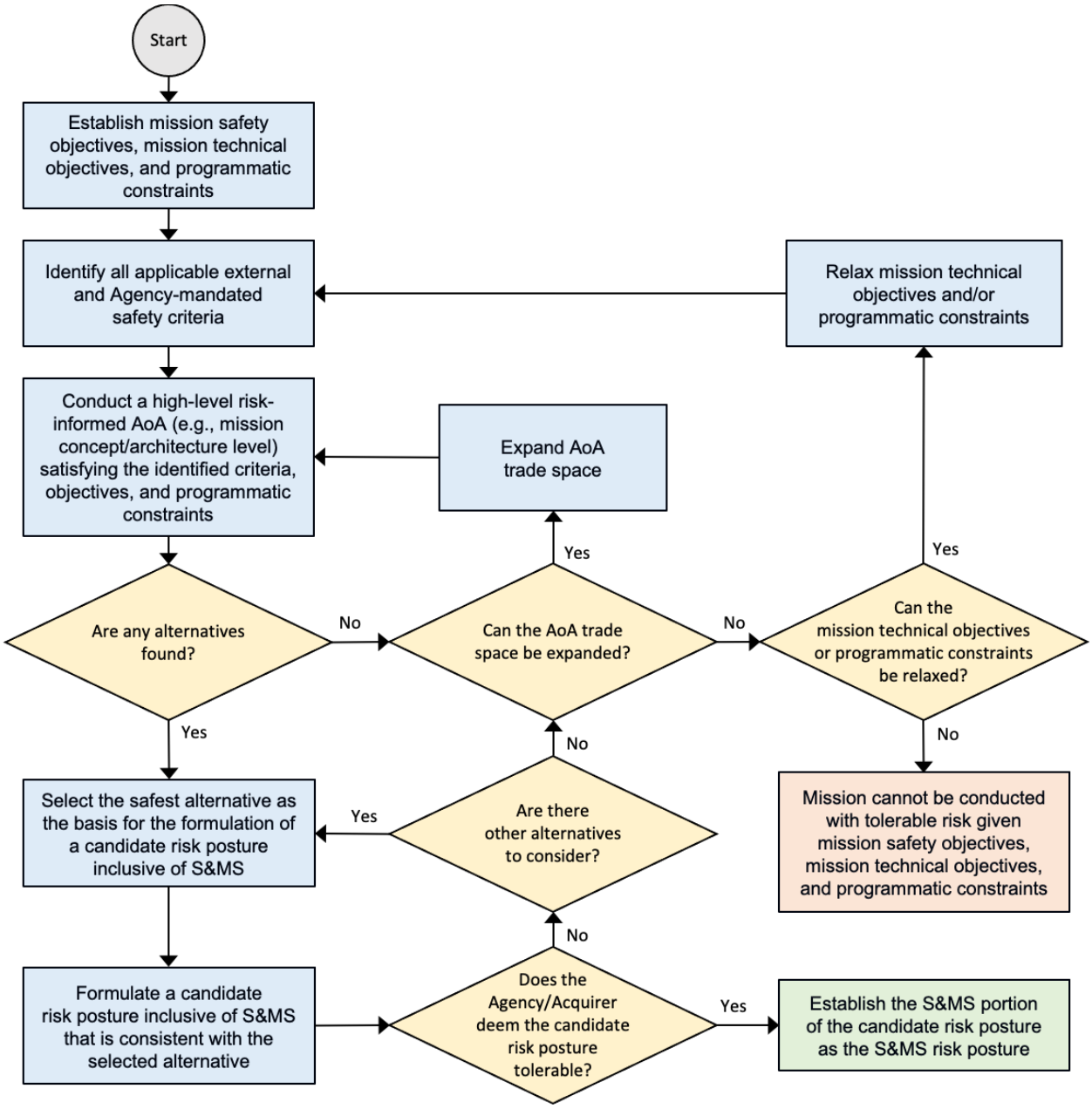

Figure 3. A process for establishing a mission S&MS risk posture

6.5.2 Because the S&MS risk posture has a technical basis in the risk-informed AoA, it can be said to be feasible. For the same reason, it can be said to be arguable, provided that the validity and sustainability of the underlying analysis assumptions can be argued in the context of the actual program or project. Also, by considering alternatives in decreasing order of safety until one with a tolerable risk posture is found, the safety risk tolerances of the S&MS are guaranteed to be as stringent as practicable.

6.5.3 Importantly, Figure 3 shows that the S&MS risk posture is established as an integral part of establishing the overall risk posture over all program or project objectives (see the block at the bottom-left of the figure). The S&MS risk posture must reflect the striking of a balance between

minimizing risks to safety and mission success and keeping programmatic risks within tolerable levels. In other words, all the elements listed in Figure 1 should be baselined together and in consideration of one another.

6.5.4 Figure 3 does not illustrate every dynamic that might go into the establishment of an S&MS risk posture. In particular, it does not explicitly diagram the case where the Agency or Acquirer decides to accept more risk than it initially was willing to accept in light of a realization that its initial risk tolerances were incompatible with what is feasible.

6.6 Determining Feasible S&MS Risk

6.6.1 An integral aspect of the process of Figure 3 is the ability to analyze the S&MS risks associated with each contender in the AoA trade space (e.g., the S&MS risk associated with a conceptual architecture and corresponding design reference mission (DRM) (or missions)). Figure 4 notionally illustrates such an analysis, in which the mission S&MS risk is built up from lower-level analyses of risk and reliability for which there is some basis in heritage. The resulting mission S&MS risks can reasonably be considered feasible given this basis, and if these S&MS risks are ASARP (i.e., if they are lower than that of the other alternatives in the AoA), then they can be used as the basis for establishing the S&MS risk posture. An analysis of this type was conducted as a prelude to NASA's Constellation program [21].

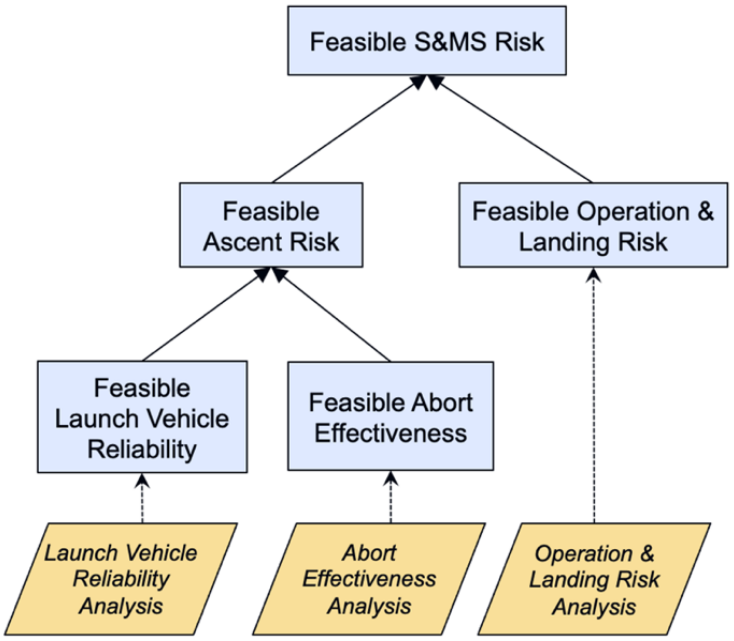

Figure 4. High-level analysis of S&MS risk for one alternative in the mission concept trade space (notional)

6.6.2 In this example, the fact that the established S&MS risk posture has its origins in a particular engineering solution does not mandate that the Provider adopt the solution for the program or project. Providers might be able to achieve even lower S&MS risks, e.g., by using innovations not considered in the trade space used to establish the S&MS risk posture.

6.7 Deriving S&MS-Related Technical and Process Requirements that Reflect Adherence to the S&MS Risk Posture

6.7.1 The established S&MS risk posture provides a stable, consistent basis for allocating S&MS risk into the mission elements to inform systems engineering decision-making and the development of verifiable low-level technical and process requirements, specifications, and standards that reflect adherence to it. In this way, compliance with these low-level constraints can be said to make adherence to the S&MS risk posture "come true."

6.7.2 Figure 5 notionally illustrates the derivation of verifiable S&MS-related technical and process requirements in the context of a launch vehicle and its concept of operations. It shows the S&MS risk posture allocated, in a risk-informed manner, into separate risk tolerances for each flight phase, and from there into subsystem reliabilities within each flight phase. Eventually, at a low enough level of system/mission decomposition, these derived performance requirements, which are inherently probabilistic by virtue of being derived from risk tolerances, are translated into verifiable, deterministic technical and process requirements whose satisfaction arguably produces the required probabilistic performance. In this way, the S&MS risk analysis used for allocation is tightly integrated into the systems engineering decision-making of the program or project, and is not merely used for confirmatory analysis.

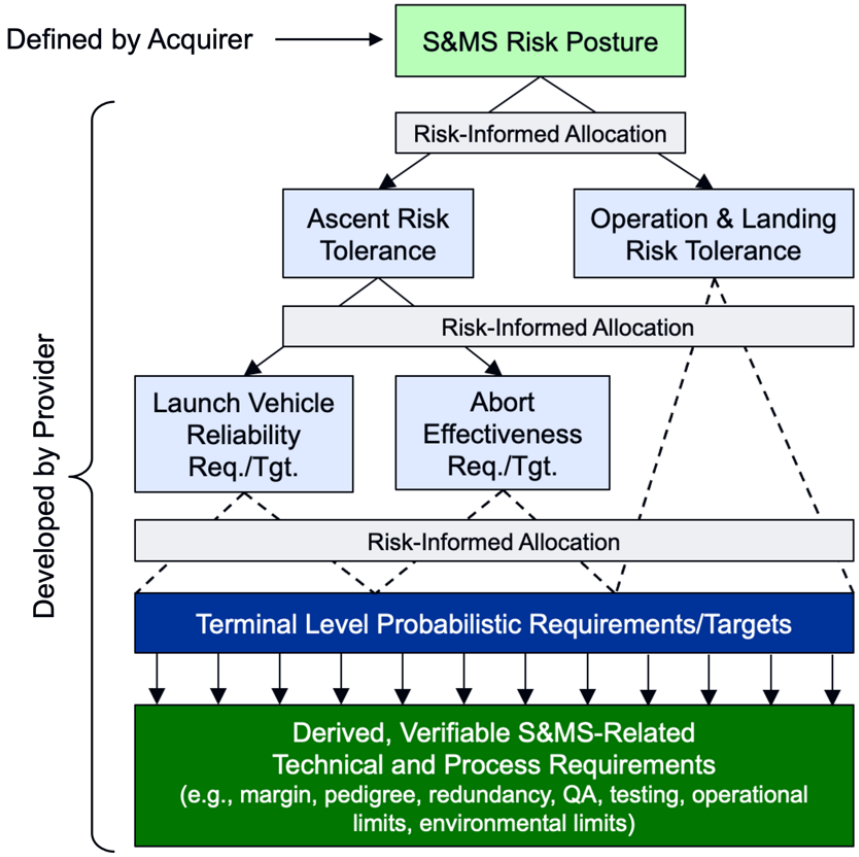

Figure 5. Derivation of verifiable S&MS-related requirements (notional)

7. ENSURING THE MISSION IS ASARP

7.1 Discussion

7.1.1 ASARP is generally applicable element of the S&MS risk posture that reflects NASA's ethical obligation to maximize safety insofar as is practicable in the execution of its space flight missions. A mission is ASARP if it is the safest means of achieving the mission technical objectives within programmatic constraints (e.g., on cost and schedule). ASARP encompasses the NASA policy, "Opportunities to improve crew safety are taken when practicable within programmatic constraints" [2]. In practice, this entails prioritizing safety in decision-making throughout the program or project life cycle insofar as is practical.

7.1.2 ASARP is separate and independent from any safety risk tolerances that may be levied on the mission to define thresholds of acceptable safety risk. Indeed, ASARP does not refer to any specific values or thresholds of safety risk. Rather, it refers to the safety of the given mission solution in the context of other mission solutions that could have been realized instead.

7.1.3 A claim that a mission is ASARP may be supported by an argument that a reasonable, sustained, and proactive search for the safest practical solution has been maintained throughout the entirety of the program or project life cycle (e.g., from Pre-Phase A: Concept Studies, through Phase F: Closeout). This implies that decisions and actions affecting safety have considered sufficiently broad sets of reasonable alternatives; that the safety risk of each alternative has been assessed as rigorously as practicable; and that safety has been consistently prioritized in the selection of the implemented alternative. The scope of decision-making relevant to ASARP includes management and operational decisions as well as system design decisions.

7.1.4 ASARP applies not only to the control or elimination of explicitly identified and analyzed sources of safety risk, but also to the robustness of the solution with respect to potentially unidentified and/or underappreciated (UU) sources (through conservative application of margin, redundancy, quality, etc.).

7.1.5 A minimum condition for ASARP is the consideration of applicable established good system safety and safety management practices in decision-making, such as the use of the best available technology (BAT). Established practice is typically captured in consensus technical and process standards and can be focused on very specific details of design, manufacture, analysis, management, operation, etc. Additionally, ASARP implies that reasonable consideration has been given to the use of novel practices and/or the development of new technologies that might reduce safety risk below that which would result from rote application of established practice.

7.1.6 The programmatic constraints within which an ASARP solution is pursued are not necessarily absolute. A solution might exist outside these constraints having a safety risk that is low enough to warrant relaxation of one or more constraints (e.g., by increasing the budget). Thus,

the pursuit of an ASARP solution can extend beyond the programmatic constraints, potentially involving rebaselining of those constraints in the interest of safety.[23]

7.1.7 Engineering judgement factors into the pursuit of an ASARP solution. Resources available for risk assessment might be limited, schedules might be tight, phenomena might be poorly understood, and decision-making might have to be made under conditions of significant uncertainty. Correspondingly, a determination that a solution is ASARP does not require absolute proof that a global safety risk minimum has been found and implemented, but instead rests on a foundation of competent, good-faith effort, sound judgement, and risk-informed decision-making RIDM.

7.1.8 In this guidance document, safety applies to all at-risk entities. This guidance document does not take a position concerning relative valuations among at-risk entities for the purpose of ASARP determination.

[23] This is somewhat analogous to how, in NPR 8705.4 [16], Class A and B risk tolerances are "driven more by technical objectives," whereas Class C and D risk tolerances are "driven more by programmatic constraints," suggesting a willingness to relax programmatic constraints in the interest of low technical risk for Class A and B missions.

8. DEVELOPING S&MS SUCCESS CRITERIA

8.1 Discussion

8.1.1 S&MS success criteria are focused on demonstrating, to the Acquirer, adherence to the S&MS risk posture at each LCR. The S&MS success criteria must be defined by the Provider since they are associated with the Provider's specific implementation of a potentially novel solution, but must also be accepted by the Acquirer as valid in that for each LCR they collectively indicate, to the Acquirer's satisfaction, adherence to the S&MS risk posture.

8.1.2 The S&MS success criteria must address the adequacy of all aspects of the Provider's effort upon which S&MS risk significantly depends. This includes not only technical attributes of the mission and its systems, but also Provider processes, capabilities, and organizational factors insofar as they affect S&MS. Table 2 presents an illustrative set of S&MS assurance elements that address a broad range of factors having the potential to affect S&MS risk, including so-called "soft" factors relating to Provider organization and management. These factors manifest differently in different life-cycle phases, but in general provide a foundation for defining valid sets of S&MS success criteria. The development of a table along the lines of Table 2, customized to the particulars of the program or project, is recommended as a means of ensuring that the resulting S&MS success criteria are adequately scoped, and as a means of effectively arguing their validity with respect to the S&MS risk posture.

8.1.3 Table 3 presents a set of illustrative, notional S&MS success criteria, defined at a relatively high-level. In general, the criteria in Table 3 address Acquirer expectations concerning Provider progress across the S&MS assurance elements of Table 2. The life-cycle phases in Table 3 do not include every phase defined in [7]. More importantly, it is reiterated here that this guidance document does not advocate for any specific life-cycle phases or LCRs. The life-cycle phases identified in Table 3 are illustrative only. An actual program or project using this guidance may define more, fewer, or altogether different life-cycle phases.

8.1.4 In general, S&MS success criteria should be defined at a high enough level that they can be specified as part of program or project initialization, recognizing that they may require refinement prior to phase execution based on program or project developments up to that point, but they should also be specific enough to address the full scope and depth of the Acquirer's assurance needs.

8.1.5 The S&MS success criteria in Table 3 are expressed as objectives[24] (rather than, e.g., as deliverables), is in keeping with the objectives-driven approach to S&MS assurance of this guidance document. Deliverables and other artifacts that substantiate the accomplishment of the S&MS success criteria count as S&MS evidence and are expected to be incorporated into the S&MS assurance case that is submitted to the corresponding LCR. Their production could, if desired, therefore count as LCR *entrance* criteria (along with the production of the S&MS assurance case itself).

[24] Specifically, the S&MS success criteria are *means objectives* by which the Provider achieves the *fundamental objective* of adhering to the established S&MS risk posture.

Table 2. S&MS Assurance Elements (Illustrative)

Illustrative Elements of S&MS Assurance	
S&MS Assurance Element	Comments
Mission S&MS risk is adequately understood	The mission is well defined (e.g., via the specification of a DRM), mission hazards are well understood, the response of the system to hazardous events/faults/failures is well characterized, individual risks are identified, and mishap consequences and likelihoods are adequately defined, at a level of detail commensurate with the current level of mission/system definition. Risk-significant uncertainties in any of the above are adequately identified and characterized, including the potential for unknown and/or underappreciated (UU) sources of S&MS risk, e.g., due to novelty, complexity, cost constraints, or schedule pressure.
he boundaries and assumptions within which S&MS risk is evaluated are understood	The boundaries and assumptions within which acceptable mission S&MS risk is to be achieved are defined, including the concept of operations, system definition, environmental stress limits, operational limits, system condition, extent of personnel training, etc. These collectively define a "normalcy map" within which S&MS risk is adequately understood and deemed acceptable.
Effective S&MS-related management processes and controls are in place	The Provider's S&MS-related management processes and controls (risk management, quality, software assurance, configuration management, etc.) are compliant with all levied and agreed-upon S&MS-related process standards; S&MS is managed proactively and holistically as an integrated part of a management system that includes other mission execution domains (e.g., cost, schedule); audits and reports indicate a robust safety culture; systems are in place to effectively monitor performance, including leading indicators, and identify and manage emerging risks (e.g., via precursor analysis); processes for post-flight data review and lessons learned are effective; risk acceptance procedures are adequately formalized and technically sound; etc. Effective S&MS-related management processes and controls maintain the system within its normalcy map throughout the program or project life cycle.
The S&MS risk posture is adhered to	Assessed S&MS risk provides adequate confidence that S&MS risk posture is being adhered to, considering the work to be done (e.g., S&MS-related technology maturation, hazard control development) and accounting for all hazards, including those not yet identified. System/mission definition decisions are risk-informed, involving adequate trade studies and the prioritization of safety in decision-making, with documented rationales.

Mission complies with all externally mandated and/or Acquirer-levied S&MS-related requirements	Per defined verification protocols.

8.1.6 For programs or projects where the Acquirer needs a very high level of assurance, the S&MS success criteria can become quite extensive, explicitly touching on accomplishments at a correspondingly high level of detail. For example, the NASA Human Systems Integration (HSI) Handbook [22] provides a representative table of HSI success criteria, reproduced in Table 4, whose number is on par with the higher-level S&MS success criteria of Table 3.[25] Defining S&MS success criteria at this level of detail across all SMA disciplines would result in a much larger set of S&MS success criteria than that that of Table 3, but for high priority programs and projects, or for programs and projects that put human lives at risk, such a set of S&MS success criteria might be necessary in order to address the full spectrum of S&MS-related issues about which the Acquirer needs to be assured.

8.1.7 Providers that are Acquirers to lower-level Providers will typically need to include S&MS success criteria relating to lower-level Provider activities upon which they depend, such as subsystem development, which in turn could relate to subsystem definition, manufacture, testing, analysis, or acceptance, depending on the LCR.

8.1.8 Neither Table 3 nor Table 4 are intended to be used as-is for any specific program or project. They are intended to be illustrative only, to communicate the underlying concept that the S&MS success criteria address all program or project activities upon which adherence to the S&MS risk posture significantly depends, across all SMA disciplines.

8.1.9 In any case, the Provider must work closely with the Acquirer to develop S&MS success criteria that both reflect the Provider's S&MS-related planning and provide indication, to the Acquirer's satisfaction, of whether or not the phase has been successfully executed according to the S&MS-related planning and therefore that the S&MS risk posture is adhered to.

[25] Not all success criteria in Table 4 are expressed as objectives. It is the strong recommendation of this guidance document that in general, S&MS success criteria be expressed as objectives where practicable to do so.

Table 3. Illustrative S&MS success criteria

Life-Cycle Phase	LCR	S&MS Success Criteria (notional)
Concept Development	Mission Concept Review (MCR)	• All at-risk entities (e.g., crew, public, environment, asset, mission objective) have been identified. • An S&MS risk posture has been established, covering all relevant at-risk entities. • Major sources of S&MS risk have been identified at a level consistent with the level of detail of the mission concept, and initial S&MS risk control strategies have been developed. • The selected concept(s) can feasibly adhere to the S&MS risk posture given the mission hazards and S&MS risk control strategies. • The selected concept(s) can feasibly adhere to the S&MS risk posture given the technological challenges. • All mandated S&MS-related requirements have been identified.
System Design	System Requirements Review (SRR)	• The S&MS risk posture has been baselined. • The process for allocating the S&MS risk posture into the product breakdown structure (PBS) is valid. • The process for adhering to the S&MS risk posture in design is adequate. • Mandated S&MS-related requirements are complied with.[26] • All prior corrective actions have been resolved.
	Preliminary Design Review (PDR)	• Identified S&MS risks have been eliminated, controlled, or accepted, and/or plans and resources are in place to eliminate, control, or accept them. • The baselined preliminary design and operational procedures are consistent with the S&MS risk posture. • The baselined preliminary design and operational procedures include sufficient monitoring, maintenance, and logistics to maintain adherence to the S&MS posture. • Mandated S&MS-related requirements are complied with. • All prior corrective actions have been resolved.

[26] S&MS-related requirements include any process requirements that may be levied on the conduct of any life-cycle phase.

	Critical Design Review (CDR)	• Identified S&MS risks have been eliminated, controlled, or accepted. • The baselined detailed design specifications and operational procedures are consistent with the S&MS risk posture.[27] • The baselined detailed design specifications and operational procedures include sufficient monitoring, maintenance, and logistics to maintain adherence to the S&MS posture. • Mandated S&MS-related requirements are complied with. • All prior corrective actions have been resolved.
System Realization	Production Readiness Review (PRR)	• Production process quality requirements are consistent with the baselined detailed design specifications. • Production processes are consistent with the production process quality requirements. • Production plans include all necessary spares, etc., required to maintain adherence to the S&MS risk posture during mission operations. • Quality assurance (QA) processes are consistent with the project's S&MS risk posture. • Mandated S&MS-related requirements are complied with. • All prior corrective actions have been resolved.
	System Acceptance Review (SAR)	• The system is compliant with the design specifications. • The system is consistent with the S&MS risk posture. • Mandated S&MS-related requirements are complied with. • All prior corrective actions have been resolved.
Mission Execution	Mission Readiness Review (MRR)	• The system is consistent with its as-accepted configuration and condition. • Provisions for maintaining the system consistent with the S&MS risk posture are in place (e.g., spares, maintenance, anomaly management). • System operators are trained on mission operations, including contingencies. • Mandated S&MS-related requirements are complied with. • All prior corrective actions have been resolved.

[27] Acceptance of a design that is inconsistent with the baseline S&MS risk posture should be predicated on a relaxation and rebaselining by the Acquirer of the S&MS risk posture, so that design is consistent with the rebaselined S&MS risk posture, keeping in mind that rebaselining of the S&MS risk posture can affect the Acquirer's adherence to the higher-level S&MS risk posture that may be levied on it.

Closeout	Disposal Readiness Review (DRR)	• The as-is system is consistent with the S&MS risk posture. • System operators are trained on disposal operations, including contingencies. • Mandated S&MS-related requirements are complied with. • All prior corrective actions have been resolved.

Table 4. HSI success criteria (reproduced from [22])

Review	HSI Success Criteria
Mission Concept Review (MCR)	• HSI Lead identified • Elicited stakeholder and user community goals • Supported function allocation • Developed HSI operational concepts for inclusion in ConOps • Documented design constraints • Produced high-level HSI requirements • Initiated HSI Planning • Drafted HSI Plan • Supported Feasibility Activities • Documented performance metrics and measures
System Requirements Review (SRR)	• Established HSI Team including Lead and domain SMEs • Baselined HSIP • Supported function allocation • Generated domain and interface requirements • Incorporated HSI inputs into ConOps
Mission Definition Review (MDR) /System Definition Review (SDR)	• Documented HSI products and resources in HSI Plan • Supported feasibility assessments and modeling including use of mockups, models, and simulations
Preliminary Design Review (PDR)	• Refined requirements: formed and validated derived HSI requirements • Updated HSI Plan and input into other technical plans, as appropriate • Completed technical trade studies • Refined interfaces and evaluated design compatibility

Critical Design Review (CDR)	• Baselined HSI requirements and verifications • Updated HSI Plan and input into other technical plans, as appropriate • Documented and incorporated trade study results • Incorporated model/prototype results into detailed design • Validated components and interfaces against operational concept
Production Readiness Review (PRR)	• Updated HSI Plan • HSI cost and schedule estimates are within program or project constraints • Approved model and prototype results
System Integration Review (SIR)	• Documented system integration test results
Test Readiness Review (TRR)	• Completed HSI input to system-level test objectives, requirements, plans and procedures
System Acceptance Review (SAR)	• Completed HSI requirement verification against end product system • Completed end product validation against users' needs • Accepted operations support products by end users
Operational Readiness Review (ORR) /Flight Readiness Review (FRR)	• Endorsed system certification for operations with humans • Endorsed user certification for operations with the system
Post-Launch Assessment Review (PLAR) /Critical Event Readiness Review (CERR) /Post-Flight Assessment Review (PFAR)	• Documented user/maintainer safety, health, and performance • Documented lessons learned demonstrating an operational return on HSI investment • Documented lessons learned showing implementation of necessary corrections and improvements
Decommissioning Review (DR)	• Captured HSI knowledge is placed into program or project documentation system

9. OVERVIEW OF THE "W-ENGINE" FOR S&MS ASSURANCE

9.1 Introduction

9.1.1 The activities associated with S&MS assurance during each life-cycle phase are codified in the "W-Engine" for S&MS assurance illustrated in Figure 6.

9.2 Initializing the "W-Engine"

9.2.1 The "W-Engine" for S&MS assurance is initialized at the beginning of the program or project. The main activities of "W-Engine" initialization are 1) establishing an S&MS risk posture and levying any additional S&MS-related technical and/or process requirements, which is the responsibility of the Acquirer, and 2) conducting initial, life-cycle scope S&MS-related planning, which is the responsibility of the Provider. Guidance on item 1 is provided in Sections 5.3 and 6. Guidance on item 2 is provided in Section 5.4. Of particular importance to S&MS-related planning is defining (and justifying the adequacy of) the S&MS success criteria to be used by the Acquirer to evaluate program or project status at LCRs. Valid sets of S&MS success criteria for each life-cycle phase enable the "W-Engine" to operate on each phase sequentially.

9.3 Executing the "W-Engine"

9.3.1 Within each life-cycle phase, the S&MS assurance framework is focused on meeting the S&MS success criteria defined for the associated LCR(s). The activities of the framework can be partitioned into planning, execution, and S&MS risk acceptance.

9.3.2 Each life-cycle phase has associated with it the set of S&MS success criteria developed for it during initial S&MS-related planning. However, because subsequent developments may affect the adequacy or appropriateness of the set, at the beginning of each phase the Provider and Acquirer recapitulate them, making any adjustments needed, including any revisions to the argument that they are valid. With the S&MS success criteria for the phase baselined, the Provider refines, as part of overall systems engineering planning for the phase, the initial S&MS-related planning, so that planning for the phase is at a detailed, executable level. Along with this detailed S&MS-related planning for the phase, the Provider also refines the argument for the validity of the S&MS-related planning with respect to the phase's S&MS success criteria. This includes specification of the S&MS evidence that will be produced to substantiate achievement of the S&MS success criteria. The Acquirer and Provider then negotiate audit, reporting, and/or other provisions relating to Acquirer insight and oversight needs. The Audits may focus on technical, process, and/or organizational aspects of the Provider's effort, depending on the Acquirer's assurance needs. This also includes allowances for *ad hoc* audits and inspections the Acquirer may wish to conduct in response to emerging information (e.g., from Provider reports, mishaps, etc.) in addition to any prescribed audits and inspections. The Technical Authorities (TAs) then evaluate the S&MS-related planning for the phase, supported by the associated argument for its validity and including the negotiated audit support and reporting agreements, and concur or non-concur on its validity. Given satisfaction with the S&MS-related planning for the phase, the associated insight and oversight provisions, and the readiness of the Provider, the Acquirer grants the Provider the authority to execute the SMA activities of the phase.

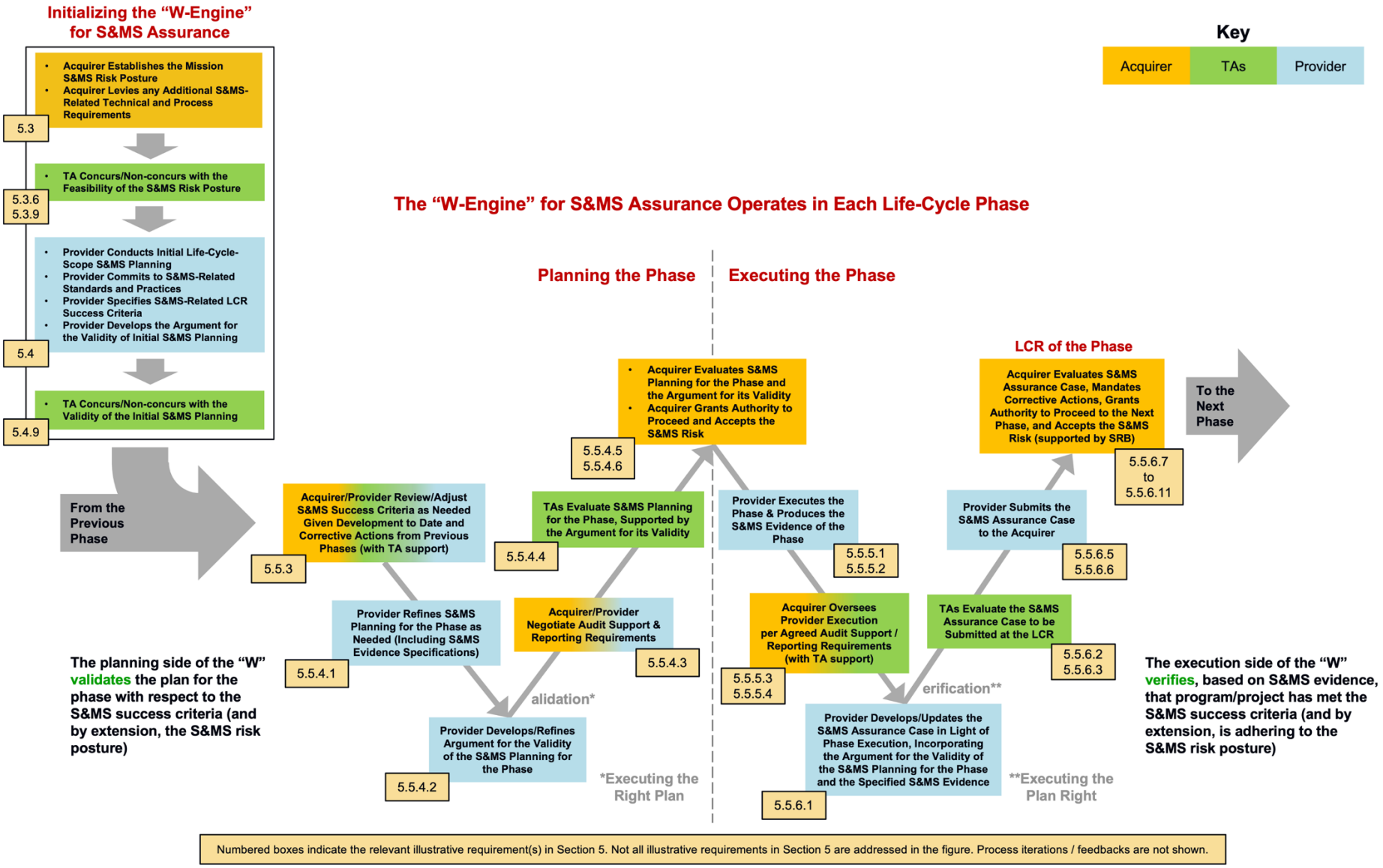

Figure 6. The "W-Engine" for S&MS assurance

9.3.3 The Provider executes the S&MS-related planning for the phase, producing the agreed-upon S&MS evidence needed to substantiate the claim that the S&MS success criteria for the phase have been met, overseen by the Acquirer and TAs as agreed. During execution, circumstances can arise that necessitate modifications to the S&MS-related planning for the phase, which need to go through the same process of evaluation and approval as the initial S&MS-related planning in order for the Acquirer to be assured that the planning for the phase remains valid. At the end of the phase, the Provider develops an S&MS assurance case (or updates the S&MS assurance case is from the previous LCR) to address the achievement of the S&MS success criteria of the current phase, using the argument that was developed during S&MS-related planning for the phase, substantiated by the specified S&MS evidence. If circumstances arise during the current phase that invalidate any portion of the S&MS assurance case developed in previous phases, those invalidated portions of the case must be revised such that the S&MS assurance case as a whole is sound.

9.3.4 The TAs evaluate the S&MS assurance case for technical soundness prior to the LCR, after which the Provider submits it to the LCR as the principal S&MS assurance product for the program or project. A nominal S&MS assurance case argues, with evidence, that the S&MS success criteria across all LCRs are valid and that the S&MS success criteria of all phases up to the current phase have been met. The Acquirer, possibly supported by an SRB, conducts a structured, critical, and skeptical evaluation of the submitted S&MS assurance case, identifying any deficits in the argument or the evidence that either prevent moving forward and/or warrant corrective action. Nominally, consistent with the principle of single-signature accountability for risk acceptance, the Acquirer treats granting the Provider the authority to proceed through the life cycle as an S&MS risk acceptance decision requiring single-signature risk acceptance. The phase ends with the Acquirer granting the Provider authority to proceed, potentially with mandated corrective actions coming out of the LCR.

10. SPECIFYING S&MS EVIDENCE

10.1 Discussion

10.1.1 A program's or project's S&MS evidence comprises the artifacts that are marshaled by the Provider to substantiate, to the satisfaction of the Acquirer, that the S&MS success criteria have been met and that the Provider is adhering to the S&MS risk posture. S&MS evidence provides the evidentiary basis for the claims of the S&MS assurance case, and as such is an integral part of the S&MS assurance case. The S&MS evidence to be produced in a given life-cycle phase is specified in the S&MS-related planning for the phase that is developed to an executable level of detail at the start of the phase.

10.1.2 Because the function of the S&MS evidence is to substantiate, to the Acquirer's satisfaction, the satisfaction of the claims of the S&MS assurance case to which they are attached, the Provider must work closely with the Acquirer to develop S&MS evidence specifications that meet the Acquirer's assurance needs. Thus, S&MS evidence specifications might include specifying the degree of certainty the Acquirer needs in order to accept a reliability claim (e.g., at least 95% probability of 99.9% reliability), the number of simulation hours needed in order to accept a training claim, or the use of a certain standard in order to accept a particular process claim. In general, S&MS evidence specifications function as verification protocols for the claims they substantiate and should be developed accordingly.

10.1.3 Providers that are Acquirers to lower-level Providers will typically need to specify S&MS evidence that relates to or originates with the lower-level Providers. Such evidence could take the form of subsystem requirements, test results, analyses, or actual hardware, or could take the form of a lower-level Provider's validated S&MS assurance case (along with the documented evaluation of that case) attesting to the satisfactory completion of lower-level Provider activities upon which the Provider depends.[28]

10.1.4 As mentioned in Section 8, the production of S&MS evidence in accordance with the agreed-upon S&MS evidence specifications could, if desired, count as LCR entrance criteria (as part of S&MS assurance case production itself). Table 5 notionally illustrates the kinds of S&MS evidence that might be produced, as a function of life-cycle phase.

[28] As used here, a lower-level Provider's S&MS assurance case is "validated" if it provides a sound basis for granting the lower-level Provider the authority to proceed through its life cycle, per the requirements of Section 5.5.6.

Table 5. Illustrative examples of S&MS evidence

Life-Cycle Phase	LCR	LCR-Specific S&MS Evidence
Concept Development	MCR	• List of all at-risk entities (e.g., crew, public, environment, assets) • The S&MS risk posture • Analyses of alternative mission concepts at the level of feasibility, including S&MS risk identification, S&MS risk control strategies, and technology gaps • Selected mission concept, defined at sufficient level of detail to be baselined (e.g., as a DRM) • Rationale for the selected mission concept (e.g., RISR per the NASA RIDM Handbook [23]) • Preliminary approach to V&V for the selected concept(s)
System Design	SRR	• Baselined S&MS risk posture • The process for allocating the S&MS risk posture into the PBS • The S&MS analysis plan
	PDR	• The baselined preliminary design and operational procedures • Rationales for S&MS-risk-significant system design decisions (e.g., RISR per the NASA RIDM Handbook) • Traceability matrices from the S&MS risk posture to the preliminary design requirements and operational procedures • S&MS analysis of the baselined DRM, including contingencies, addressing significant S&MS risks, risk controls, uncertainties associated with identified S&MS risks, and the potential for UU risks • Monitoring and instrumentation trade studies • Maintenance analyses • Logistics analyses
	CDR	• The baselined detailed design specifications and operational procedures • Rationales for S&MS-risk-significant system design decisions (e.g., RISR per the NASA RIDM Handbook) • Traceability matrices from the S&MS risk posture to the baselined design specifications and operational procedures • S&MS analysis of the baselined DRM, including contingencies, addressing significant S&MS risks, risk controls, uncertainties associated with identified S&MS risks, and the potential for UU risks • Monitoring and instrumentation trade studies • Maintenance analyses • Logistics analyses

System Realization	PRR	• Production process quality requirements • Production process descriptions • Rationales for S&MS-risk-significant production process decisions (e.g., RISR per the NASA RIDM Handbook) • Traceability matrices from baselined detailed design specifications to production process quality requirements, QA requirements, and software development and assurance processes
	SAR	• System verification matrices • List of non-conformances and their resolutions • S&MS analysis of the as-is system with respect to the S&MS risk posture
Mission Execution	MRR	• System status • Mission support status • Training records/certifications
Closeout	DRR	• System condition/status reports • S&MS analysis with respect to the disposal-related aspects of the S&MS risk posture. • Disposal-related training records/certifications

11. DEVELOPING AN S&MS ASSURANCE CASE

11.1 Discussion

11.1.1 An S&MS assurance case is a compelling, comprehensible, and valid argument, supported by evidence, that a Provider is adhering to the established S&MS risk posture. It is developed by the Provider and submitted to the Acquirer at LCRs as the primary S&MS-related input to the Acquirer's decision to grant the Provider the authority to proceed to the next life-cycle phase.

11.1.2 The elements of the S&MS assurance case are [24]:

a. An explicit set of claims, for example, that the probability of an accident or a group of accidents is low.

b. Evidence justifying the claims, for example, representative operating history, redundancy in design, or results of analysis.

c. Structured arguments that link the evidence to the claims using logically valid rules of inference.

11.1.3 The interaction of these elements is illustrated in Figure 7 for a claim supported by two independent arguments. Formalisms such as Goal Structuring Notation (GSN) [25] or Claims, Arguments, and Evidence (CAE) [26] may be used to impose rigor on the S&MS assurance case. Additional guidance can be found in [11, 12, 27].

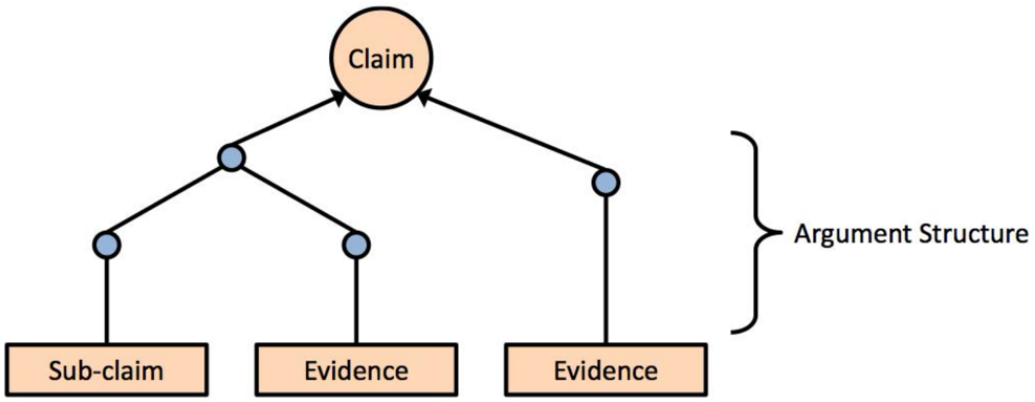

Figure 7. A claim supported by two independent arguments

11.1.4 The nominal S&MS assurance case structure specified in this guidance document is illustrated in Figure 8. The central claim of the S&MS assurance case in Figure 8 (i.e., the top

claim) is, "The program/project is adhering to the established S&MS risk posture."[29,30] This claim is supported by the claim that the S&MS success criteria up to and including the LCR in question have been met, along with the argument, made by the Provider during initial S&MS-related planning, that the S&MS success criteria are valid with respect to adherence to the S&MS risk posture. The claim that the S&MS success criteria of a given LCR have been met is supported by the argument, made by the Provider during the detailed S&MS-related planning for the phase, that successful execution of the S&MS-related activities of the phase are valid with respect to the S&MS success criteria. Finally, the claim that the S&MS-related activities of the phase have been successfully executed is supported by the S&MS evidence marshaled for that purpose.

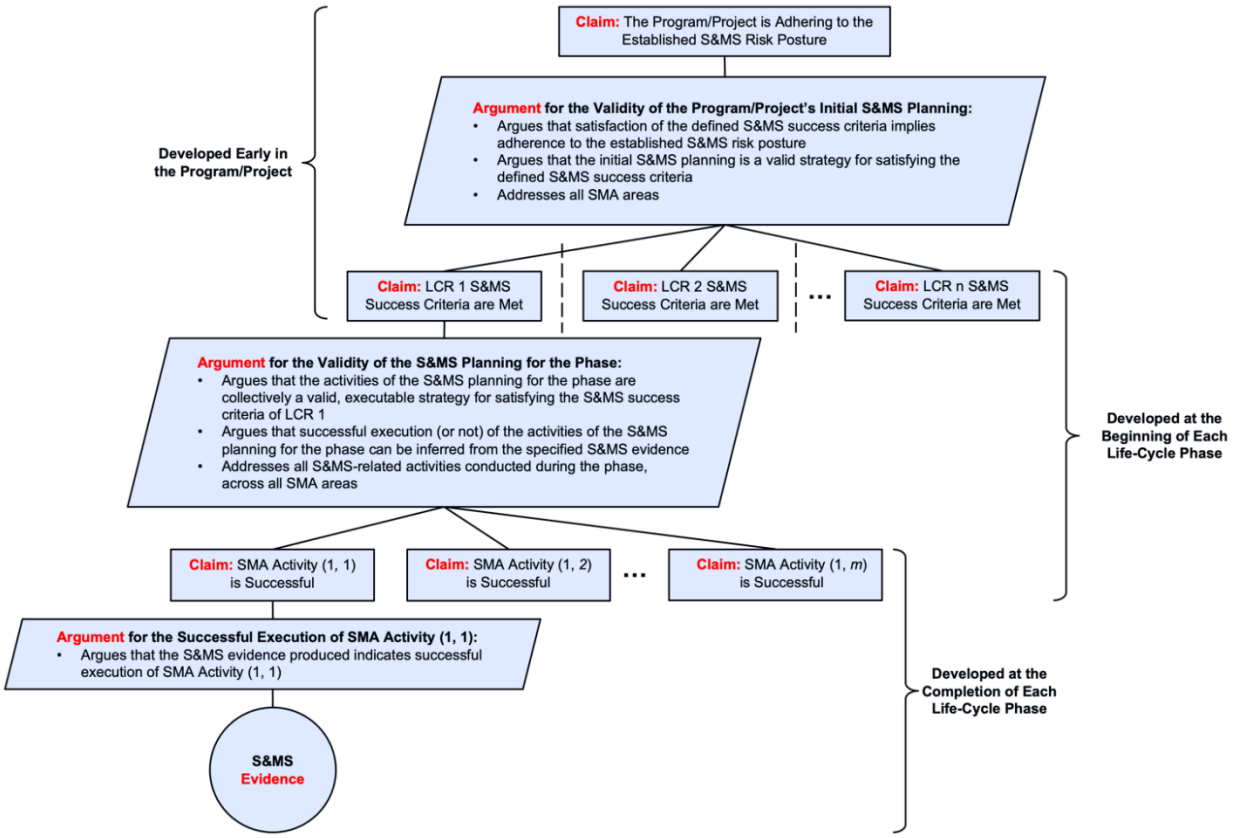

Figure 8. Nominal structure of the S&MS assurance case

11.1.5 The S&MS assurance case evolves over the program or project life cycle and is submitted by the Provider to the Acquirer at each LCR. Initially, the case has the structure specified by the

[29] Deviations from the nominal case may be needed if the Provider cannot make the case that the S&MS risk posture is being adhered to (e.g., if technology development is not going as planned, if test failure causes cannot be identified, or if a supply chain has been disrupted).

[30] This guidance document recommends against a top claim of the form, "There is adequate assurance that the program/project is adhering to the established S&MS risk posture" because it is the Acquirer, not the Provider, who must be adequately assured, and who determines whether or not they are indeed adequately assured. It is not for the Provider to claim adequate assurance. The S&MS assurance case submitted by the Provider to the Acquirer provides the (primary) *basis* for that assurance, but it cannot itself make claims about the adequacy of that basis.

top portion of Figure 8 indicated by the text, "Developed Early in the Program/Project." This portion of the case makes an argument of the form, "*If* the LCR-specific S&MS success criteria are met, *then* the S&MS risk posture is adhered to." Its purpose is to decompose adherence to the S&MS risk posture into the LCR-specific accomplishments defined by the S&MS success criteria.

11.1.6 The middle and bottom portions of Figure 8 operate in each life-cycle phase.[31] It is the job of the Provider, through sequential life-cycle phase-specific S&MS planning and execution, to make the claim, "The LCR S&MS success criteria are met," come true. The middle portion of Figure 8 indicated by the text, "Developed at the Beginning of Each Life-Cycle Phase," makes arguments of the form, "*If* the SMA activities of the phase are successful, *then* the S&MS success criteria of the phase are met." The bottom portion of Figure 8 indicated by the text, "Developed at the Completion of Each Life-Cycle Phase," argues, for each phase, substantiated by the relevant S&MS evidence, that the SMA activities of the phase are indeed met. In other words, the S&MS evidence resolves the conditionals (the *ifs*) of the higher-level arguments of the S&MS assurance case, thereby substantiating the top claim that S&MS risk posture is adhered to.

[31] It may be the case that initial S&MS planning, including the development of S&MS success criteria, is an early task within the life cycle, rather than prior to it. For example, NPR 7120.5 [4] specifies that success criteria are developed during Formulation.

12. S&MS ASSURANCE WITHIN THE NASA PROGRAMMATIC HIERARCHY

12.1 Discussion

12.1.1 Figure 9 notionally provides an integrated view of S&MS assurance throughout the Agency. The figure illustrates the concept that the Acquirer-Provider relationship can exist at different levels in the programmatic hierarchy, and that the same organizational entity (e.g., a Program) can simultaneously be a Provider in one relationship (e.g., to a Mission Directorate) and an Acquirer in another (e.g., from a Project).

12.1.2 The left side of Figure 9 illustrates the flowdown of the S&MS risk posture from the Administrator level of the NASA programmatic hierarchy. This guidance document takes the position that the Acquirer is the entity that establishes the S&MS risk postures for its Providers, but these S&MS risk postures can flow down, whole or in part, from higher level entities.[32] The requirement in Section 5.3 that Acquirer-established S&MS risk tolerances align with the Agency's risk posture ensures a coherent, Agency-wide approach to S&MS assurance, consistent with the philosophy of risk leadership set forth in NPD 1000.0 [1].

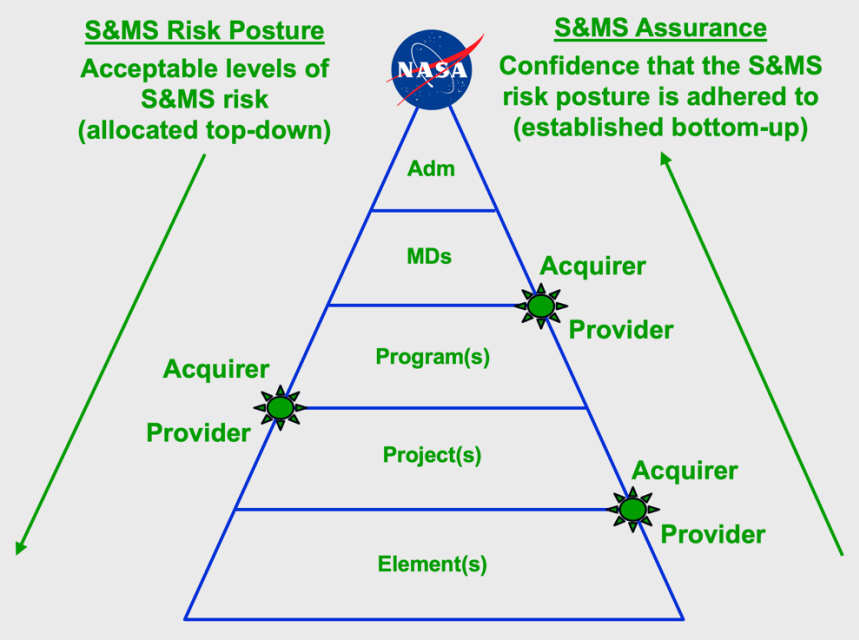

Figure 9. S&MS assurance within the NASA programmatic hierarchy

12.1.3 The right side of Figure 9 illustrates the building up of S&MS assurance from lower levels of the NASA programmatic hierarchy. Entities who are confident that their Providers are adhering to their S&MS risk postures are in a position to have confidence that they are adhering

[32] For example, NPD 8705.2 [17] requires the specification of Administrator-approved safety goals and safety thresholds that define long-term targeted and maximum tolerable levels of risk to the crew as guidance to developers in evaluating "how safe is safe enough" for a given type of mission.

to their own S&MS risk postures, presuming of course that they themselves are on track. Conversely, an Acquirer who does not have confidence that their Providers are adhering to their S&MS risk postures are simply not in a position to have confidence in their own adherence, if that adherence depends on the performance of their Providers.

12.1.4 Acquirers and Providers should coordinate their LCRs so that the timing of their corresponding LCRs reflects the dependencies between them. In general, for LCRs that reflect system and/or mission definition, the Acquirer-level LCR should precede the Provider-level LCR. For example, in the case of SRR, Acquirer-level requirements should be baselined before they are flowed down to the Provider. Correspondingly, the Acquirer's SRR should precede the Provider's SRR. Conversely, for LCRs that reflect system and/or mission realization, the Provider-level LCR should precede the Acquirer-level LCR. For example, in the case of SAR, Provider-level subsystem acceptance should precede Acquirer-level integrated system acceptance. Broadly speaking, Acquirer-level LCRs should precede Provider-level LCRs for activities that are predominantly concerned with the left side of Figure 9, whereas Provider-level LCRs should precede Acquirer-level LCRs for activities that are predominantly concerned with the right side of Figure 9. This same distinction between downward and upward can be seen in the process interactions of the NASA systems engineering engine, as illustrated in Figure 10, reproduced from [7].

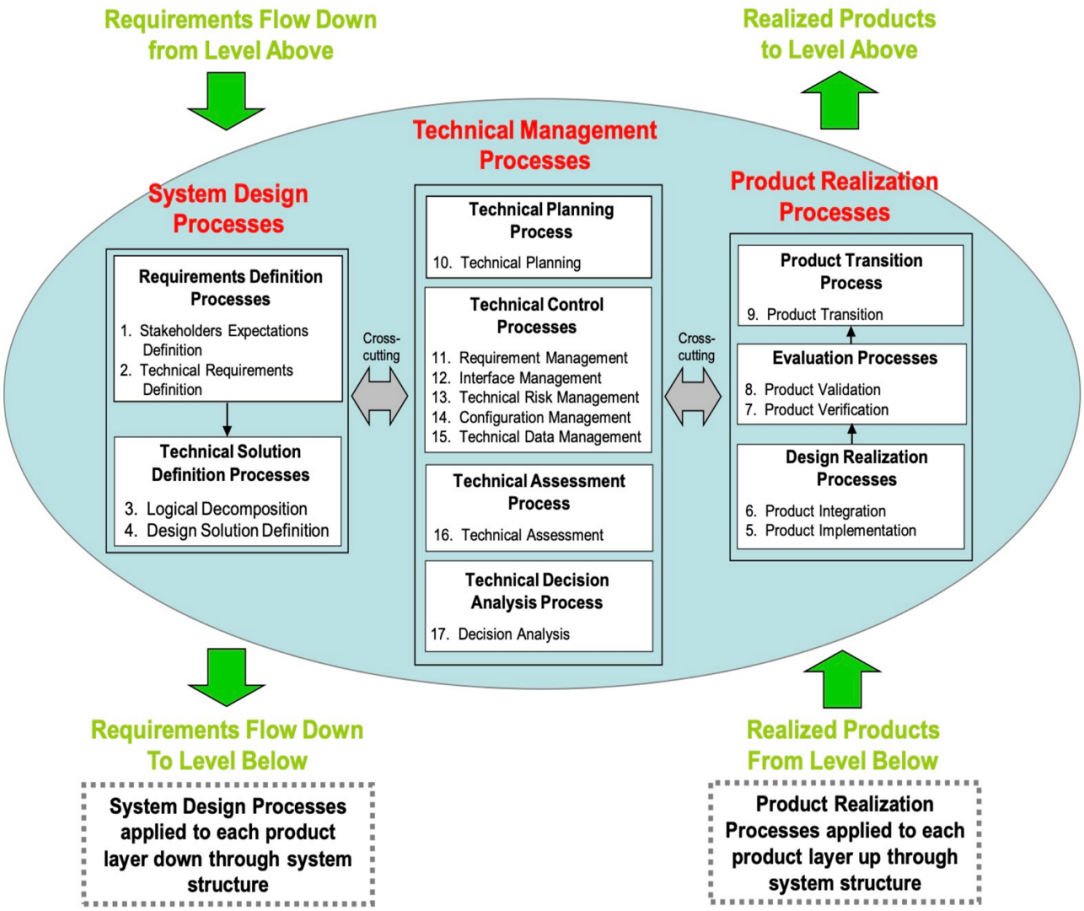

Figure 10. The NASA system engineering (SE) engine

13. EXAMPLE REQUIREMENTS COMPLIANCE MATRICES

13.1 Instructions

13.1.1 The example requirements compliance matrices in Table 6 through Table 9 illustrates a means of documenting a program's or project's compliance or intent to comply with S&MS-assurance-framework-related requirements, using the illustrative requirements of section 5.

13.1.2 For each illustrative requirement, the matrices provide:

a. The paragraph number of the requirement.

b. The requirement statement.

c. A "Comply?" field for identifying the program's or project's approach to the requirement. An "FC" is inserted for "fully compliant," "T" for "tailored," or "NA" for a requirement that is "not applicable."

d. A "Responsible Individual" field for identifying, by position title and organization name, the specific individual or individuals responsible for complying with the requirement.

e. A "Justification" field for documenting the rationale for tailoring, how the requirement will be tailored, or why the requirement is not applicable.

13.1.3 Table 6 and Table 7 list the illustrative Acquirer requirements and the illustrative TA requirements.[33] Table 8 and Table 9 list the illustrative Provider requirements.

13.1.4 Table 6 and Table 8 list the illustrative requirements that apply once to each program or project. Table 7 and Table 9 list the illustrative requirements that apply once for each life-cycle phase. It is expected that a multi-phase program or project would use one instance each of the Table 6 matrix and the Table 8 matrix, and multiple instances each of the Table 7 matrix and the Table 9 matrix – one for each phase.

[33] The TA requirements have been grouped with the Acquirer requirements for convenience. In general, a requirement levied on the TA is expected to be complied with by the TA at the organizational level above the one producing the information for which a TA concurrence decision is required.

Table 6. Example Acquirer Requirements Compliance Matrix – Life-Cycle Scope

Paragraph Number	Requirement Statement	Comply?	Responsible Individual	Justification
5.3.2	At program or project initiation, the Acquirer **shall** identify all at-risk entities and associated mission safety objectives.			
5.3.3	At program or project initiation, the Acquirer **shall** establish an S&MS risk posture that includes a set of risk tolerances which: a. Align with the Agency's risk posture. b. Address each mission safety objective. c. Address each mission technical objective.			
5.3.4	The Acquirer **may** define the S&MS risk posture: a. Quantitatively or qualitatively. b. In absolute or relative terms.			
5.3.5	The Acquirer **shall** include in the S&MS risk posture the specification that the mission is ASARP.			
5.3.6	Prior to Provider S&MS-related planning, the Acquirer **shall** obtain a TA concurrence decision, including documented rationale, regarding: a. The alignment of the S&MS risk posture with the Agency's risk posture. b. The completeness of the S&MS risk posture, in terms of: (1) The completeness of the set of at-risk entities. (2) The establishment of a mission safety objective for each at-risk entity. (3) The establishment of a risk tolerance for each mission safety objective and each mission technical objective. c. The feasibility of adhering to the safety-related elements of the mission S&MS risk posture.			
5.3.7	Prior to Provider initial S&MS-related planning, the Acquirer **shall** levy S&MS-related technical and process requirements deemed necessary to ensure and/or assure adherence to the established S&MS risk posture.			
5.3.8	The Acquirer **should** keep the number of Acquirer-levied S&MS-related technical and process requirements to a minimum.			
5.3.9	Prior to Provider initial S&MS-related planning, the Acquirer **should** obtain a TA concurrence decision, including documented rationale, regarding the necessity of the Acquirer-levied S&MS-related technical and process requirements for ensuring and/or assuring adherence to the S&MS risk posture.			

5.3.10	TAs **should** consider treating TA non-concurrences generated by the requirements of this section as formal dissents.			
5.4.9	At program or project initiation, the Acquirer **shall** obtain a TA concurrence decision, including documented rationale, regarding the validity of the initial S&MS-related planning, including the S&MS success criteria.			
5.4.11	TAs **should** consider treating TA non-concurrences generated by the requirements of this section as formal dissents.			

Table 7. Example Acquirer Requirements Compliance Matrix – Phase-Specific

Paragraph Number	Requirement Statement	Comply?	Responsible Individual	Justification
5.5.3.2	Providers and Acquirers **shall** subject all adjustments made to the S&MS success criteria to the requirements of Section 5.4.			
5.5.4.3	Prior to life-cycle phase execution, the Acquirer, in negotiation with the Provider, **may** define S&MS audit and reporting requirements for the phase as needed to: a. Monitor Provider progress relative to the S&MS-related planning for the phase (e.g., via the tracking and trending of S&MS-related technical metrics). b. Assess the adequacy of implementation of the phase's S&MS-related process requirements. c. Understand, analyze, or investigate unplanned events that occur during phase execution.			
5.5.4.4	Prior to life-cycle phase execution, the Acquirer **shall** obtain a TA concurrence decision, including documented rationale, regarding: a. The validity of the detailed S&MS-related planning for the phase with respect to the S&MS success criteria of the associated LCR(s). b. The validity of the S&MS evidence specifications as verifications that the associated S&MS success criteria have been met. c. The adequacy of the S&MS audit and reporting requirements for the phase to provide the Acquirer with sufficient and timely insight into the Provider's execution of the phase.			
5.5.4.6	The Acquirer **shall** treat acceptance of the Provider's S&MS-related planning for the phase as an S&MS risk acceptance decision requiring single-signature risk acceptance.			
5.5.4.7	TAs **should** consider treating TA non-concurrences generated by the requirements of this section as formal dissents.			
5.5.5.3	The Acquirer and TA **should** review Provider reports and conduct audits of S&MS-related Provider processes as needed to assess the quality and effectiveness of their execution and develop an adequate understanding of any unplanned events.			
5.5.5.4	The Acquirer **may** process all Provider reports and Acquirer audits of S&MS-related Provider processes according to existing Acquirer issue management processes.			

5.5.6.2	Prior to each LCR, the Acquirer **shall** obtain a TA concurrence decision, including documented rationale, regarding: a. The validity of the argument of the S&MS assurance case that S&MS success criteria up to and including those of the pending LCR have been met. b. The conformance of the S&MS evidence to the S&MS evidence specifications committed to by the Provider in the S&MS-related planning for the phase. c. The validity of the substantiation of the claims of the S&MS assurance case by the S&MS evidence.			
5.5.6.3	In reviewing the Provider's S&MS assurance case prior to each LCR, the TA **should** document as actionable findings, and make available to both the Acquirer and Provider, any instances where: a. The S&MS assurance case does not provide sufficient assurance that the S&MS success criteria have been met. b. The S&MS assurance case indicates that the S&MS success criteria have not been met or are no longer met.			
5.5.6.7	The Acquirer **shall** evaluate the S&MS assurance case submitted by the Provider at each LCR.			
5.5.6.8	In reviewing the Provider's S&MS assurance case at each LCR, the Acquirer, possibly supported by an SRB, **shall** document as findings any instances where: a. The S&MS assurance case does not provide sufficient assurance that an S&MS success criterion has been met. b. The S&MS assurance case indicates that an S&MS success criterion has not been met or that a previously met S&MS success criterion is no longer met.			
5.5.6.9	The Acquirer **shall** render a documented judgement, with supporting rationale, regarding whether or not the Acquirer is adequately assured that the Provider is adhering to the S&MS risk posture and has complied with all applicable externally mandated and/or Acquirer-levied S&MS-related technical or process requirements.			
5.5.6.10	The Acquirer's rendered judgement in 5.5.6.9 above **may** be conditional on the satisfactory completion of corrective actions levied by the Acquirer on the Provider.			
5.5.6.11	The Acquirer **shall** treat granting the Provider the authority to proceed through the life cycle as an S&MS risk acceptance decision requiring single-signature risk acceptance.			

5.5.6.12	TAs **should** consider treating TA non-concurrences generated by the requirements of this section as formal dissents.			

Table 8. Example Provider Requirements Compliance Matrix – Life-Cycle Scope

Paragraph Number	Requirement Statement	Comply?	Responsible Individual	Justification
5.4.6	At program or project initiation, the Provider **shall** conduct initial S&MS-related planning that: a. Describes, at a high level, how the Provider intends to adhere to the established S&MS risk posture. b. Defines the S&MS success criteria that need to be satisfactorily demonstrated at each LCR to show that the Provider is adhering to the established S&MS risk posture. c. Specifies a baseline set of standards, requirements, and practices the Provider commits to in the service of ensuring and assuring adherence to the established program or project S&MS risk posture, including all externally mandated and/or Acquirer-levied S&MS-related technical and process requirements.			
5.4.7	The Provider **should** consult with the Acquirer in the development of S&MS success criteria in order to understand Acquirer S&MS assurance needs and expectations at each LCR.			
5.4.8	At program or project initiation, the Provider **shall** develop an argument that establishes the validity of the initial S&MS-related planning with respect to satisfaction of the defined S&MS success criteria, and the validity of the S&MS success criteria with respect to adherence to the established S&MS risk posture.			
5.4.10	At program or project initiation, the Provider **shall** obtain Acquirer approval of the initial S&MS-related planning, including the S&MS success criteria, indicating that the Acquirer considers satisfaction of the defined S&MS success criteria to be adequate grounds for proceeding through the program or project life cycle insofar as S&MS is concerned.			

Table 9. Example Provider Requirements Compliance Matrix – Phase-Specific

Paragraph Number	Requirement Statement	Comply?	Responsible Individual	Justification
5.5.3.1	Upon entering a new life-cycle phase, the Provider **may** adjust the S&MS success criteria of that phase as needed to reflect the current status of the program or project.			
5.5.3.2	Providers and Acquirers **shall** subject all adjustments made to the S&MS success criteria to the requirements of Section 5.4.			
5.5.4.1	Prior to life-cycle phase execution, the Provider **shall** conduct detailed S&MS-related planning for the life-cycle phase as needed to: a. Specify, at an executable level, the S&MS-related activities that will be conducted during the phase. b. Specify the S&MS evidence the Provider will produce to verify achievement of the S&MS success criteria of the phase.			
5.5.4.2	Prior to life-cycle phase execution, the Provider **shall** develop an argument that establishes the validity of the detailed S&MS-related planning for the life-cycle phase, i.e.: a. That successful execution of the phase according to the S&MS-related planning will result in achieving the S&MS success criteria of the associated LCR. b. That the S&MS evidence the Provider will produce meet the assurance needs of the Acquirer with respect to achieving the S&MS success criteria.			
5.5.4.5	Prior to life-cycle phase execution, the Provider **shall** obtain Acquirer approval of its S&MS-related planning for the phase, including provisions for S&MS-related audit and reporting, indicating that the Acquirer: a. Accepts that the S&MS-related planning is a valid means of achieving the S&MS success criteria. b. Accepts that the specified S&MS evidence is sufficient to substantiate achievement of the associated S&MS success criteria. c. Accepts that the S&MS audit and reporting requirements for the phase meet the Acquirer's insight needs. d. Accepts that the Provider is ready to execute the S&MS-related planning.			
5.5.5.1	The Provider **shall** execute the life cycle phase in accordance with the approved S&MS-related planning for the phase.			

5.5.5.2	In the event that the Provider determines that a departure from the S&MS-related planning is warranted, the Provider **shall** first replan the S&MS-related activities of the phase to reflect the departure according to the requirements of Section 5.5.4.			
5.5.6.1	Prior to each LCR, the Provider **shall** produce an S&MS assurance case (which **may** be an updating of the S&MS assurance case of the previous LCR), addressing the status of the program or project: a. With respect to the S&MS success criteria of the LCR. b. With respect to the S&MS success criteria of previous LCRs. c. With respect to the established S&MS risk posture.			
5.5.6.4	The Provider **may** address all TA S&MS assurance case review findings according to existing Provider issue management processes.			
5.5.6.5	The Provider **shall** submit the S&MS assurance case to the Acquirer at each LCR.			
5.5.6.6	The Provider **may** submit the S&MS assurance case in the form of a summary document, with references to supporting material that is available for Acquirer review.			

Appendix A: ESTABLISHING AND OPERATIONALIZING A RISK POSTURE

A.1 Introduction

A.1.1 Consistent with NPD 1000.1, *NASA Governance and Strategic Management Handbook*, the achievement of objectives, defined at various levels of the NASA organizational hierarchy, constitute success with respect to NASA operations and activities. Correspondingly, per NPR 8000.4, *Agency Risk Management Procedural Requirements*, risk is defined as the potential for shortfalls with respect to the achievement of objectives, and risk management generally is focused on ensuring that the risk to objectives is within acceptable levels. In other words, risk management at NASA is anchored to two bedrock elements:

1. A defined set of objectives that motivate NASA's operations and activities and the achievement of which define success.
2. A defined level of acceptable risk to each objective, the achievement of which motivates NASA's risk management activities and defines the successful management of risk.

A.1.2 These elements are captured in an organization's *risk posture*, defined in NPR 8000.4 as:

> *"Risk Posture: An expression of the agreed upon limits of risk an organization's leadership team is willing to accept in order to achieve one or more of its objectives. It is defined up front and in tandem with the development of objectives, consistently with Risk Leadership principles, and serves as the attitudinal framework for seeking a balance between the likelihood and benefit of achieving the objective(s), vs. the likelihood and severity of risks that may be introduced by the pursuit of achievement. Risk posture may change with time, in reflection of the evolution of leadership team attitudes or because of changes in priorities, but at any particular time, risk posture provides the de-facto basis for risk-informed decision making and continuous risk management."*[34]

A.1.3 It is worth noting that the term *risk posture* differs from the term *risk profile*, in that the former refers to the limits of acceptable risk, without reference to the actual risk an organization may be facing, whereas the latter refers to the actual risk an organization is facing, without reference to the limits of acceptable risk. The NASA Risk Management Handbook (NASA/SP-2024-3422) defines risk profile as:

> *"Risk Profile: The ensemble of assessed risks to an activity's top-level objectives."*

An organization whose risk profile is within its risk posture is successfully managing its risks.

---

[34] *Risk posture* as defined in NPR 8000.4 is closely analogous the term *risk appetite* as defined in the Enterprise Risk Management (ERM) Playbook jointly developed by the Chief Financial Officers Council (CFOC) and the Performance Improvement Council (PIC): *"Risk Appetite: The articulation of the amount of risk (on a broad/macro level) an organization is willing to accept in pursuit of strategic objectives and value to the enterprise."*

A.1.4. In the context of NASA's objectives, which originate with NASA's strategic objectives and flow down through NASA's directorates and into its programmatic and institutional organizations, risk postures likewise originate at the Agency level and are flowed down into programmatic and institutional organizations in tandem with the flowdown of objectives.

A.2 Establishing a Risk Posture

A.2.1 Risk postures originate at the Agency level in forums such as the Acquisition Strategy Meeting (ASM), where factors such as cost, performance, NASA ownership, workforce, policy, and schedule are prioritized in order of the importance of achieving the objectives related to each driver. These prioritizations are captured in a high-level *risk posture statement*, which is essentially a table that expresses the importance of achieving the objectives in each driver category, in terms of the amount of risk the Agency is willing to tolerate.

A.2.2 Table A-10 notionally illustrates a high-level risk posture statement of the type that could be applicable to a space flight program or project. A high-level risk posture statement for an institutional organization would typically have different objectives and categories, particularly relating to developing and maintaining capabilities and providing mission support services.

Table A-10. Example high-level risk posture statement (notional)

Risk Tolerance	Objectives Category	Rationale for Risk Tolerance
Very Low	**Safety**	NASA's constant attention to safety is the cornerstone upon which we build mission success. – NPD 1000.0
Low	**Cost**	The element must be producible within the allocated funding. Cost overruns threaten cancellation.
Low	**Technical Performance**	Technical requirements are fixed and cannot be relaxed without revisiting the entire mission architecture.
Moderate	**Ownership**	Long term, it is required that NASA own the overall design of the element.
Moderate	**Workforce**	Workforce retention is desired to the extent practical given the required skillset.
High	**Policy**	This acquisition is not considered instrumental for cultivating a competitive, domestic capability for this service.
High	**Schedule**	NASA has flexibility within a range of dates for full transition to P&O.

A.2.3 NPR 8000.4 defines risk tolerance as:

> *"Risk Tolerance: An expression of the limit of acceptable probability of a shortfall with respect to the achievement of an explicitly established and stated objective, which is defined consistently with the overall agreed upon Risk Posture and risk vs. benefit balance pursued by an organization, according to its established and communicated Risk Leadership principles."*

A.2.4 In other words, a risk tolerance is an upper bound on the amount of risk to an objective that an organization is willing to accept. If the risk to an objective is above its risk tolerance, then the risk is unacceptable. If the risk is below the risk tolerance, and especially if the risk is far below the risk tolerance, then the risk is acceptable.

A.3 Operationalizing a Risk Posture

A.3.1 As discussed in Part 1 of the NASA Risk Management Handbook, a risk posture may be defined by high-level leaders in global qualitative terms, but it is the responsibility of lower-level organizational managers and technical risk experts to refine the risk posture to the point where the risks to the organization's defined objectives can be compared to the risk tolerances associated with those objectives to determine whether or not the organization's risks are acceptable. The character of the individual risk tolerances associated with the various objectives can vary within a given risk posture. An important part of operationalizing a high-level risk posture is making sure that:

1. The operationalized risk tolerances faithfully reflect the high-level risk tolerances. This entails interactions between the organizational unit that is operationalizing the risk tolerances and the Agency-level originators of the high-level risk tolerance to ensure that Agency risk tolerance expectations are met.
2. The operationalized risk tolerances are feasible. This entails risk-informed decision making (RIDM) early in the activity to ensure not only that the strategy is the right one, but also that the operationalized risk tolerances are realistic. RIDM provides assurance that risks can be managed to within the operationalized risk tolerances given the programmatic constraints.
3. Adherence to the operationalized risk tolerances is arguable to relevant oversight entities and decision makers. In order for the risk posture to function as the basis for risk acceptance decision-making, it must be possible to make the case that the risks an operation or activity are facing are within the stated risk tolerances. Because risk is inherently probabilistic and future-oriented, adherence to the risk posture cannot be "proven" in the conventional sense, but instead must be convincingly argued using potentially diverse lines of reasoning and pieces of evidence. These lines of reasoning and pieces of evidence are dependent on the organization's approach to achieving the objectives and managing the risk. Consequently, the operationalized risk tolerances (and the operationalized risk posture generally) can only be finalized in light of the organization's approach to achieving the objectives and managing the risk.

A.3.2 Table A-11 illustrates the refinement of high-level risk tolerances of Table A-10 into operational risk tolerances that are specific enough to provide a valid basis for risk management and risk acceptance decision-making.

Table A-11. Example operationalized risk posture (notional)

Risk Tolerance	Objectives Category	Operationalized Objective	Operationalized Risk Tolerance
Very Low	**Safety**	No Harm to Public	Casualty Expectation < X
		Safe Crew Return	Probability of Loss of Crew < Y%
		Avoid On-Orbit Collisions	Probability of On-Orbit Collision < Z%
Low	**Cost**	RDT&E Costs within Budget	Probability of Overbudget < M%
		Operating Costs within Budget	Probability of Overbudget < N%
Low	**Technical Performance**	Baseline Technical Requirement	Probability of Failure to meet Baseline Technical Requirement < Q%
		Threshold Technical Requirement	Probability of Failure to meet Threshold Technical Requirement < R%
Moderate	**Ownership**	NASA Ownership of Design	N/A (NASA can choose to retain ownership of design or not)
Moderate	**Workforce**	Workforce Retention > T%	Probability of Failure to meet Workforce Retention Objective < U%
High	**Policy**	None	N/A (NASA has chosen to not flow down a commercialization objective)
High	**Schedule**	Baseline Launch Date	Consistent with Similar Missions
		Threshold Launch Date	Probability of Failure to meet Threshold Launch Date < Z%

National Aeronautics and Space Administration