Implementing an Objectives-Driven, Risk-Informed, and Case-Assured Approach to Safety and Mission Success at NASA

Dezfuli H.[a*], Everett H.C.[b], Youngblood R.[b], Forsbacka M.[a]
[a]National Aeronautics and Space Administration, Washington D.C., USA
[b]Idaho National Laboratory, Idaho Falls, USA
[*]Contact author

Abstract: NASA is developing a "Standard for Assurance of Space Flight Safety and Mission Success" that implements an objectives-driven, risk-informed, and case-assured approach to safety and mission success (S&MS) for NASA space flight programs and projects. The standard aligns with the philosophy of risk leadership that has recently been established in NASA policy to assure acceptable levels of flight crew safety and mission success risk. It is consistent with existing NASA risk management requirements and is compatible with NASA program management and systems engineering requirements.

The methodology described in the standard is presented in terms of an S&MS assurance framework that is designed to allow substantial flexibility in the specific means by which programs and projects achieve acceptable mission S&MS risk. Such flexibility is necessary to accommodate the increasingly broad range of acquisition strategies employed by NASA, including commercial transportation services, as well as to accommodate the increasingly rapid evolution of space flight-related technologies and practices.

A key feature of the S&MS assurance framework is the specification of S&MS success criteria for each life-cycle review (LCR). The S&MS assurance case is structured around these criteria, the satisfaction of which indicates that the program/project is adhering to the S&MS risk posture. This enables the evolving S&MS assurance case to be used as a fundamental program/project submittal at each LCR, where its inherent structure of argument, supported by evidence, directly supports the evaluation of the program/project with respect to the S&MS success criteria, and by extension, the S&MS risk posture. As such, the S&MS assurance case is integral to program/project systems engineering, risk management, and S&MS oversight activities, and provides the principal basis for S&MS risk acceptance by the Decision Authority throughout the program/project life cycle.

Keywords: NASA, Assurance Case, Safety Case, Objectives-driven.

1. INTRODUCTION

NASA is developing a "Standard for Assurance of Space Flight Safety and Mission Success" that implements an objectives-driven, risk-informed, and case-assured approach to safety and mission success (S&MS) for NASA space flight programs and projects that codifies the intent of NASA policy to assure acceptable levels of flight crew safety and mission success risk [1]. It is objectives-driven in that S&MS-related activities are anchored to an explicitly established and stated *S&MS risk posture* defining the limits of acceptable risk to safety and to the mission technical objectives. It is risk-informed in that decisions made throughout the life cycle are informed by evaluations of their effects on S&MS risk and, in particular, on the standing of the program/project with respect to the S&MS risk posture. It is case-assured in that the onus is on the provider of the space flight system or service to make the case to the acquirer of said system or service that the S&MS risk posture is indeed being adhered to. This approach to S&MS contrasts with traditional prescriptive approaches where S&MS risk is deemed acceptable based on compliance with accepted technical and process standards, even in the absence of any attempt to explicitly characterize the S&MS risk itself.

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

The S&MS assurance framework defined in the standard builds on existing case-based assurance practices and lessons learned in other industries 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 NASA policy to assure acceptable levels of flight crew safety and mission success risk into existing NASA processes, rather than to establish a separate and/or parallel process.

The standard is consistent with NASA's existing requirements for programmatic decisions to accept S&MS risks [2] and compatible with NASA's existing program and project management requirements [3,4], acquisition policy [5], and systems engineering practices [6].

2. ROLES & RESPONSIBILITIES IN THE S&MS ASSURANCE FRAMEWORK

The roles and responsibilities in the S&MS assurance framework are defined generically in that they refer to the generic organizational entities: Acquirer, Provider, Technical Authority (TA), and Standing Review Board (SRB). The standard makes no assumptions about the organizational or management structures within these entities.

2.1. Acquirer (NASA entity)

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 key decision points (KDPs).

2.2. Provider (NASA or non-NASA entity)

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.

2.3. TA and SRB (NASA entities)

TAs and SRBs are independent technical review entities that are integral to 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.

3. THE "W-ENGINE" FOR S&MS ASSURANCE

The S&MS assurance framework takes the form of a "W-Engine" for S&MS assurance, as illustrated in Figure 1. The W-Engine is initialized at the outset of a program or project and is implemented iteratively over the phases of the program/project life cycle. The framework of Figure 1 assumes a single life-cycle review (LCR) at the end of each life-cycle phase. It is intended that in actual application, the 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. As such, the standard does not advocate for any specific life-cycle phases or LCRs. Instead, it is meant to accommodate the potentially wide variety of program and project structures that may be associated with both traditional and non-traditional acquisition strategies. The elements of the engine are summarized in the following subsections.

3.1. Initializing the "W-Engine" for S&MS Assurance

The main role of the Acquirer in initializing the W-Engine is to establish the mission S&MS risk posture and levy any additional S&MS-related technical or process requirements considered essential to S&MS assurance.[1] As discussed previously, the S&MS risk posture defines the limits of acceptable S&MS risk and is central to

[1] The Acquirer should keep the number of Acquirer-levied S&MS-related technical and process requirements to a minimum. The over-imposition of requirements runs counter to the intent of NASA to give Providers flexibility in the means by which they adhere to the established S&MS risk posture.

the objectives-driven, risk-informed, and case-assured approach of the S&MS assurance framework. The establishment of an S&MS risk posture is addressed in more detail in Section 4 below.

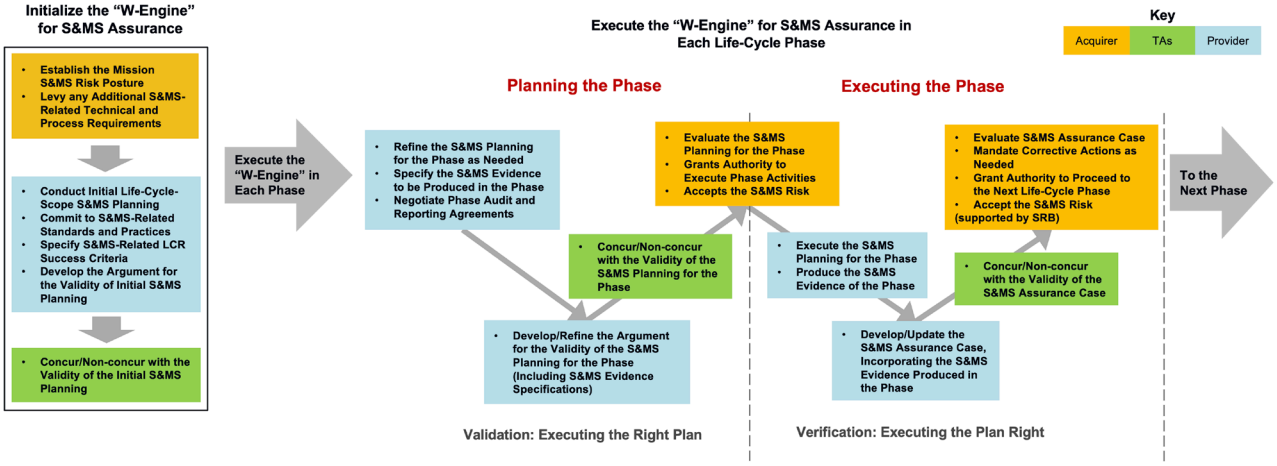


Figure 1. The "W-Engine" for S&MS Assurance

The role of the Provider in initializing the W-Engine is to conduct initial S&MS-related planning[2] reflecting 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). In particular:

a) Initial S&MS-related planning describes, at a high level, how the Provider intends to adhere to the established S&MS risk posture.
b) 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.
c) Initial S&MS-related planning specifies the *S&MS success criteria* to be used by the Acquirer to evaluate program or project status at LCRs. S&MS success criteria play a key role in the S&MS assurance framework and must be defined such that satisfaction of the S&MS success criteria indicates, to the Acquirer's satisfaction, that the S&MS risk posture is being adhered to. Therefore, the S&MS success criteria must address 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.

In addition, the Provider is required to develop an *argument* that establishes the validity of the initial S&MS-related planning with respect to the defined S&MS success criteria, and the validity of the S&MS success criteria with respect to the established S&MS risk posture. In other words, the argument should make the case that successful execution of the S&MS planning will result in the S&MS success criteria being satisfied, and that satisfaction of the S&MS success criteria indicates that the S&MS risk posture is being adhered to. As will be seen in Section 5 below, 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*.

Finally, the Acquirer obtains a concurrence decision from the TAs regarding the validity of the initial S&MS-related planning, and the Provider obtains approval from the Acquirer to proceed in the program/project life cycle.

3.2. S&MS Assurance Within a Life-Cycle Phase

Within a life-cycle phase the W-Engine has two primary activities: 1) planning the phase, and 2) executing the phase. Phase planning and execution are conducted by the Provider. The Acquirer, assisted by the Independent

[2] The S&MS assurance framework 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.

Technical Review Entities, evaluates the Provider activities to 1) validate the S&MS-related planning for the phase, and 2) verify the successful execution of the S&MS-related planning at the LCR that terminates the phase.

3.2.1. Phase-specific S&MS-related planning

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 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.

The specification of *S&MS evidence* is a key element of phase-specific S&MS-related planning. The 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 therefore 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 each life-cycle phase is specified at the start of the phase to ensure that it isn't defined *ex post facto* as whatever ended up being produced in the phase.

Because the function of the S&MS evidence is to substantiate, to the Acquirer's satisfaction, 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 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.

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.

In addition, as with the initial S&MS-related planning, the Provider is required to develop an *argument* that establishes the validity of the phase-specific S&MS-related planning. The argument should make the case that successful execution of the phase-specific S&MS planning will result in the S&MS success criteria being satisfied, and that the S&MS evidence that will be produced is sufficient to assure the Acquirer that the S&MS success criteria have been met. As will be seen in Section 5 below, the arguments for the validity of the phase-specific S&MS-related planning forms the basis for the lower-level structure of the S&MS assurance case.

Finally, the TAs 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 overall readiness of the Provider, the Acquirer grants the Provider the authority to execute the activities of the phase.

3.2.2. Execution 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[3], and producing the S&MS evidence that will be used to substantiate successful phase execution. The Acquirer and TA review Provider reports and conduct audits of S&MS-related Provider processes as agreed upon, to assess the quality and effectiveness of phase execution and develop an adequate understanding of any unplanned events.

During execution, 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." Figure 2 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 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.

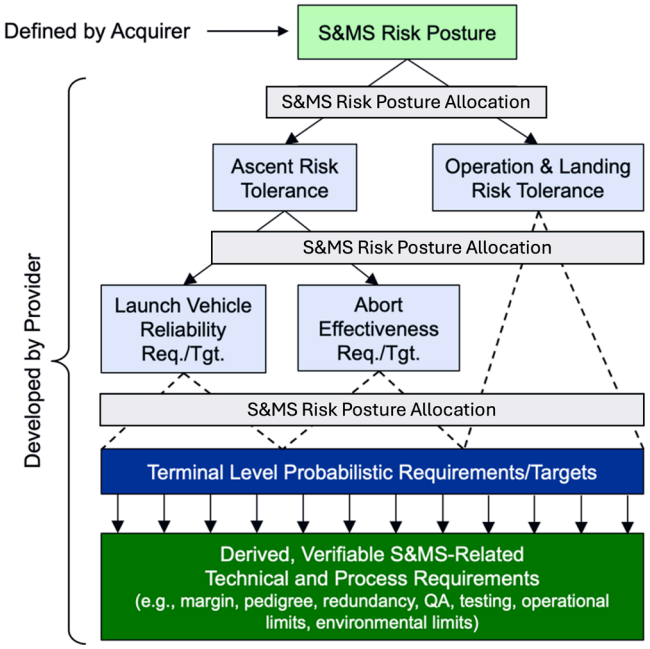


Figure 2. Derivation of Verifiable S&MS-related Requirements (notional)

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. The S&MS assurance case is the principal submittal to the LCR at the end of the phase and provides the primary basis for Acquirer S&MS risk acceptance and approval to continue in the life cycle. Prior to each LCR, the Acquirer obtains a TA concurrence decision regarding the validity of the case, including the substantiation of the claims of the case by the S&MS evidence, as well as any findings by the TA concerning areas of insufficient assurance. 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

[3] Modifications to S&MS-related planning must go through the same process of evaluation and approval as the original planning.

acceptance. The phase ends with the Acquirer granting the Provider authority to proceed, potentially with mandated corrective actions coming out of the LCR.

S&MS assurance case development is addressed in more detail in Section 5 below.

4. ESTABLISHING AN S&MS RISK POSTURE

An S&MS risk posture is defined in the standard as an ensemble of risk tolerances associated with the mission safety and technical objectives, along with the expectation that the mission will be as safe as reasonably practicable (ASARP). It may be expressed quantitatively and/or qualitatively, and in absolute or relative terms.

At the leadership level, stakeholder expectations concerning the S&MS risk posture are typically qualitative and derived from Agency priorities. However, adherence to it requires it to be allocatable into the system down to the level of verifiable requirements and specifications (e.g., as lower-level reliabilities, availabilities, margins, operating limits, quality controls, etc.). Therefore, at least for high-priority objectives, it is expected that stakeholders' qualitative risk tolerances will tend to be translated into quantitative risk tolerances as an integral part of the SE process. The recommended character of an S&MS risk posture as a function of risk tolerance class [7] is presented in Table 1.

Table 1. Graded Approach to Establishing an S&MS Risk Posture

Mission/Instrument Risk Tolerance Class	Recommended Character of the S&MS Risk Posture
A	• Stringent, quantitative S&MS risk posture (e.g., very low mission success risk tolerance: "P(LOM) ≤ 1 in X") • ASARP
B	• Less stringent, quantitative S&MS risk posture (e.g., moderately low mission success risk tolerance: "P(LOM) ≤ 1 in Y") • ASARP
C	• 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
D	• ASARP

A valid S&MS risk posture has the following five 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* – 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. Such mandated risk criteria should be 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) *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. 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). However, it 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). ASARP is discussed in more detail in Section 6 below.

e) *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.

Figure 3 illustrates a recommended 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, and ASARP. It takes place as part of the initialization of the W-Engine. At the core of the process is the conduct of an analysis of alternatives (AoA) to determine levels of S&MS risk that are both feasible and ASARP.

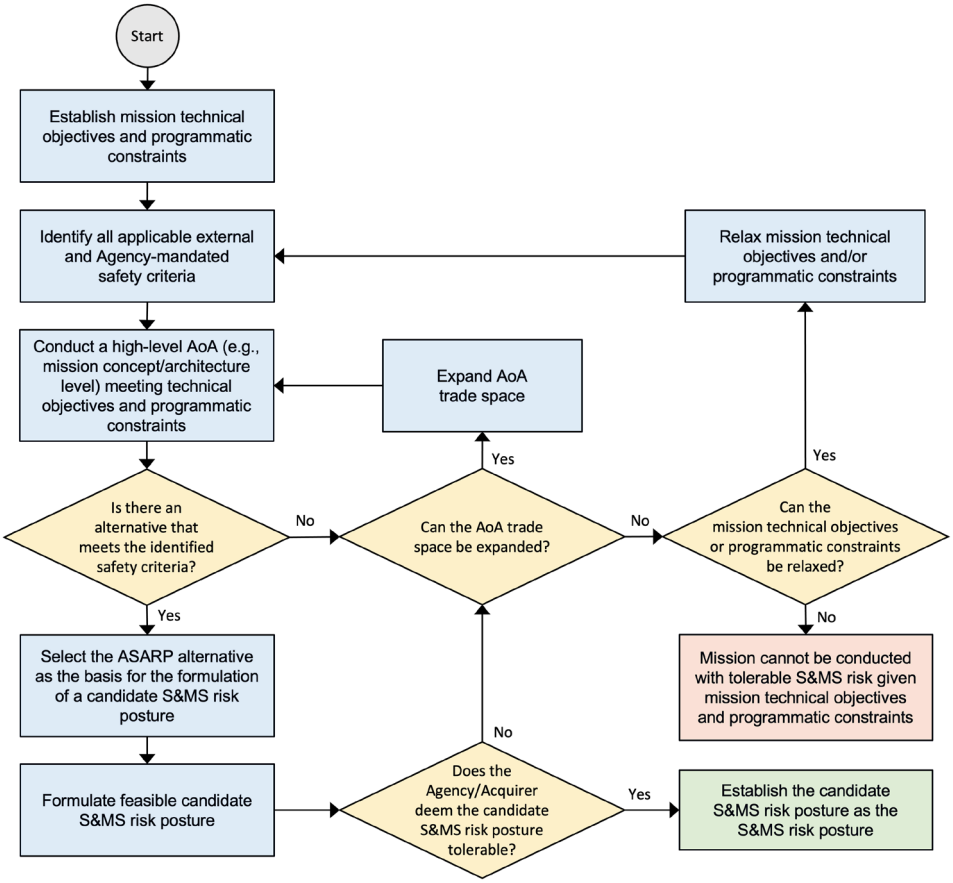


Figure 3. Recommended Process for Establishing a Mission S&MS Risk Posture

5. DEVELOPING AN S&MS ASSURANCE CASE

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.

The elements of the S&MS assurance case are [8]:

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.

The interaction of these elements is illustrated in Figure 4 for a claim supported by two independent arguments. Formalisms such as Goal Structuring Notation (GSN) [9] or Claims, Arguments, and Evidence (CAE) [10] may be used to impose rigor on the S&MS assurance case but are not necessary.

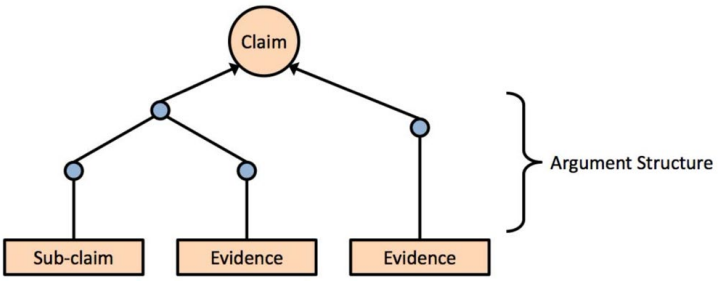


Figure 4. A Claim Supported by Two Independent Arguments

The nominal S&MS assurance case structure specified in the S&MS assurance framework is illustrated in Figure 5. The central claim (i.e., the top claim) is, "The program/project is adhering to the established S&MS risk posture."[4,5] 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.

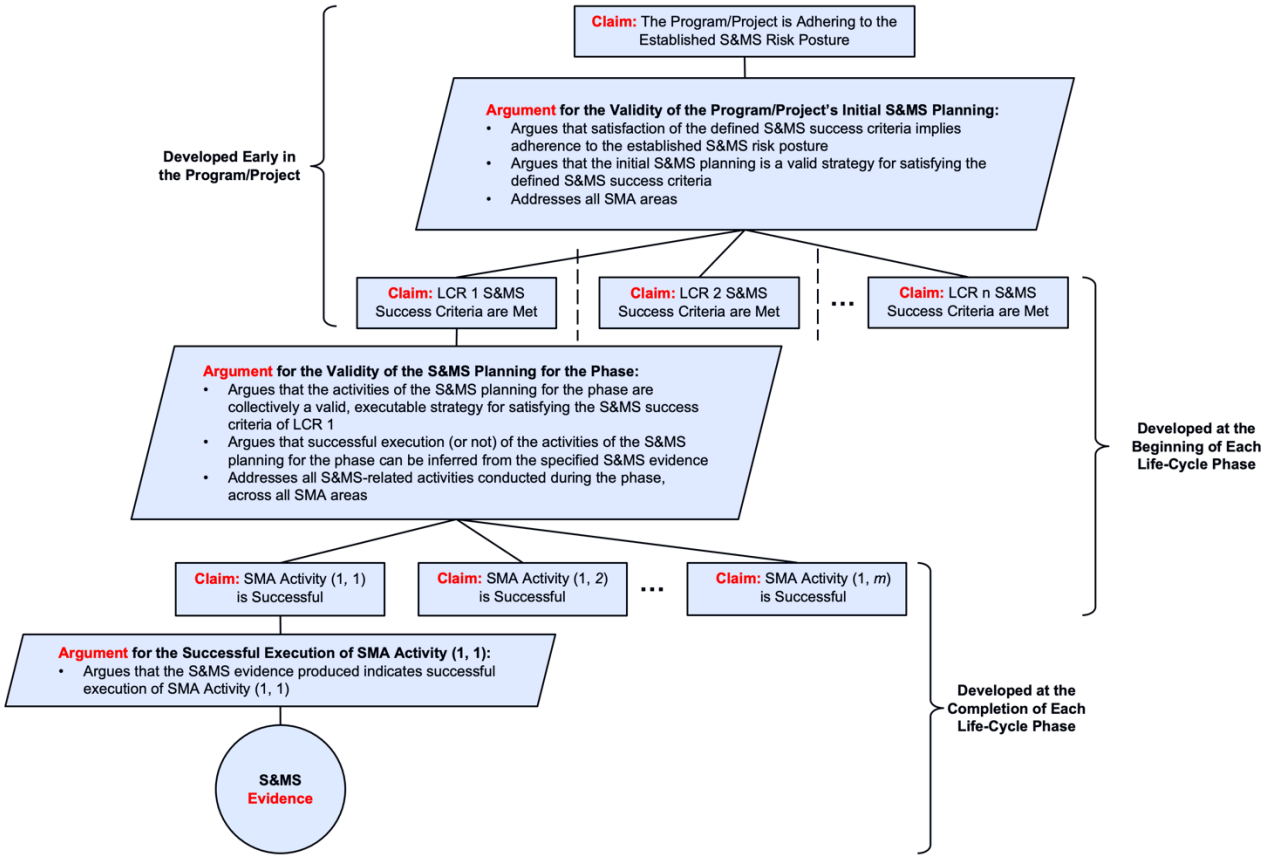


Figure 5. Nominal Structure of the S&MS Assurance Case

[4] 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).

[5] This standard 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.

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 top portion of Figure 5 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.

The middle and bottom portions of Figure 5 operate in each life-cycle phase.[6] 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 5 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 5 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 S&MS-related 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.

6. ENSURING THE MISSION IS ASARP

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" [1]. In practice, this entails prioritizing safety in decision-making throughout the program or project life cycle insofar as is practical.

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.

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.

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.).

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.

[6] 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 [3] specifies that success criteria are developed during Formulation.

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.

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 RIDM.

In the S&MS assurance framework, safety applies to all at-risk entities. It does not take a position concerning relative valuations among at-risk entities for the purpose of ASARP determination.

7. CONCLUSION

The "Standard for Assurance of Space Flight Safety and Mission Success" currently under development by NASA defines an objectives-driven, risk-informed, and case-assured framework for S&MS that implements NASA policy for safety and mission success as set forth in NPD 8700.1. Its promulgation is expected to facilitate NASA's evolution away from the traditional approach to acceptable S&MS risk, in which S&MS risk is deemed to be acceptable based on compliance with an often extensive set of prescriptive S&MS-related technical and process requirements, to a more flexible and agile approach that accommodates diversity and fosters innovation in the means by which NASA safely achieves its goals and objectives. This evolution has been motivated by a number of factors, such as the increasing use of commercial space transportation services, the emergence of innovative new technologies such as additive manufacturing, and the ongoing transformation of systems engineering (SE) practice from document-centric to model-based.

Acknowledgements

The authors would like to thank the NASA Office of Safety and Mission Assurance (OSMA) for their sponsorship of the work underlying this study [11], and Chet Everline at the Jet Propulsion Laboratory for his valuable contributions to the development of the S&MS assurance framework and the associated standard. Support to the Idaho National Laboratory was provided through Strategic Partnership Project (SPP) #01717 - Development and Implementation of Risk Management and System Safety Framework at NASA.

References

[1] NPR 8700.1, NASA Policy for Safety and Mission Success. NASA. 2022.
[2] NPR 8000.4, Agency Risk Management Procedural Requirements. NASA. 2022.
[3] NPR 7120.5, NASA Space Flight Program and Project Management Requirements. NASA. 2021.
[4] NPR 7120.8, NASA Research and Technology Program and Project Management Requirements, NASA. 2018.
[5] NPD 1000.5, Policy for NASA Acquisition. NASA. 2020.
[6] NPR 7123.1, NASA Systems Engineering Processes and Requirements. NASA. 2023.
[7] NPR 8705.4, Risk Classification for NASA Payloads. NASA. 2021.
[8] Bishop P and Bloomfield R. A Methodology for Safety Case Development. Sixth Safety Critical Systems Symposium: Industrial Perspectives on System Safety, 1998.
[9] Kelly T and Weaver R. The Goal Structuring Notation – A Safety Argument Notation. 2004.
[10] Adelard. CAE Framework, https://claimsargumentsevidence.org.
[11] Dezfuli H et al. Modernizing NASA's Space Flight Safety and Mission Success (S&MS) Assurance Framework in Line with Evolving Acquisition Strategies and Systems Engineering Practices, https://ntrs.nasa.gov/api/citations/20220003490/downloads/SMS%20Assurance%20Framework%20White%20Paper%20STI.pdf. 2021.