Modernizing NASA's Space Flight Safety and Mission Success (S&MS) Assurance Framework In Line With Evolving Acquisition Strategies and Systems Engineering Practices

Homayoon Dezfuli (NASA)
Chris Everett (Idaho National Laboratory)
Robert Youngblood (Idaho National Laboratory)
Chet Everline (Jet Propulsion Laboratory)

Office of Safety and Mission Assurance
National Aeronautics and Space Administration
NASA Headquarters
Washington, D.C. 20546

June 2021

Table of Contents

1 Introduction

The purpose of this paper is to present the objectives-driven, case-based safety and mission success (S&MS) assurance framework being developed by the NASA Office of Safety and Mission Assurance (OSMA), including its motivations and its implementation via a S&MS Assurance Standard [1] that is under development, supplemented by supporting standards including an S&MS Analysis Management Standard [2] that is also under development. This paper also discusses the retirement of NPR 8705.5 [3] and Chapter 2 of NPR 8715.3 [4], and how it is being accommodated by [1] and [2].

1.1 The Need to Evolve NASA's S&MS Assurance Framework

A need to evolve NASA's S&MS assurance framework has emerged in recent years, as articulated in findings from a variety of assessments from a number of internal and external stakeholders, such as the NASA System Safety Steering Group (S3G) [5] and the Aerospace Safety Advisory Panel (ASAP) [6-10]. The following subsections discuss some of the major motivations behind the development of the S&MS framework discussed in this paper.

1.1.1 The Need to Accommodate New Acquisition Models

In the last several years, NASA has begun to commercialize certain programs. This new acquisition strategy makes essential use of contractors in a manner that is different from NASA's use of contractors during earlier programs. In particular, NASA is making use of commercial transportation services, using commercially developed launch vehicles, such as the SpaceX Falcon 9, operated by the commercial provider rather than by NASA. For commercial service acquisition, the space flight program/project life cycles and life cycle reviews (LCRs) specified in, and required by, NPR 7120.5, *NASA Space Flight Program and Project Management Requirements* [11] are not practically applicable, given that NASA does not oversee the design, development, testing, and evaluation (DDT&E) of the systems used by the service provider.

Instead, S&MS assurance in a commercial service context should entail mechanisms by which 1) NASA, as the service acquirer, specifies the level of, say, launch reliability it expects from the provider (presumably as a function of NASA's overall risk tolerance for mission failure), as well as expectations for the protection of the relevant entities potentially put at risk by the service (i.e., crew, the public, equipment or property, or the environment), and 2) the service provider assures NASA that these expectations have been met (or, during implementation, that they are on track to being met), but in a manner of the provider's choosing, consistent with the provider's means of achieving them, so long as there is agreement between NASA and the provider that the S&MS assurance mechanism is valid.

1.1.2 The Need to Accommodate Evolving Systems Engineering Practices

In recent years, the discipline of systems engineering (SE) has been undergoing fundamental changes that reflect, in large part, the increasing use of digital technology. In particular, there is a movement at NASA towards a model-based systems engineering (MBSE) paradigm, including model-based mission assurance (MBMA) [12]. In MBSE, a virtual model of the system is created, typically while it is still in the designing and planning phase. The model is used as a singular reference source — a "single source of truth" — for SE activities and associated data. Moreover, the role of modeling and simulation in the identification and analysis of potential mission mishaps and/or accidents has been increasing, to the point where it is beginning to displace some traditional analysis techniques, such as probabilistic risk assessment (PRA) based on linked fault trees and

event trees. Modeling and simulation are being used both as alternatives to traditional PRA techniques, and combined with traditional PRA techniques to furnish hybrid approaches for assessing S&MS performance.[1]

An S&MS assurance framework that requires the provider to conduct specific prescribed S&MS analysis techniques will inevitably be rendered obsolete by continuing advances in SE practice. For NASA's S&MS assurance framework to provide value into the future, it must be agnostic with respect to the particular means by which S&MS-related information is produced, focusing instead on assuring that S&MS-related decisions are adequately informed by valid S&MS-related information.

1.1.3 The Need to Stipulate Acceptable Levels of S&MS Risk

Beginning in 2009, ASAP began advising NASA to establish acceptable risk levels for crewed space flight missions, issuing, in its Annual Report for 2009 [6], recommendation 2009-01-02A, stating:

> *The ASAP recommends that NASA stipulate directly the HRR acceptable risk levels including confidence intervals for the various categories of activities (e.g., cargo flights, human flights) to guide managers and engineers in evaluating 'how safe is safe enough.' These risk values should then be shared with other organizations [COTS] that might be considering the creation of human-rated transport systems so that they are aware of the criteria to be applied when transporting NASA personnel in space. Existing thresholds that the Constellation Program has established for various types of missions might serve as a starting point for such criteria.*

The charter of ASAP is to make recommendations related to safety, rather than S&MS broadly, and recommendation 2009-01-02A is consistent with that charter. However, in its 2013 report [7] ASAP raised the general issue of "risk accretion," writing that "there are many forms of risk in human space flight. Budgets, schedules, and mission accomplishment all have their attendant risks," and that risk accretion had been observed "in the Commercial Cargo Program, the Commercial Crew Program (CCP), the International Space Station (ISS), and Exploration Systems Development (ESD)." ASAP stresses the need to determine acceptable levels of risk, writing:

> *This "risk tolerance" decision requires balancing many factors, such as financial cost, schedule, national prestige, international relationships, human welfare, public opinion, and ethical considerations, to determine whether the chance of a mishap is outweighed by the likely mission benefit.*

In the most recent revision of the *NASA Governance and Strategic Management Handbook* [13], NASA began actively implementing a philosophy of *risk leadership* within an established risk posture that can and should extend all the way to the initial selection of mission proposals, especially recognizing and factoring in the various classes of missions, where each class can accept a different level of risk. NASA acknowledges the ASAP findings, writing:

> *There is a recognized need to define an appropriate risk posture along the lines of 'how safe is safe enough'. For instance, the ASAP noted in its recommendation 2009-01-02a:*

[1] S&MS Performance is defined in this paper as the likelihood that Mission Goals will be accomplished, and the likelihood that at-risk entities (people, assets, terrestrial environment, extraterrestrial environments, …) will not be adversely affected.

> *"[a risk-informed design] approach is viable only if a common understanding of "sufficiently safe" exists...and ...inconsistent "safe-enough" thresholds among various developers [can develop] if not carefully managed."*

An S&MS assurance framework that is responsive to ASAP's and the Agency's concerns about acceptable risk needs to include a mechanism for establishing risk tolerances (i.e., limits on the acceptable levels of S&MS performance) at a level of detail that meets stakeholder needs (mission, campaign, operation, etc.).

1.1.4 The Need for Improved Integration of S&MS into Systems Engineering

In its 2018 report [9], ASAP issued recommendation 2018-02-01, stating:

> *NASA Safety and Mission Assurance should have a coordinated, in-depth system of safety assurance tools and processes to verify effective programmatic safety compliance, system safety practices, safety process function, safety culture, and overall safety posture at all levels of the organization.*

In response, the OSMA conducted an S&MS capability assessment (SMSCA) [14] that found (among other things) that:

> *"S&MS was often treated as an afterthought at LCRs, and that the level of independent evaluation of S&MS at those reviews may be inadequate. This may be due not only to organizational stovepiping of S&MS and systems engineering, but also the conceptual stovepiping of S&MS that arises from not treating S&MS performance (e.g., probability of loss of mission, P(LOM), and probability of loss of crew, P(LOC)), as performance attributes of the system, to be managed within the systems engineering framework in an equivalent manner to other system performance attributes.*

The recommendation associated with this finding was:

> *S&MS should be integrated into systems engineering throughout the program/project life cycle. This includes processes for incorporating stakeholder S&MS expectations, such as S&MS performance targets, into system/mission definition, requirements definition, requirements validation, product realization, requirements verification, system validation, and operation and sustainment. Plans, analyses, etc., affecting S&MS should be subject to independent evaluation (e.g., by the SMA TA), but accountability for them and for the uses to which they are put should reside with program/project managers. Programs and projects should develop well-defined S&MS objectives for each life cycle phase, from which S&MS-related LCR success criteria are defined. This integration should be fully reflected in Agency NPRs, standards, etc.*

An S&MS assurance framework that is responsive to these recommendations should recognize that acceptable S&MS performance is a stakeholder objective and should be treated as such. In an SE context, this means that S&MS performance expectations should be elicited, codified, realized, and verified as an integrated part of the overall SE activity, using, to the maximum extent practicable, the same SE mechanisms used to address the stakeholders' technical objectives.

1.1.5 The Need for Clearer Accountability

In its report, "Recommended Updates to NASA Directives and Guidance to Clarify Technical Authority for Greatest Optimization" [15], OSMA documented a number of findings and made a number of recommendations concerning, among other things, potential conflicts of interest and

misalignment of authority with accountability in the existing implementation of Technical Authority. In its 2020 report [10], ASAP made a number of findings with respect to accountability, particularly with respect to systems engineering and integration (SE&I), including "a complex distribution of responsibilities and a lack of technical accountability for the integrated [Exploration Systems Development] (ESD) system," that "clear accountability for integrated SE&I risk management decision-making (as opposed to risk assessment) is ambiguous" in the Artemis program, and, for that program, "it remains unclear to the Panel who actually holds key accountability for integrated SE&I across the whole enterprise and between component programs." ASAP summarized their assessment of the Advanced Exploration Systems (AES) program by writing:

> *As NASA defines and initiates the acquisition strategy, architectural framework, and program structure for the long-term Artemis campaign, the Agency should ensure that clear roles and responsibilities are delineated, specifically related to the SE&I function. An SE&I approach with clear accountability is necessary to manage risk across the complete enterprise, especially given the meager experience base related to sending humans beyond LEO.*

An S&MS assurance framework that is responsive to these findings and recommendations should clearly define roles and responsibilities for each actor involved in achieving acceptable S&MS performance, with S&MS-related decision-making and S&MS accountability residing unambiguously within a well-defined programmatic chain of authority.

2 Objectives-Driven, Case-Based S&MS Assurance

OSMA has been addressing the need to evolve NASA's S&MS assurance framework in response to these and other findings for a number of years, beginning in the mid-2000s with the development of the NASA System Safety Handbook, Volume 1 [16], and continuing with a second volume of the handbook [17], as well as a number of white papers, etc., focusing on various specific aspects of S&MS assurance [5, 18-20]. The S&MS assurance framework that has emerged from these efforts is best described as *objectives-driven* and *case-based*, as explained in the following subsections.

2.1 An Objectives-Driven Approach to S&MS

An objectives-driven approach to S&MS is one that explicitly focuses S&MS efforts on meeting stakeholders' *fundamental S&MS objectives*, namely the achievement of mission technical objectives and the protection of at-risk entities from adverse mission consequences. These fundamental S&MS objectives, along with fundamental objectives in other domains such as cost, are what the stakeholders actually care about. Other S&MS-related objectives, such as failure tolerance, compliance with quality standards, or implementation of a problem reporting and corrective action (PRACA) process, are meaningful only to the extent that they support the fundamental S&MS objectives. In other words, they are *means objectives* that indicate particular *strategies* for meeting the fundamental S&MS objectives.

An objectives-driven approach to S&MS is appropriate for addressing NASA's evolving S&MS assurance framework needs because the achievement of fundamental objectives is really the only thing that the Acquirer needs to be assured of. Hence, given the clear articulation of the fundamental S&MS objectives, the Provider can be given the freedom to decide for itself (subject

to appropriate concurrences and approvals) the best means for achieving them. The NASA System Safety Handbook [16, 17] and the NASA Reliability & Maintainability (R&M) Standard [21] are explicitly objectives-driven. As described on the OSMA website, the R&M Standard represents "a new strategy to emphasize intent… to ensure that the Safety and Mission Assurance (SMA) disciplines and programs are addressing the challenges of NASA's changing missions, acquisition and engineering practices, and technology." The approach entails developing "a system of strategies and objectives that build upon each other to support the top objective, which states that 'system performs as required over the lifecycle to satisfy mission objectives'" [22]. An objectives-driven approach to S&MS is consistent with U.S. policy regarding regulations on the commercial use of space, which directs the Secretary of Transportation to consider replacing prescriptive requirements in the commercial space flight launch and re-entry licensing process with performance-based criteria [23]. In response to this policy, the Federal Aviation Administration (FAA) issued a new streamlined launch and reentry rule, 14 CFR Part 450 [24], that replaces prescriptive requirements with performance-based criteria. The new rule allows launch and reentry vehicle operators to focus on innovation as it replaces cumbersome, prescriptive requirements with flexible, performance-based criteria, resulting in better accommodation of the evolving commercial space transportation industry.

As illustrated in Figure 1, fundamental S&MS objectives are defined in strict association with fundamental mission objectives. For example, if fundamental mission objective #1 is "Collect 10 kg of lunar regolith and return it to Earth," then the associated fundamental S&MS objective #1 might be to do so with 90% probability of success.[2] Additionally, there is the qualitative fundamental S&MS objective that the mission be as safe as reasonably practicable (ASARP), which entails improving mission safety wherever practicable in an effort to optimize safety within the operational and management constraints of the mission. Below the fundamental objectives are the means objectives (A, B, C, and D in the figure), which collectively represent the Provider's strategies for meeting the fundamental mission objectives with likelihoods that meet the fundamental S&MS objectives.[3]

An objectives-driven approach to S&MS places an increased burden on the Provider to validate its solution (e.g., as defined by the means objectives / strategies), since the validity of the solution is not necessarily supported by past experience or adherence to existing standards.[4] This is in contrast to a prescriptive approach to S&MS in which solutions are presumptively deemed valid with respect to acceptable (but unspecified) S&MS performance by virtue of compliance.[5] An objectives-driven approach to S&MS also places an increased burden on the Acquirer and the independent technical review entities to evaluate the Provider's solution (and the Provider's validation of its solution), which can entail evaluation of the kind of novel and innovative strategies

[2] Strictly speaking, this is a fundamental mission success objective. In general, fundamental S&MS objectives partition into fundamental safety objectives and fundamental mission success objectives.

[3] The Acquirer may levy requirements for specific strategies it considers necessary for S&MS assurance, such as a requirement for a launch abort system (LAS). However, prescriptive levying by the Acquirer of such S&MS-related technical and process requirements should be done judiciously and with clear justification, recognizing that they constrain the solution space without necessarily providing an overall benefit to S&MS.

[4] It is possible that a valid solution cannot be found for a given set of fundamental S&MS objectives and mission constraints, in which case the Acquire would need to relax one or more objectives and/or constraints in order to move forward.

[5] Merely framing a prescriptive approach in terms of the "strategy" of compliance, without arguing the achievement of fundamental S&MS objectives, does not meet the definition of "objectives-driven."

the objectives-driven approach is meant to foster. Ultimately, the objectives-driven approach to S&MS holds each actor (Provider, Acquirer, and independent technical review entities) accountable for explicitly understanding (and in the Acquirer's case, accepting) the assessed S&MS performance of the Provider's solution.

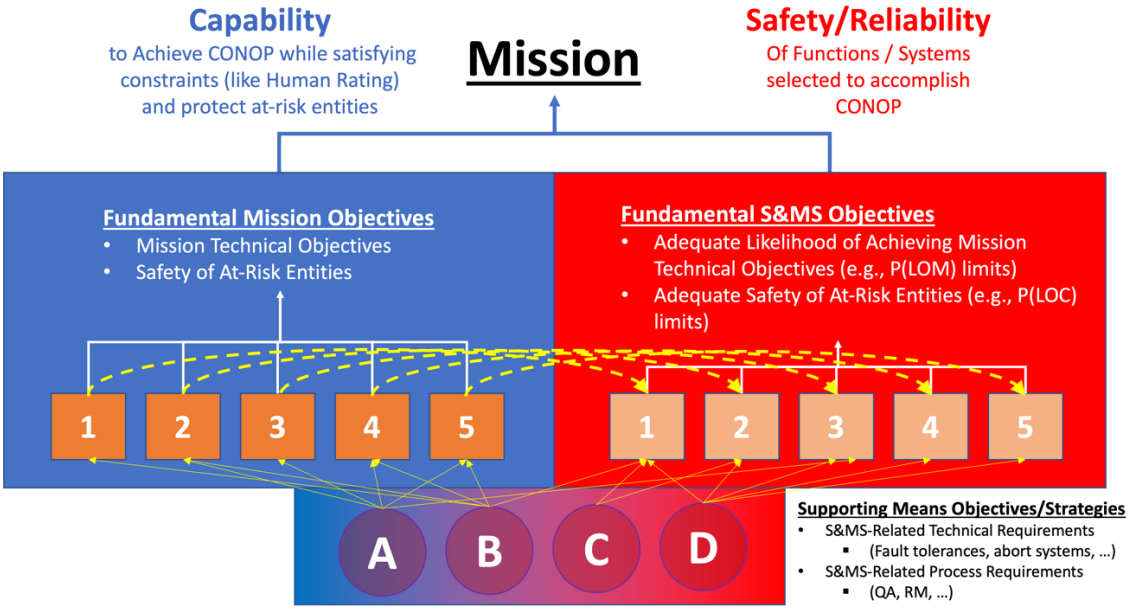

Figure 1. Fundamental S&MS Objectives in Context

2.2 Case-Based Assurance of S&MS Objectives

Fundamental S&MS objectives are inherently probabilistic, often relating to low levels of risk. Unfortunately, in general, low levels of risk cannot be absolutely proven. It is possible to furnish evidence that supports a claim that risk is low or reliability is high, but this is not the same as being able to measure those things in the same way that it's possible to definitively characterize the mass of a vehicle. Since reliability and risk cannot be proven, they have to be argued, based on convincing evidence; hence the use of the word "case."

The S&MS assurance case is defined as "a compelling, comprehensible and valid argument, supported by evidence, that a Provider has met, or is on track to meeting, the S&MS objectives." An S&MS Assurance case has two main elements: 1) an *S&MS argument*, typically presented in a hierarchical tree form, explicating the top-level claim that the Provider meets, or is on track to meeting, its S&MS objectives, in terms of a more specific set of claims; and 2) *S&MS evidence*, which substantiates those claims. 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. Figure 2 notionally illustrates the general structure of an S&MS assurance case. Additional guidance can be found in [16, 17, 27][6].

The S&MS assurance case is, by construction, what the Acquirer needs to support its S&MS risk acceptance decisions. OSMA has been proposing increased use of S&MS assurance cases in one form or other for some years, as reflected explicitly in [16, 17]. Further discussion of the benefits of a case-based approach to S&MS and the use that can be made of selected existing standards can

[6] The context of [16, 17] is system safety, but interpreted broadly enough to essentially equate to S&MS.

be found in the white paper, "Technical Resources Available for Development of a Prototype SMS Assurance Standard" [28]. Additionally, as part of its performance-based streamlining of its launch and reentry license requirements, a number of commercial providers advocated for the use of safety cases for equivalent level of safety (ELOS) demonstrations, with the FAA agreeing that such an approach would be allowed, though not required [29].

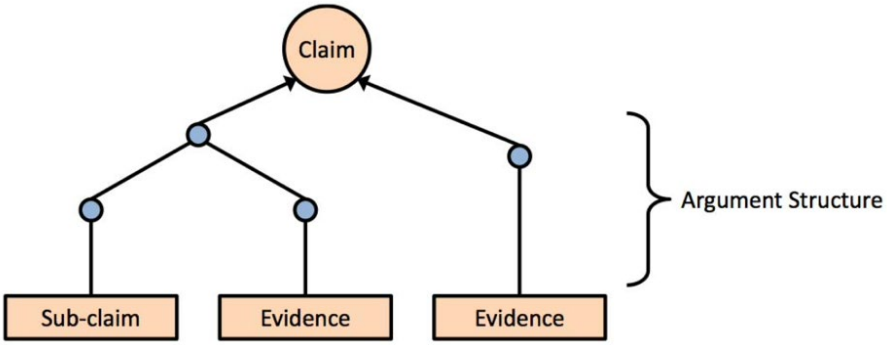

Figure 2. Notional S&MS assurance case structure

2.3 Comparison to a Prescriptive Approach

The differences between an objectives-driven, case-based approach to S&MS vs. a prescriptive approach is illustrated in Figure 3. Traditionally, in many application areas, documentation of compliance with prescriptive S&MS-related requirements has been deemed to provide presumptive assurance of adequate S&MS performance. Assuming that the requirements are a complete and valid set, there are advantages to this. One advantage is that a system is typically either "in compliance" or not, which simplifies the task of oversight, without necessarily improving the effectiveness of oversight. However, there are multiple disadvantages to reliance on prescriptive requirements: 1) such reliance tends to put the burden of "completeness and validity" on the drafters of the requirements, rather than on the system developers and operators; 2) it promotes a culture of compliance, rather than a culture of ownership of the safety and performance problems; 3) there is a tendency for drafters of prescriptive requirements to impose unnecessary burden on the system developers and operators, and; 4) it is difficult to formulate a comprehensive set of prescriptive requirements for novel technologies that operates without stifling the sort of innovation that NASA undertakings require. Trying to formulate prescriptive requirements a priori ends up forcing developers to request waivers from them; but waivers need, in principle, to be considered carefully in the context of a holistic technical basis for adequate S&MS performance, which is not available early in system development.

The objectives-driven, case-based approach to S&MS starts with articulation by the Acquirer of fundamental mission and S&MS objectives (and possibly some limited set of means objectives/strategies the Acquirer considers essential). The Provider is then challenged to formulate comprehensive sets of derived requirements whose collective satisfaction can be argued to meet the fundamental objectives. These derived requirements define the Provider's solution and drive subsequent SE activities. The S&MS assurance case then: 1) argues that satisfaction of these requirements provides reasonable assurance of satisfaction of the fundamental objectives; and 2) argues, supported by evidence, that the present development actually satisfies (or is on track to satisfy) these requirements. The S&MS assurance case is logically structured, evidence-based, comprehensive, and auditable; it is meant to be a primary basis for S&MS risk acceptance by the Acquirer.

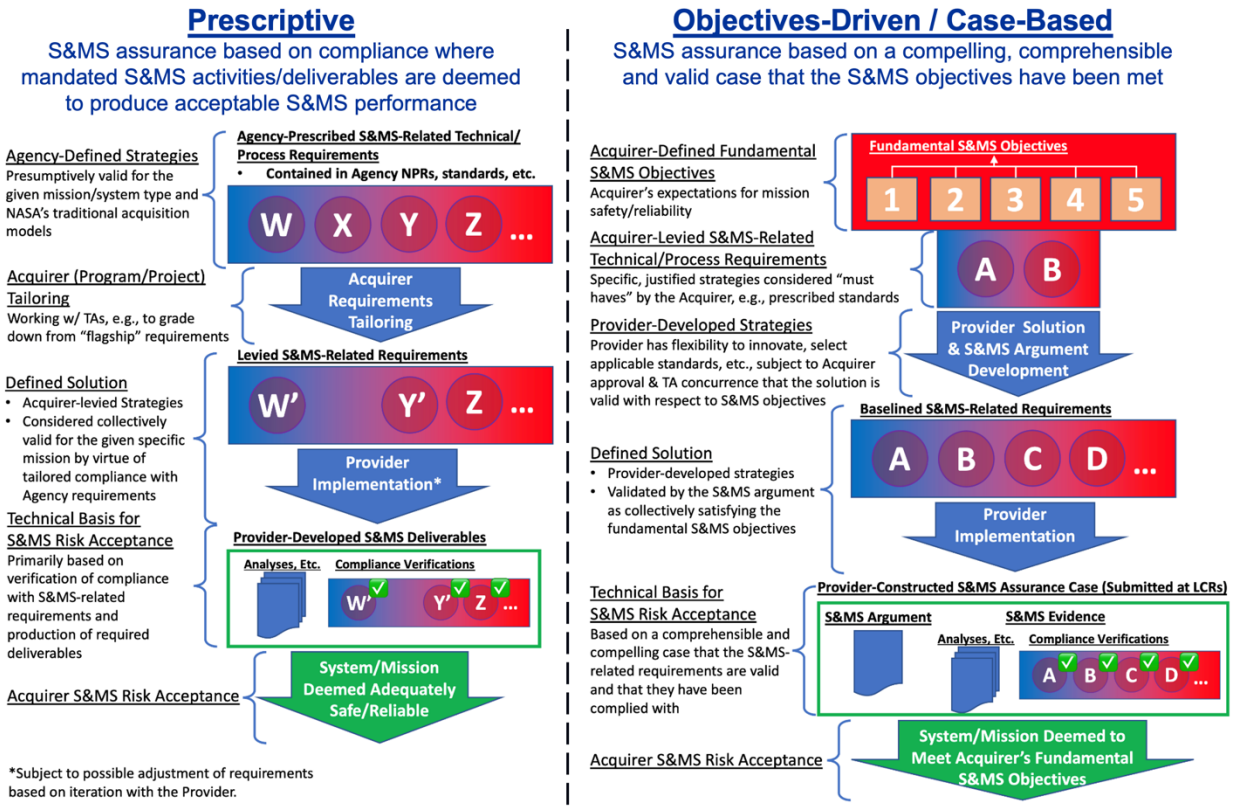

Figure 3. Objectives-driven, case-based vs. prescriptive S&MS

3 The Proposed S&MS Assurance Framework

The S&MS assurance framework proposed in this paper addresses the program/project-specific establishment of fundamental S&MS objectives (and any levied means objectives) and their assurance throughout the program/project life cycle.

3.1 Establishing Fundamental S&MS Objectives

3.1.1 Protection of At-Risk Entities

NPR 8715.3 [4] defines safety as freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. Figure 4 is an example taxonomic decomposition of safety into a set of specific at-risk entities within the more general categories of human safety, environmental safety, and asset safety.

3.1.2 Establishing Minimum Tolerable Levels of Safety

A minimum tolerable level of safety is a level of safety below which the risk of harm to the potentially affected entity is too high to justify the mission. Establishing minimum levels of safety is essentially a weighing of the potential for harm to one or more of the identified at-risk entities against the potential benefits of the mission, should it succeed. Consequently, minimum tolerable levels of safety are mission specific and are a function of the mission technical objectives, and it would not be appropriate to establish blanket minimum tolerable levels of safety absent an assessment of the value of the mission technical objectives.

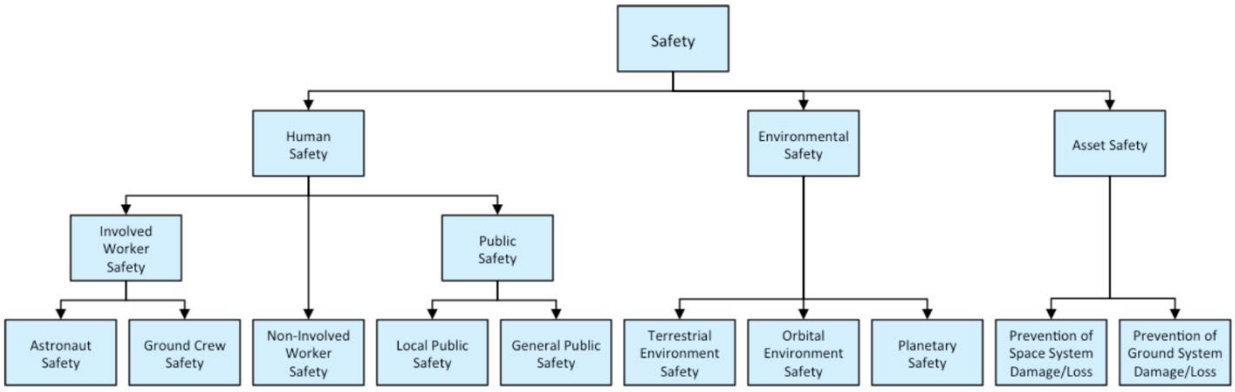

Figure 4. A generic safety taxonomy

Minimum tolerable levels of safety need not necessarily be quantified. For example, a minimum tolerable level of safety might be expressed as "at least as safe for the combined ascent and entry phases as the Space Shuttle was at the end of its operational life," reflecting a continuing tolerance of the level of safety that had already been tolerated in a prior system.

For some at-risk entities, minimum tolerable levels of safety are imposed by external stakeholders. For example, launch service providers are subject to 14 CFR 450, which imposes fatality risk criteria of 1×10^{-6} per launch to any individual member of the public and 1×10^{-5} per launch to any individual neighboring operations personnel [24]. Nuclear missions are subject to the Presidential direction that requires the probability of an accident resulting in exposure of 25 millirem to 5 rem to not exceed 10^{-2}, the probability of an exposure of 5 rem to 25 rem to not exceed 10^{-4}, and the probability of an exposure exceeding 25 rem to not exceed 10^{-5} [30]. Such requirements must be incorporated into the fundamental S&MS objectives of the mission. This does not, however, prevent NASA from establishing additional, more stringent minima, if it so chooses.

3.1.3 Addressing ASARP

In addition to meeting minimum tolerable levels of safety, adequate safety also consists of being ASARP. The ASARP principle is a reflection of NASA's ethical obligation to maximize safety insofar as is practicable, regardless of whether or not the mission meets minimum tolerable levels of safety. Being ASARP entails a continuous, proactive search for safety improvements, along with the prioritization of safety in decision-making, within limits of practicality.

3.1.4 Establishing Minimum Tolerable Levels of Mission Success Likelihood

In a similar manner, the mission technical objectives are identified and a minimum tolerable level of mission success likelihood given to each. Figure 5 presents a generic mission technical objectives taxonomy, showing prime, extended, and contingency objectives.[7]

3.2 Defining Adequate Progress Towards Meeting the Fundamental S&MS Objectives

NPR 7120.5 [11] establishes an SE management framework based on a phased life cycle model. Each life cycle phase has a specific function and results in defined deliverables (e.g., baseline design specifications, delivered system, delivered service, disposed system). The Acquirer maintains assurance that the program/project is on track to meeting its objectives, including the

[7] This taxonomy is notional and is presented to illustrate the potentially multidimensional nature of mission objectives. It is not meant to imply that all missions have objectives of the illustrated types.

fundamental S&MS objectives, by conducting life cycle reviews (LCRs) that provide a periodic assessment its technical and programmatic status and health. Example success criteria for these LCRs are provided in NPR 7123, *NASA Systems Engineering Processes and Requirements* [31].

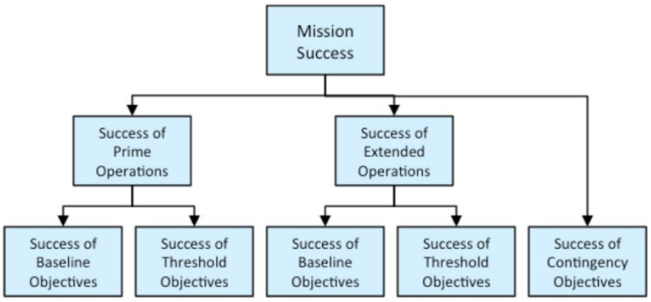

Figure 5. A generic mission objectives taxonomy

The proposed S&MS assurance framework recognizes that new acquisition paradigms may go beyond the prescribed life cycles and LCRs in NPR 7120.5, but also recognizes the need for the Acquirer to periodical assure itself that the Provider is on track to meeting the fundamental S&MS objectives. Such periodic assessments give the Acquirer an opportunity to identify areas where assurance is lacking and some form of intervention or corrective action is appropriate. Therefore, the S&MS framework involves, and in fact is organized around, LCRs as the principal forum at which the S&MS assurance is provided to the Acquirer (to the extent that the state of the program/project warrants it). A set of *S&MS success criteria* is defined for each LCR that indicate that the Provider is on track to meeting the fundamental S&MS objectives (as well as any Acquirer-levied S&MS means objectives/strategies) and that the program/project can progress further in the life cycle.

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 are collectively sufficient to indicate adequate progress towards and/or achievement of the fundamental S&MS objectives (and any levied means objectives). At a high level, the S&MS success criteria should address the generic elements of S&MS assurance shown in Table 1. These elements are addressed in different ways in different life cycle phases and at different LCRs, but in general provide a framework for developing valid S&MS success criteria, as well as for organizing the S&MS assurance case. It is the intent of Table 1 to illustrate, rather than to prescribe, how S&MS assurance decomposes into specific concerns about which an Acquirer may wish to be assured. The main point is that the Acquirer must have a well-developed and valid rationale for being assured of the fundamental S&MS objectives given satisfaction of the S&MS success criteria. The S&MS assurance elements represent an (illustrative) initial decomposition of that rationale that is consistent with the general philosophy of identifying, understanding, and controlling the threats to acceptable S&MS performance.

The validity of the S&MS success criteria is of crucial importance to S&MS assurance. To this end, the Provider must develop, and Acquirer accept, an argument for the validity of the S&MS success criteria along with the S&MS criteria themselves. The S&MS success criteria and associated argument can be thought of as the top level of the S&MS assurance case, connecting the fundamental S&MS objectives (and Acquirer-levied S&MS-related requirements) to the S&MS success criteria, which comprise the as-yet undeveloped leaf-level claims of the case. With the S&MS success criteria established, S&MS assurance activity can focus sequentially on the

Provider's phase-specific activities, evaluating them against the S&MS success criteria in accordance with the defined LCRs.

Table 1. Elements of S&MS Assurance (Illustrative)

Elements of S&MS Assurance	
S&MS Assurance Element	Comments
Mission S&MS performance is adequately understood	Mission hazards are well understood; the response of the system to hazardous events/faults/failures is well characterized; 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 identified and characterized.
The boundaries and assumptions within which S&MS performance is evaluated are understood	The boundaries and assumptions within which acceptable mission S&MS performance 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.
Effective S&MS-related management processes and controls are in place	The Provider's S&MS-related management processes and controls (e.g., risk management, quality, software assurance, configuration management) are compliant with all levied and agreed-upon S&MS-related process standards; S&MS is managed 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 identify and manage emerging risks (e.g., precursors); processes for post-flight data review and lessons learned are effective; risk acceptance procedures are adequately formalized and technically sound; etc.
Mission S&MS performance meets (or is forecasted to meet) minimum tolerable levels of mission S&MS performance	Assessed S&MS performance provides adequate confidence that minimum tolerable levels of S&MS performance will be met, 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.
Mission safety performance is (or will be) ASARP	System/mission definition decisions have been risk-informed, involving adequate trade studies and the prioritization of safety in decision-making, with documented rationales; plans and processes are in place to ensure future decisions are ASARP.
Mission complies with all Acquirer-levied S&MS-related requirements	Per defined verification protocols.

Table 2 illustrates the kinds of S&MS success criteria that might be defined for a generic set of LCRs associated with a generic project life cycle. These criteria are examples only. In actual application, development of S&MS success criteria would depend on the specific life cycle used, the objectives of each life cycle phase, and the S&MS activities needed to ensure that the phase objectives have been accomplished in a manner consistent with the fundamental S&MS objectives

(and any levied means objectives). They should be high-level enough that they can be specified as part of program/project initialization, recognizing that they may require refinement prior to phase execution based on program/project developments up to that point. In general, S&MS success criteria should focus on Provider efforts to *ensure* adequate S&MS performance, understanding that S&MS ensurance is the proper subject of S&MS assurance. In any case, the success criteria for a given LCR must be baselined prior to executing the activities that are the subject of that LCR.

Table 2. Example S&MS success criteria for a generic project life cycle.

Life Cycle Phase	LCR	S&MS Success Criteria
Concept Development	Mission Concept Review (MCR)	• All at-risk entities (e.g., crew, public, environment, asset, mission objective) have been identified. • Feasible S&MS objectives (e.g., limits on P(LOC), P(LOM), casualty expectation (E_c)) have been defined with respect to each at-risk entity. • The project's risk posture has been established with respect to the S&MS objectives, consistent with the Agency risk posture. • The selected concept(s) is feasible given the mission hazards. • The selected concept(s) is feasible given the technological challenges. • The selected concept(s) is as safe as reasonably practicable (ASARP). • All applicable mandated S&MS-related technical and process requirements have been complied with.
System Design	System Requirements Review (SRR)	• S&MS objectives (e.g., limits on P(LOC), P(LOM), E_c) have been baselined. • The process for allocating requirements into the product breakdown structure (PBS) is valid with respect to the S&MS performance objectives. • The process for allocating requirements into the product breakdown structure (PBS) is valid with respect to the ASARP objective. • The process for addressing S&MS performance in design is adequate with respect to the S&MS objectives. • The process for addressing S&MS performance in design is adequate with respect to the ASARP objective. • All applicable mandated S&MS-related technical and process requirements have been complied with. • All prior corrective actions have been resolved.
	Critical Design Review (CDR)	• The baselined detailed design specifications and operational requirements are valid with respect to the S&MS objectives. • The baselined detailed design specifications and operational requirements are valid with respect to the ASARP objective. • The baselined detailed design specifications and operational procedures include sufficient monitoring, maintenance access, and logistics to adequately sustain S&MS performance. • All applicable mandated S&MS-related technical and process requirements have been 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 sustain S&MS performance during operation. • Quality assurance (QA) processes are consistent with the project's risk posture. • Software development processes are consistent with the project's risk posture. • Software assurance processes are consistent with the project's risk posture. • All applicable mandated S&MS-related technical and process requirements have been complied with. • All prior corrective actions have been resolved.
	System Acceptance Review (SAR)	• The system is compliant with the design specifications. • System performance is deemed valid with respect to the S&MS objectives. • All applicable mandated S&MS-related technical and process requirements have been 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 S&MS performance (e.g., spares, maintenance, anomaly response) are in place. • System operators are trained on mission operations, including contingencies. • All applicable mandated S&MS-related technical and process requirements have been complied with. • All prior corrective actions have been resolved.
Closeout	Disposal Readiness Review (DRR)	• The as-is system is deemed valid with respect to the disposal-related S&MS performance objectives. • System operators are trained on disposal operations, including contingencies. • All applicable mandated S&MS-related technical and process requirements have been complied with. • All prior corrective actions have been resolved.

3.3 The "W-Engine" for S&MS Assurance

Within each life cycle phase, S&MS assurance is focused on meeting the S&MS success criteria defined for the associated LCR(s). The activities associated with S&MS assurance during the phase are codified in the "W-Engine" for S&MS assurance illustrated in Figure 6. These activities can be partitioned into planning, execution, and S&MS risk acceptance.

3.3.1 Planning for the Phase

Each life cycle phase has associated with it the set of S&MS success criteria developed for it at program/project initiation, as discussed in section 3.2. 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 (and validating) any adjustments needed (Box

1), including revision to the associated argument to ensure that the S&MS success criteria remain valid. With the S&MS success criteria baselined, the Provider develops a detailed executable *S&MS plan for the phase* (as part of overall SE planning for the phase) (Box 2A), along with an *S&MS argument for the phase* that validates the plan with respect to the S&MS criteria (i.e., it explains how the S&MS plan addresses the criteria) (Box 2B). This includes specification of the evidence that will be produced to verify that the criteria have indeed been met. The Technical Authorities (TAs) evaluate the S&MS argument for the phase and concur or non-concur on its technical soundness (Box 3), and given an acceptable plan, the Acquirer and Provider negotiate audit, reporting, and/or other provisions relating to Acquirer insight/oversight needs (Box 4).[8] Given satisfaction with these plans among the parties, the Acquirer grants the Provider the authority to execute them (Box 5).

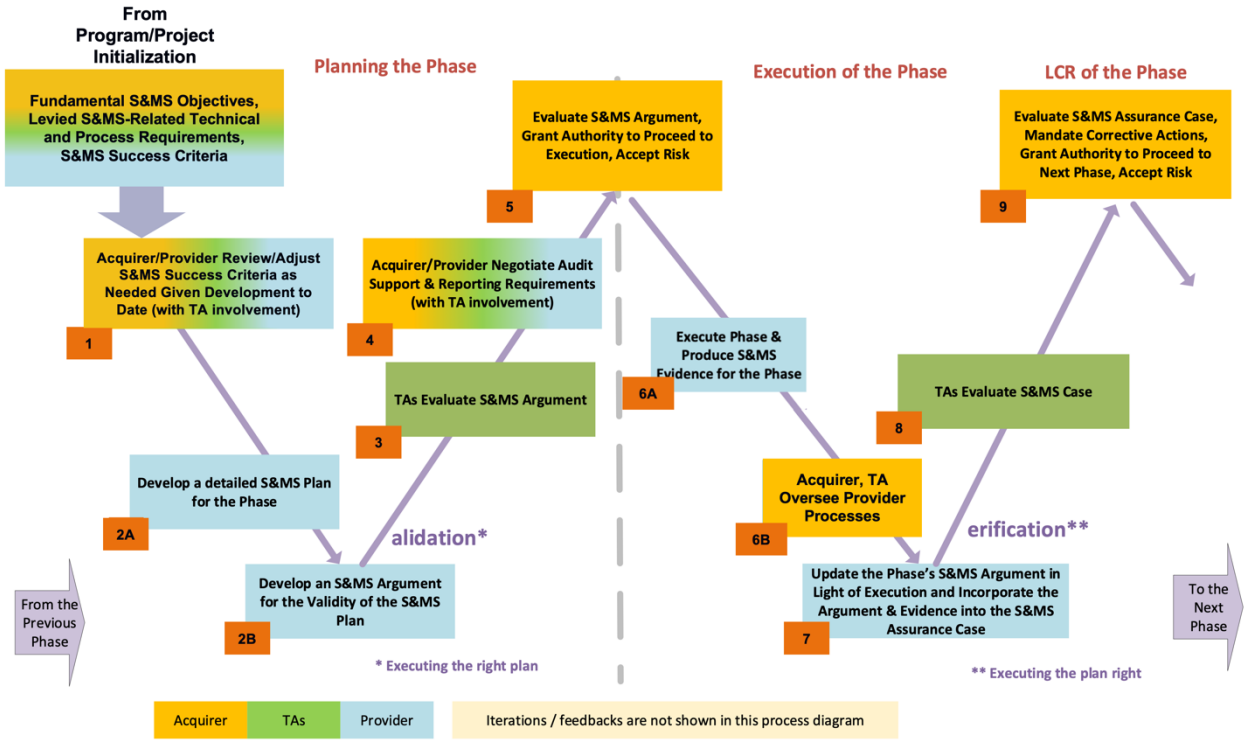

Figure 6. The "W-Engine" for S&MS assurance in a given life cycle phase

3.3.2 Execution of the Phase

The Provider executes the S&MS plan for the phase, producing the agreed-upon S&MS evidence needed to verify that the S&MS success criteria for the phase have been met (Box 6A), overseen by the Acquirer and TAs as agreed (Box 6B). During execution, circumstances can arise that necessitate modifications to the plan, which need to go through the same process of evaluation and approval as the initial plan in order for the plan to remain validated. At the end of the phase, the S&MS assurance case is updated from the previous LCR (if applicable) to address the achievement of the S&MS success criteria of the current phase, using the S&MS argument for the phase that

[8] This includes allowances for *ad hoc* audits and inspections the Acquirer may wish to conduct in response to emerging information (e.g., from Provider reports, ASAP findings, etc.), in addition to any prescribed audits and inspections.

was developed during planning, substantiated by the S&MS evidence that was produced during execution (Box 7).

3.3.3 S&MS Risk Acceptance

The TAs evaluate the S&MS assurance case for technical soundness prior to the LCR (Box 8), after which the Provider submits it to the LCR as the principal S&MS assurance product for the program/project.[9] A nominal S&MS assurance case argues, with evidence, that the S&MS success criteria of the phase have been met.[10] The role of the evaluator (Acquirer, TA, or Standing Review Board (SRB)) is to conduct a structured, critical, and skeptical evaluation, identifying any deficits in the argument or the evidence that either prevent moving forward and/or warrant corrective action. In any case, consistent with the principle of single-signature accountability for risk acceptance emphasized by ASAP [8], each success criterion should be individually accepted by the Acquirer as met. The phase ends with the Acquirer granting the Provider authority to proceed, potentially with mandated corrective actions coming out of the LCR (Box 9).

3.3.4 Closed-Loop Acquirer S&MS Oversight

The "W-Engine" provides for closed-loop oversight by the Acquirer of the Provider's S&MS-related activities by ensuring that the Acquirer has the information needed to evaluate Provider progress, identify any assurance deficits (i.e., deficits in Provider progress towards meeting S&MS objectives and/or deficits in the Provider's case that progress is on track), and issue corrective actions. The main sources of information are 1) S&MS audit findings and Provider reports per Box 4 of Figure 6, and; 2) the S&MS assurance case presented at LCRs. Corrective actions can be issued as part of "in-line" oversight (Box 6B of Figure 6) or issued as a condition for Acquirer acceptance of S&MS risk coming out of an LCR (Box 9 of Figure 6). Other information sources may also be used for oversight, such as reports from ASAP, the Government Accountability Office (GAO), NASA Safety Center (NSC) safety audits, etc. The closed-loop Acquirer oversight inherent in the proposed S&MS assurance framework is illustrated in Figure 7.

3.4 High-Level View of the Proposed S&MS Assurance Framework

Figure 8 presents a high-level view of the proposed S&MS assurance framework for a generic five-phase program/project life cycle.

As discussed in previous sections, the framework begins with the specification, by the Acquirer, of a set of fundamental S&MS objectives, along with a limited set of S&MS-related technical and process requirements the Acquirer considers essential. Then, in light of the generic, essential elements of S&MS assurance, S&MS success criteria are defined for each phase along with an argument for their validity. Within each phase the "W-Engine" operates, with its activities of planning, execution, and S&MS risk acceptance. The S&MS assurance case itself evolves over the life cycle, beginning with the Provider's solution, the S&MS success criteria for the life cycle phases, and the argument for the validity of the S&MS success criteria. Then, as life cycle phases

[9] For illustrative purposes, the "W-Engine" presumes a single LCR at the end of each life cycle phase. However, this is not a hard constraint (see, e.g., [11]). In general, one or more LCRs may be incorporated into a life cycle phase at various points in the phase.

[10] A general concern has been raised that assurance cases are vulnerable to bias; confirmation bias in particular (see, for example, [32]). The proposed S&MS assurance framework addresses this in part by requiring in advance of S&MS plan execution that the S&MS argument validates the plan and that the planned S&MS evidence is sufficient to verify its successful execution. This prevents an S&MS assurance case from being developed *post hoc* in a manner that justifies the results of the phase regardless of what those results are.

are planned and executed, the S&MS assurance case incorporates their S&MS arguments and S&MS evidence, which together provide assurance that the S&MS success criteria have been met. Given the validity of the S&MS success criteria, their satisfaction is grounds for deeming the fundamental S&MS objectives to have been met (or, in the case of an intermediate LCR, deeming the program/project to be on track to meeting them). Throughout, TAs provide concurrences according to their role within NASA's system of institutional checks and balances.

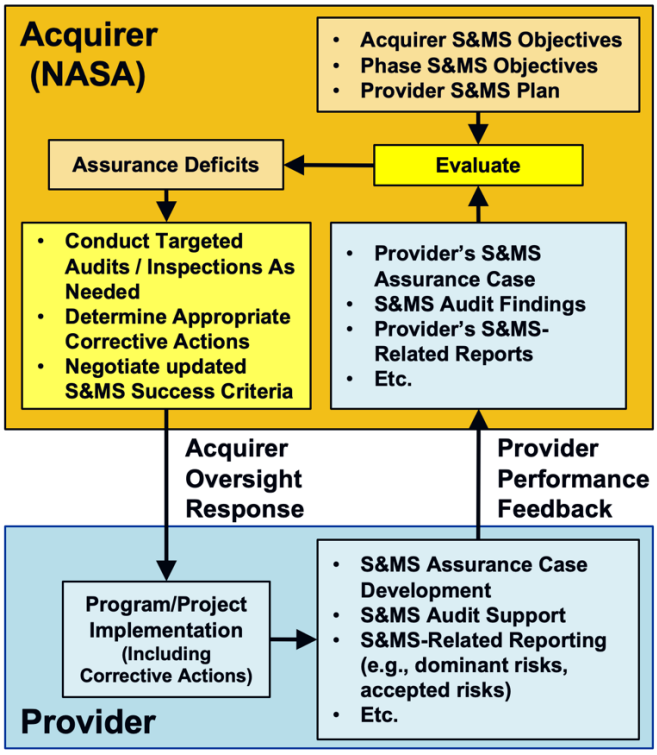

Figure 7. Closed-loop Acquirer S&MS oversight

3.5 Summary of Roles & Responsibilities in the Proposed S&MS Assurance Framework

Table 3 summarizes the roles & responsibilities of the Acquirer, Provider, and independent technical review entities (i.e., TAs and the SRB) in the proposed S&MS assurance framework.

3.6 Special Topics

3.6.1 Ensuring Adequate S&MS Assurance During Acquisition

It is critical to S&MS that the Provider develops and submits a valid S&MS assurance case at each LCR and that the Provider grants the Acquirer access to processes, systems, facilities, personnel, and information that the Acquirer deems necessary for S&MS assurance (e.g., audits). Therefore, Provider commitments to engage in specific S&MS-assurance-related activities (e.g., specific numbers of tests) and to grant specific accesses to the Acquirer should not be finalized except as part of detailed planning (Box 2A of Figure 6). The concern is that premature specification of such activities/access, especially when written into contracts, can run counter to what the Acquirer ultimately needs for S&MS assurance.

This is an area still under development. The S&MS assurance framework must: 1) support acquisition decision-making where S&MS assurance depends on such decisions; 2) be agnostic

with respect to the contractual practices of the Acquirer; 3) not over-constrain the phase-specific planning space in a way that prevents the development of an adequate S&MS assurance case (e.g., due to funding limits that limit testing), and; 4) not over-constrain Acquirer access to the Provider in a way that prevents the Acquirer from developing the insight needed for S&MS assurance (e.g., due to proprietary information).

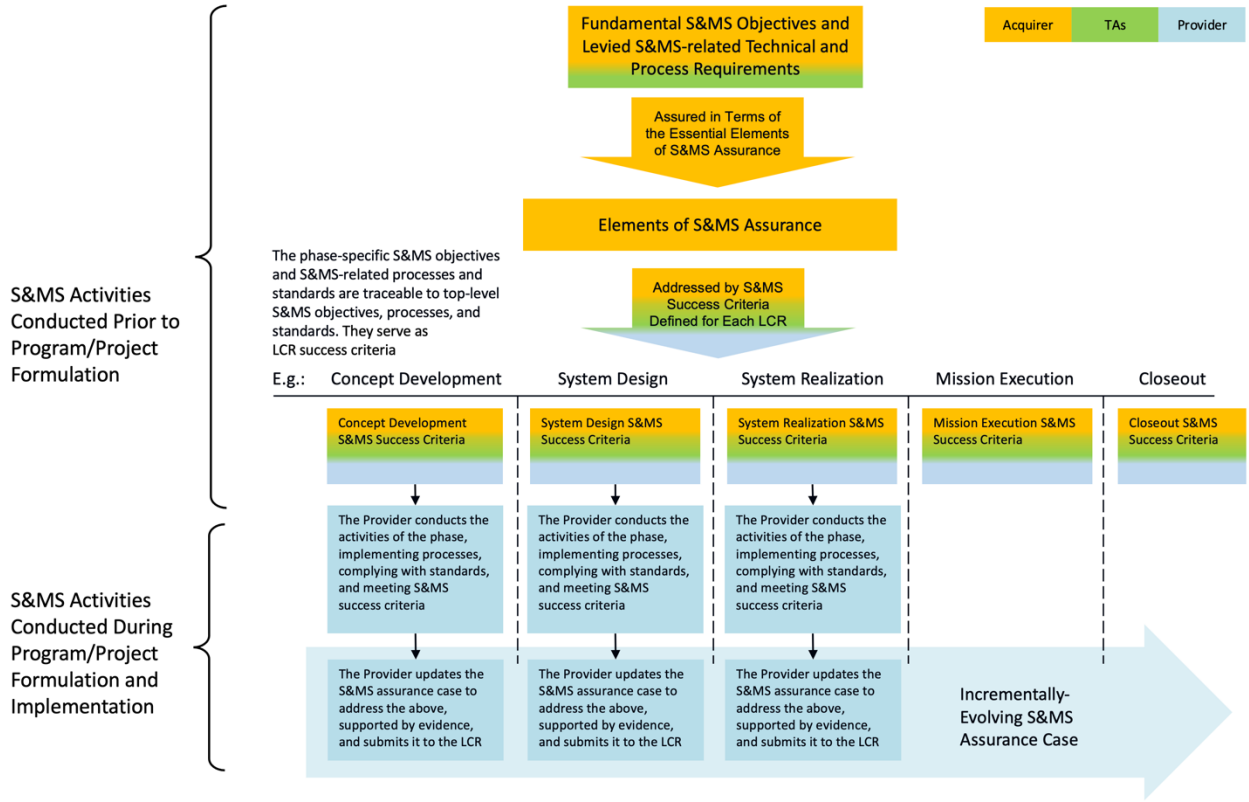

Figure 8. High-level view of the proposed S&MS assurance framework

3.6.2 Human-Rating in the Proposed S&MS Assurance Framework

NPR 8705.2, Human-Rating Requirements for Space Systems, defines a Human-Rated System as one that: 1) accommodates human needs; 2) effectively utilizes human capabilities; 3) controls hazards with sufficient certainty to be considered safe for human operations, and; 4) provides the capability to safely recover the crew from emergency situations. Objectives 3 and 4 are clearly within the scope of S&MS, and as such are implicitly addressed by the proposed S&MS assurance framework. Objective 3 is a fundamental S&MS objective relating to crew safety, and objective 4 is an S&MS-related technical objective mandating a crew recovery capability.

As such, they can be included among the S&MS objectives and reflected in the S&MS success criteria of the applicable LCRs. However, objectives 1 and 2 are not S&MS-related, but instead have more to do with relatively straightforward SE considerations given the human element of the crewed system.[11] They are not "unprovable" in the way that probabilistic objectives such as P(LOC) limits are, and are thus amenable to conventional verification & validation (V&V). In

[11] Objective 1, "Accommodate human needs," is arguably S&MS-related to the extent that life safety depends on a habitable environment, which puts constraints on acceleration, noise, vibration, temperature, atmospheric composition, nourishment, waste disposal, etc.

neither case (objectives 1 and 2 or objectives 3 and 4) is there a need for a separate, parallel assurance process for human rating, nor is there a need for a human rating certification process separate from the LCRs, except perhaps to formally acknowledge that human rating objectives have been factored into the relevant nominal SE and S&MS assurance processes.

Table 3. Summary of roles & responsibilities in the proposed S&MS assurance framework.

Acquirer
• Impose system/mission-level fundamental S&MS objectives on the Provider (e.g., P(LOM), P(LOC) limits, ASARP, HR objectives) • Levy, as deemed necessary, S&MS-related technical and process requirements on the Provider. • Define the systems engineering (SE) model to be used (i.e., life cycle phases, phase SE objectives, and life cycle reviews (LCRs)). • Define, in negotiation with the Provider, S&MS success criteria for each LCR. • Define, in negotiation with the Provider, S&MS-related audit and S&MS-related reporting requirements for each life cycle phase. • Approve, for each life cycle phase, the Provider's S&MS plan for the phase, informed by the Providers S&MS argument for the phase (arguing the validity of the S&MS plan as keeping the Provider on track to meeting the fundamental S&MS objectives (and any levied S&MS-related technical and process requirements)). • Evaluate, at each LCR, the Provider's S&MS assurance case, determine the Provider's standing with respect to the S&MS success criteria of the LCR, and the readiness of the Provider to proceed in the life cycle. • Formally accept the S&MS risk associated with decisions to proceed through the life cycle. • Conduct S&MS audits, inspections, etc., of the Provider, and evaluate Provider reports, as needed to maintain ongoing insight into Provider performance. • Provide oversight in the form of corrective actions, recommendations, etc., based on insights gained via LCRs, audits, reports, etc.
Provider (NASA or non-NASA entity)
• Negotiate, with the Acquirer, S&MS success criteria for each LCR and argue their validity. • Negotiate, with the Acquirer, S&MS-related audit and S&MS-related reporting requirements for each life cycle phase. • Develop, for each life cycle phase, an S&MS plan for the phase that nominally meets the S&MS success criteria of the corresponding LCR, including specification of the S&MS evidence that will verify the S&MS success criteria have been met. • Develop, for each life cycle phase, and S&MS argument for the phase that establishes the validity of the S&MS plan with respect to the S&MS success criteria of the LCR. • Execute the approved S&MS Plans in concert with program/project execution. • At each LCR, submit an S&MS assurance case that argues, with evidence, that the S&MS success criteria have been met (and therefore that the Provider is ready to proceed in the life cycle). • Support Acquirer S&MS audits, inspections, etc., and deliver agreed-upon reports.
Independent Technical Review Entities (NASA entities)
• Act as independent, critical, and skeptical elements of NASA's system of checks and balances. • Concur or non-concur with the achievability of the fundamental S&MS objectives. (TAs) • Concur or non-concur with the validity of the S&MS success criteria. (TAs) • For each life cycle phase, concur or non-concur with the validity of the Provider's S&MS plan. (TAs) • For each life cycle phase, concur or non-concur with the technical adequacy of the S&MS assurance case prior to submittal to the LCR. (TAs) • SRB evaluates the S&MS assurance case at each LCR and presents its findings and recommendations to the Convening Authorities. (SRB)

3.6.3 Campaign-Level and Capability-Centric Objectives

Much of NASA's current planning goes beyond individual missions to address the need for various types of in-space architectures and the development of specific spaceflight capabilities (e.g., Gateway, Human Landing System (HLS)). The proposed S&MS assurance framework is well suited to address the issue of adequate S&MS performance beyond the mission level. The objectives-driven approach to S&MS-related requirements has the flexibility and agility to adapt to campaign-level objectives and to general capabilities that are not necessarily defined in the context of any reference mission. Applying the framework would entail the Acquirer associating a fundamental S&MS objective with each objective/capability, expressing stakeholder expectations regarding the likelihood that the desired objective/capability will be achieved.

4 Standards-Based Implementation of the Proposed S&MS Assurance Framework

4.1 The Motivation for a Standards-Based Approach to S&MS Assurance Framework Implementation

NASA's new acquisition model makes essential use of contractors in a manner that is different from the use of contractors during earlier programs such as the Shuttle. Contractors were involved in the Shuttle program, but in earlier programs, NASA had closer control over activities than NASA will have in the future; the new acquisition model is different. A traditional way for NASA to manage what it is getting from its in-house Providers is to levy requirements via NPRs, but NASA cannot levy NPRs on non-NASA entities. However, NASA can fulfill its assurance responsibilities by contractually requiring compliance with Standards, either existing ones or newly developed ones. The S&MS Assurance Standard is intended to support that approach for S&MS.

4.2 The Standard for Assurance of Safety and Mission Success

OSMA is in the process of developing a *Standard for Assurance of Safety and Mission Success* (i.e., the S&MS Assurance Standard) [1] that implements the proposed S&MS assurance framework of Section 3 above. Much of the discussion in this white paper is also contained in this standard, along with the requirements needed to implement each of the framework elements identified in Figures 6 and 8, with each box in Figure 8 covered by a distinct requirement. The S&MS Assurance Standard is a process standard, as opposed to a technical standard, in that its requirements pertain to the process by which S&MS is assured, and does not contain any requirements specifying what level of S&MS performance is required or how that level of performance is to be achieved.

4.3 Supporting S&MS-Related Standards, Handbooks, etc.

In the proposed S&MS assurance framework, technical and process requirements are not unilaterally levied on the Provider (with the possible exception of some limited number of essential requirements, as discussed in Section 2). Instead, as shown on the right-hand side of Figure 3, the Acquirer gives the Provider a set of fundamental S&MS objectives, and it is up to the Provider (with appropriate concurrences and the Acquirer's approval) to commit to some set of technical and process requirements in the S&MS plan that are consistent with the Provider's solution and give the Acquirer confidence that the fundamental S&MS objectives will be met. These requirements are expected to span the entirety of S&MS-related disciplines, such as orbital debris, payload safety, planetary protection, quality, reliability and maintainability, software assurance,

and system safety. Technical and/or process standards, handbooks, and other sources of good S&MS-related practice in these disciplines are vital resources from which the Provider may draw, as illustrated in Figure 9. These can include not only NASA standards but also industry consensus standards that are applicable to the Provider's solution and approved by the Acquirer, consistent with NPR 7120.10A, which states that the selection of technical standards necessary to promote mission success and engineering excellence shall prioritize voluntary consensus standards over NASA or other government agency standards, unless inconsistent, inadequate, or impractical [33]. Standards may be accepted in their entirety, in part, or as modified to apply to the Provider's potentially novel solution.

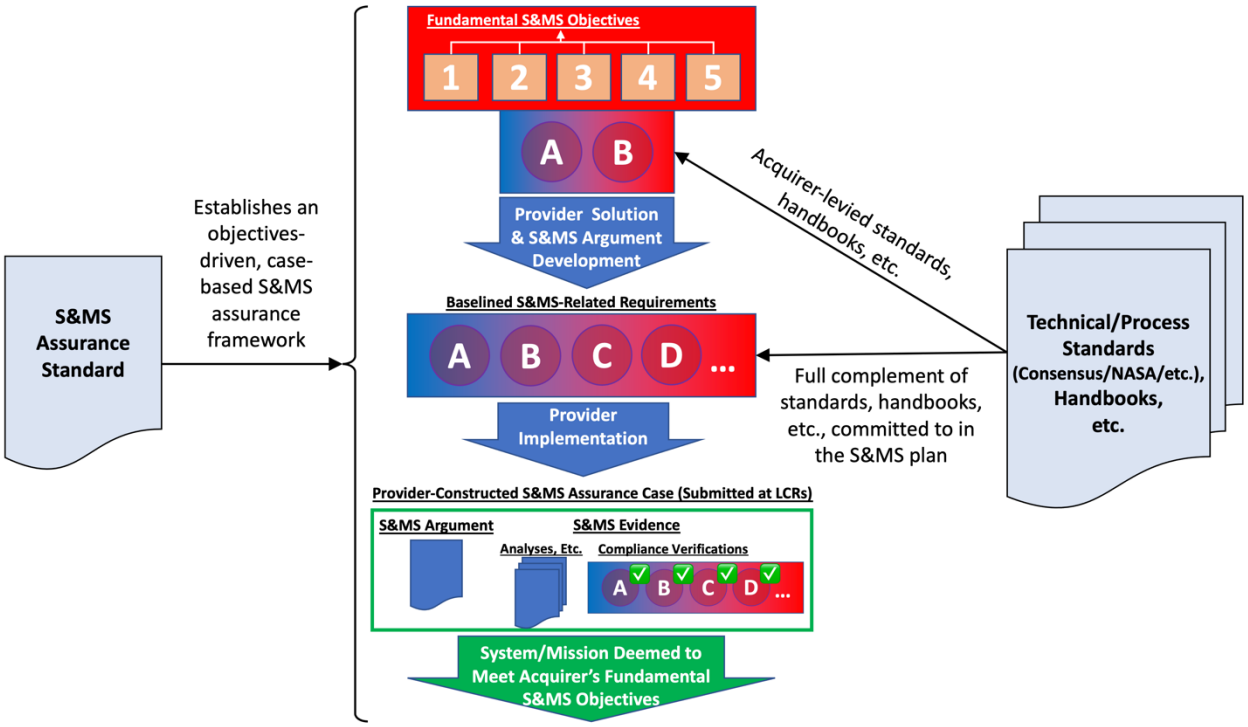

Figure 9. The role of technical and process standards, handbooks, etc., in the proposed S&MS assurance framework

The main characteristic of the proposed S&MS assurance framework with respect to the application of standards, handbooks, etc., is that their selection is derived from the fundamental S&MS objectives. This is in contrast to the situation where standards are levied on spaceflight programs/projects as a matter of Agency procedure, possibly years before the program/project is conceived and without due regard for advances in SE or acquisition practice that may have occurred in the meantime.

4.4 The S&MS Analysis Management Standard

OSMA is in the process of developing a *Safety and Mission Success Analysis Management Standard* [2] that is consistent with the objectives-driven, case-based framework of the S&MS assurance standard. It does not require the conduct of S&MS analysis, nor does it prescribe any particular S&MS analysis techniques. Instead, it focuses on requiring the Provider to: 1) derive the need for S&MS analysis from the Provider's plans for meeting the (LCR-specific) S&MS success criteria; 2) include S&MS analysis plans in the S&MS plan required by the S&MS assurance standard; 3) subject S&MS analyses to independent technical review; 4) document S&MS analyses

in a manner that supports the Acquirer's assurance needs; and 5) incorporate S&MS analyses into the S&MS assurance case as S&MS evidence. In essence, it continues the S&MS assurance standard's theme of *objectives-driven and case-based*, but specialized to S&MS analysis and drilling down to a higher level of detail.

Figure 10 illustrates how S&MS analyses might be conducted to support the S&MS success criteria of Table 2, in which case the analyses would be incorporated into the evolving S&MS assurance case as S&MS evidence. For example, the S&MS assurance case presented at MCR would be expected to argue the claim that "*The selected concept(s) is as safe as reasonably practicable (ASARP)*." The argument might involve a claim that all reasonable alternatives were analyzed. The main evidence for this would be the S&MS analysis of the alternatives, as highlighted in red in the MCR block of Figure 10. The nature of the analysis itself would have been agreed to with the approval by the Acquirer of the Provider's S&MS plan. That plan might have committed to the use of certain S&MS-analysis-related standards, handbooks, etc., such as [34] or [35].

Table X. Examples of LCR-specific SMS evidence (notional)

Life Cycle Phase	LCR	LCR-Specific SMS Evidence
Concept Development	MCR	• List of all at-risk entities (e.g., crew, public, environment, asset, mission objective) • List of SMS performance objectives (e.g., limits on P(LOC), P(LOM), casualty expectation (E_c)) for each at-risk entity. • The project's risk posture • Analyses of alternative mission concepts, at the level of feasibility, hazard identification/manageability, and technology gaps • Rationale for the selection of mission concept (e.g., RISR per the NASA RIDM Handbook)
System Design	SRR	• SMS performance objectives (e.g., limits on P(LOC), P(LOM), E_c) • The process for allocating requirements into the product breakdown structure (PBS) from the SMS performance objectives • The SMS analysis plan
	CDR	• The baselined detailed design specifications and operational requirements • Traceability matrices from Acquirer SMS objectives to baselined design specifications and operational requirements • SMS analysis of the baselined DRM, including contingencies • Monitoring and instrumentation trade studies • Maintenance analyses • Logistics analyses
System Realization	PRR	• Production process quality requirements • Production process descriptions • 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 • SMS analysis of the as-is system with respect to mission SMS objectives
Mission Execution	MRR	• System status • Mission support status • Training records/certifications
Closeout	DRR	• System condition/status reports • SMS analysis with respect to the disposal-related SMS performance objectives. • Disposal-related training records/certifications

Figure 10. Notional illustration of S&MS analyses as evidence in the S&MS assurance case

4.5 Retirement of NPR 8705.5 and NPR 8715.3 Chapter 2

One current example of the move away from prescriptive, Agency-mandated S&MS-related requirements is the planned retirement of NPR 8705.5 [3] and Chapter 2 of NPR 8715.3 [4]. A primary motivation for their retirement is the move away from unilaterally requiring PRA for Priority I projects in light of, among other things, the emergence of alternative methods such as simulation that are replacing traditional PRA as the "gold standard" of S&MS analysis. These types of blanket requirements are inconsistent with the proposed S&MS assurance framework, as discussed previously, and it is appropriate to retire them if the framework is to be adopted.

Nevertheless, as a matter of due diligence, the retirement of Agency requirements should be done judiciously and in a documented manner in order to ensure that important requirements are not inadvertently disposed of. Broadly speaking, the requirements at issue fall into the following for categories: 1) requirements relating to what types of programs/projects are required to perform what types of S&MS analyses (e.g., PRA for Priority I programs/projects); 2) requirements relating to S&MS-related planning and approval; 3) requirements relating to independent evaluation; and 3) "how to" requirements relating to acceptable S&MS analysis execution. In an objectives-driven

approach to S&MS, category 1 is moot, since the need for S&MS analysis is derived from the fundamental S&MS objectives and S&MS success criteria. Categories 2 and 3 are covered by the planning and independent evaluation elements of the proposed S&MS assurance framework, as discussed previously and illustrated in Figures 6 and 8. Category 4 is best addressed by S&MS-related standards, handbooks, etc., that are available for adoption by the Provider as commitments in the S&MS plan. To ensure traceable and reviewable disposition of the requirements of [3] and [4] in terms of the extent to which they are either accommodated in [1] and [2] or found inconsistent, a requirements disposition activity for these two NPRs is being conducted as part of the development of the two standards.

4.6 Status and Next Steps

Initial drafts of the S&MS Assurance Standard and the S&MS analysis management standard are nearing completion. It is desirable for the draft standards to have the benefit of participation from a range of S&MS domain subject matter experts (SMEs) in areas such as orbital debris, payload safety, planetary protection, quality, reliability and maintainability, and software assurance. In particular, the S&MS assurance standard would benefit from SME input on illustrative LCR-specific S&MS success criteria and S&MS evidence that can be provided as guidance. Therefore, OSMA's near-term plan is to "socialize" the draft standards among the relevant stakeholders and incorporate their feedback into revised draft standards that can be brought forward for further development. This white paper is part of that socialization effort.

5 References

1. NASA OSMA, *Standard for Assurance of Safety and Mission Success (draft)*, Washington, DC. August 2021.
2. NASA OSMA, *Safety and Mission Success Analysis Management Standard (draft)*, Washington, DC. August 2021.
3. NASA, *Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects*, NPR 8705.5A, Washington, DC. June 2010.
4. NASA, *NASA General Safety Program Requirements*, NPR 8715.3D, Washington, DC. August 2017.
5. NASA System Safety Steering Group (S3G), "Position Paper: A Vision for System Safety," NASA, Washington, DC. September 2013.
6. ASAP, *Aerospace Safety Advisory Panel Annual Report for 2009*, Washington, DC. 2010.
7. ASAP, *Aerospace Safety Advisory Panel Annual Report for 2013*, Washington, DC. 2014.
8. ASAP, *Aerospace Safety Advisory Panel Annual Report for 2014*, Washington, DC. 2015.
9. ASAP, *Aerospace Safety Advisory Panel Annual Report for 2018*, Washington, DC. 2019.
10. ASAP, *Aerospace Safety Advisory Panel Annual Report for 2020*, Washington, DC. 2021.
11. NASA, *NASA Space Flight Program and Project Management Requirements*, NPR 7120.5E, Washington, DC. August 2012.
12. NASA OSMA, "Model-Based Mission Assurance," NASA, https://sma.nasa.gov/sma-disciplines/model-based-mission-assurance.
13. NASA, *NASA Governance and Strategic Management Handbook*, NPD 1000.0C, Washington, DC. January 2020.
14. NASA OSMA, "Safety & Mission Success – Capability Assessment and Assurance Assessment Process," NASA, Washington, DC. October 2019.
15. NASA OSMA, "Recommended Updates to NASA Directives and Guidance to Clarify Technical Authority for Greatest Optimization," NASA, Washington, DC. November 2019.
16. NASA, *NASA System Safety Handbook, Volume 1: System Safety Framework and Concepts for Implementation*, NASA/SP-2010-580, NASA, Washington, DC. November 2011.
17. NASA, *NASA System Safety Handbook, Volume 2: System Safety Concepts, Guidelines, and Implementation Examples*, NASA/SP-2014-612, NASA, Washington, DC. November 2014.

18. NASA System Safety Steering Group (S3G), "The Role of NASA Safety Thresholds and Goals in Achieving Adequate Safety," NASA, Washington, DC. June 2012.

19. NASA OSMA, "Towards an Integrated Safety & Mission Success Framework," NASA, Washington, DC. November 2015.

20. NASA OSMA, "A Safety-Case-Based Approach to SMA Technical Authority (TA) Evaluation of Human-Rating Certification Packages (HRCPs)," NASA, Washington, DC. June 2017.

21. NASA, *NASA Reliability and Maintainability (R&M) Standard for Spaceflight and Support Systems*, NASA-STD-8729.1A, NASA, Washington, DC. June 2017.

22. NASA OSMA, "OSMA Introduces New Objectives-Based Strategies," NASA, https://sma.nasa.gov, Washington, DC. December 2014.

23. Trump, D., "Space Policy Directive-2, Streamlining Regulations on Commercial Use of Space," Presidential Memorandum, Washington, DC. May 2018.

24. Code of Federal Regulations (CFR), "Launch and Reentry License Requirements," 14 CFR 450, Washington, DC. December 2020.

25. Kelly, T., Weaver, R., "The Goal Structuring Notation – A Safety Argument Notation," University of York, UK. 2008.

26. Adelard, "CAE Framework," https://claimsargumentsevidence.org, UK.

27. ISO/IEC, *Systems and Software Engineering – Systems and Software Assurance*, ISO/IEC 15026, January 2013.

28. Dezfuli, H., Youngblood, R., *et al*, "Technical Resources Available for Development of a Prototype SMS Assurance Standard," NASA, Washington, DC. November 2020.

29. Federal Register, "Streamlined Launch and Reentry License Requirements," FAA, Washington, DC. December 2020.

30. Trump, D., "Presidential Memorandum on Launch of Spacecraft Containing Space Nuclear Systems," Presidential Memorandum, Washington, DC. August 2019.

31. NASA, *NASA Systems Engineering Processes and Requirements*, NPR 7123.1C, Washington, DC. February 2020.

32. Leveson, N., "The Use of Safety Cases in Certification and Regulation," MIT, Cambridge, MA. November 2011.

33. NASA, *Technical Standards for NASA Programs and Projects*, NPR 7120.10A, Washington, DC. February 2017.

34. Leveson, N., Thomas, J., *STPA Handbook*, MIT, Cambridge, MA. March 2018.

35. NASA, *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*, NASA/SP-2011-3421, Washington, DC. 2011.

6 Definitions

Acquirer	A NASA organization that tasks another organization (either within NASA or external to NASA) to produce a system or deliver a service.
Provider	A NASA or contractor organization that is tasked by an accountable organization (i.e., the Acquirer) to produce a product or service.
Mission Goals	The fundamental reasons for undertaking a particular mission.
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.
Safety and Mission Success (S&MS)	S&MS is the coordinated pursuit of Mission Goals and Safety in a manner that achieves the proper balance between them, and is consistent with the Agency's risk posture and its obligations to its stakeholders.
Fundamental Mission Objectives	The mission goals, expressed as mission technical objectives, and the protection of at-risk entities from adverse mission consequences.
S&MS Performance	The likelihood that Mission Goals will be accomplished, and the likelihood that at-risk entities (people, assets, terrestrial environment, extraterrestrial environments, …) will not be adversely affected.
Fundamental S&MS Objectives	Fundamental expectations regarding S&MS performance. Such expectations can take the form of lower limits on S&MS performance or on the maximization of S&MS performance insofar as is practicable (e.g., that the mission is as safe as reasonably practicable (ASARP)).
Means Objectives	Objectives that indicate a particular way of accomplishing a higher-level objective. Strategies for accomplishing fundamental mission objectives are expressed at means objectives.
S&MS Success Criteria	LCR-specific accomplishments that need to be satisfactorily demonstrated to show that the Provider has met or is on track to meeting the fundamental S&MS objectives, as well as any levied S&MS-related technical and process requirements, so that a technical effort can progress further in the life-cycle.
S&MS Assurance	Grounds for justified confidence that the program/project has met, or is on track to meeting, its fundamental S&MS objectives (and any Acquirer-levied S&MS-related technical or process requirements).
S&MS Assurance Case	A compelling, comprehensible and valid argument, supported by evidence, that a Provider has met, or is on track to meeting, the fundamental S&MS objectives (and any Acquirer-levied S&MS-related technical or process requirements).
S&MS Ensurance	Program/project activities done for the purpose of achieving levels of mission S&MS performance that meet the mission's fundamental S&MS objectives (and any Acquirer-levied S&MS-related technical or process requirements).