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

Chris Everett[a], Homayoon Dezfuli[b], Bob Youngblood[c]
[a] Idaho National Laboratory, Idaho Falls, ID, USA, *henry.everett@inl.gov*
[b] NASA, Washington, DC, USA, *hdezfuli@nasa.gov*
[c] Idaho National Laboratory, Idaho Falls, ID, USA, *robert.youngblood@inl.gov*

Abstract: A need to evolve NASA's safety and mission success (S&MS) assurance framework has emerged in recent years, resulting from the need to accommodate new acquisition models, particularly commercial transportation services; the need to accommodate evolving systems engineering practices; the need to stipulate acceptable levels of S&MS risk; the need for improved integration of S&MS into systems engineering; and the need for clearer risk acceptance accountability. The objectives-driven, case-assured S&MS assurance framework proposed here is responsive to that need. It is structured in terms of a "W-Engine" for S&MS assurance, in which, for each life cycle phase, S&MS success criteria are defined and validated; S&MS plans for meeting the success criteria are developed; the S&MS plan is executed; and an evolving S&MS assurance case is submitted to the LCR(s). This proposed S&MS assurance framework is notable for its lack of prescription of traditional S&MS strategies such as defined failure tolerances, margins, or analysis requirements. Instead, Providers are given latitude to propose their own strategies for meeting the S&MS performance objectives, subject to independent review and Acquirer approval. The result is a framework for S&MS assurance that is at once both rigorous and flexible.

Keywords: Safety & Mission Success, Objectives-Driven, Assurance Case

1. INTRODUCTION

This paper is a condensed version of a white paper of the same title prepared for the NASA Office of Safety and Mission Assurance (OSMA) [1]. A need to evolve NASA's safety and mission success (S&MS) assurance framework has emerged in recent years, resulting from the need to accommodate new acquisition models, particularly commercial transportation services; the need to accommodate evolving systems engineering practices; the need to stipulate acceptable levels of S&MS risk; the need for improved integration of S&MS into systems engineering; and the need for clearer accountability. The objectives-driven, case-assured S&MS assurance framework proposed here is responsive to that need. It is objectives-driven in that a Provider's[1] S&MS activities must derive from explicitly established objectives for S&MS performance (defined as the likelihoods that mission technical requirements will be accomplished, and the likelihoods that at-risk entities will not be adversely affected). It is case-assured in that the adequacy of the Provider's S&MS activities must be argued by the Provider in an S&MS assurance case that is submitted to the Acquirer at program life cycle reviews (LCRs). The framework itself is structured in terms of a "W-Engine" for S&MS assurance, in which, for each life cycle phase, S&MS success criteria are defined and validated; S&MS plans for meeting the success criteria are developed; the S&MS plan is executed; and an evolving S&MS assurance case is submitted to the LCR(s). This proposed S&MS assurance framework is

[1] Provider is a NASA or contractor organization that is tasked by a NASA Acquirer to produce a product or service.

notable for its lack of prescription of traditional S&MS requirements and strategies such as defined failure tolerances, margins, or analysis requirements. Instead, Providers are given latitude to propose their own strategies for meeting the S&MS performance objectives, subject to independent review and Acquirer approval. The result is a framework for S&MS assurance that is at once both rigorous and flexible.

2. ESTABLISHING FUNDAMENTAL S&MS OBJECTIVES

2.1. Protection of At-Risk Entities

NPR 8715.3D [2] 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 1 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.

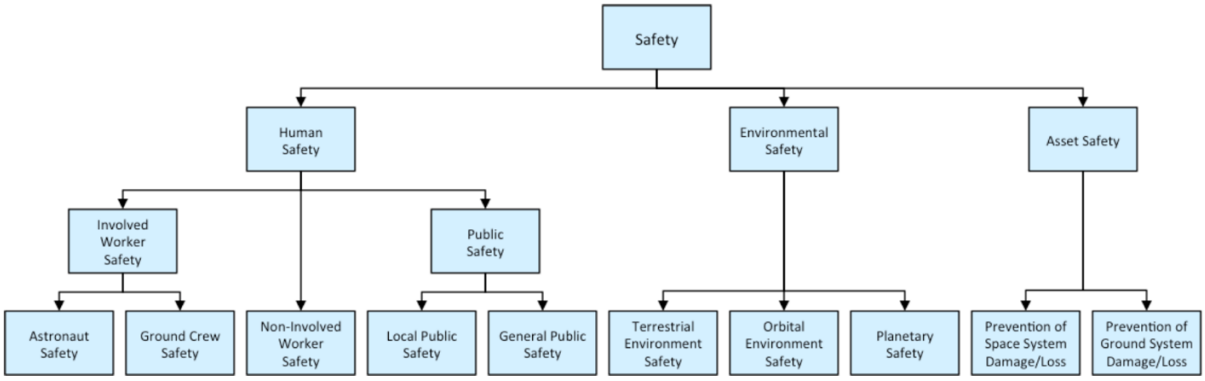

Figure 1. A Generic Safety Taxonomy

2.2. 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.

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 as previous missions of the same type" reflecting a continuing tolerance of the level of safety that had already been tolerated in prior missions. The argument that it has been met might then take the form of arguing that the safety performance at issue had been improved relative to prior missions, without necessarily having to know quantitatively what it is (nor what it was in prior missions).

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 a fatality risk criterion 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 [3]. 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.

2.3. Addressing ASARP

In addition to meeting minimum tolerable levels of safety, adequate safety also consists of being as safe as reasonably practicable (ASARP). The ASARP objective reflects NASA's ethical obligation to increase safety insofar as is practicable, beyond the minimum tolerable levels. Being ASARP entails a continuous, proactive search for safety improvements, along with the prioritization of safety in decision-making, within limits of practicality.

It is a matter of judgement as to what constitutes practicality, and therefore what constitutes being ASARP, but an argument can be made that a necessary minimum condition of being ASARP is adherence to applicable established good system safety and safety management practices, with the caveat that the Provider be afforded the opportunity to employ other means of meeting the intent of established practice, subject to independent review and Acquirer evaluation and approval.

Established practice is typically captured in consensus technical and process standards, which are often focused on very specific details of design, manufacture, analysis, management, operation, etc., of space flight systems.

2.4. 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 is given to each. Figure 2 presents a generic mission technical objectives taxonomy, showing prime, extended, and contingency objectives.[2]

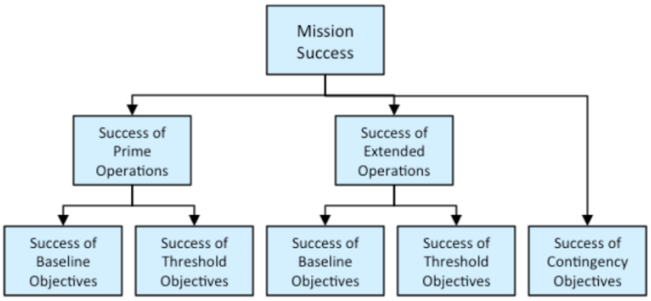

Figure 2. A Generic Mission Objectives Taxonomy

3. AUGMENTING WITH PRESCRIPTIVE S&MS-RELATED TECHNICAL AND PROCESS REQUIREMENTS

The Acquirer may mandate specific S&MS-related processes and standards for the nascent program/project, such as for risk management, quality assurance, software safety, orbital debris, etc. As a general rule, consistent with an objectives-driven approach to S&MS, such specifications should be kept to a minimum, with the understanding that they are all merely *means* to meeting the fundamental S&MS objectives and are not themselves fundamental. They should only be levied when they are considered absolutely necessary for acceptable S&MS performance, including being ASARP. A requirement for a mission abort system might fall into this category.

[2] 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.

4. DEFINING ADEQUATE PROGRESS TOWARDS MEETING THE FUNDAMENTAL S&MS OBJECTIVES

NPR 7120.5F [4] 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 fundamental S&MS objectives, by conducting LCRs that provide a periodic assessment of its technical and programmatic status and health. Example success criteria for these LCRs are provided in NPR 7123.1C [5].

The S&MS assurance framework recognizes that new acquisition paradigms may go beyond the prescribed life cycles and LCRs in NPR 7120.5F but also recognizes the need for the Acquirer to periodically assure itself that the Provider is on track to meet 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 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). The S&MS success criteria must address the adequacy of all aspects of the Provider's effort upon which S&MS performance significantly depends. This includes not only technical attributes of the mission and its systems, but also Provider processes, capabilities, and organizational factors insofar as they affect S&MS. Table 1 illustrates one possible decomposition of S&MS assurance into a set of high-level claims that address a broad range of factors having the potential to affect S&MS performance, including so-called "soft" factors relating to Provider organization and management. These factors manifest differently in different life cycle phases and at different LCRs but in general provide a foundation for defining valid S&MS success criteria. They also provide a rational basis 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 claims about which an Acquirer may wish to be assured in order to have confidence that all important factors are addressed. The main point is that the Acquirer must have a well-developed and valid rationale for being assured of adequate S&MS performance given the satisfaction of the S&MS success criteria. The illustrative claims in Table 1 represent a high-level 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 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 1: S&MS Assurance Claims (Illustrative)

Illustrative S&MS Assurance Claims	
S&MS Assurance Claim	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, including the potential for unknown and/or underappreciated sources of S&MS risk (e.g., due to novelty or complexity).
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. These collectively define a "normalcy map" within which S&MS performance is adequately understood and deemed acceptable.
Effective S&MS-related management processes and controls are in place	The Provider's S&MS-related management processes and controls (risk management, quality, software assurance, configuration management, etc.) are compliant with all levied and agreed-upon S&MS-related process standards; S&MS is managed proactively and holistically as an integrated part of a management system that includes other mission execution domains (e.g., cost, schedule); audits and reports indicate a robust safety culture; systems are in place to effectively monitor performance, including leading indicators, and identify and manage emerging risks (e.g., via precursor analysis); processes for post-flight data review and lessons learned are effective; risk acceptance procedures are adequately formalized and technically sound; etc. Effective S&MS-related management processes and controls maintain the system within its normalcy map throughout the program/project life cycle.
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: Illustrative 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.

5. 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 3. These activities can be partitioned into planning, execution, and S&MS risk acceptance.

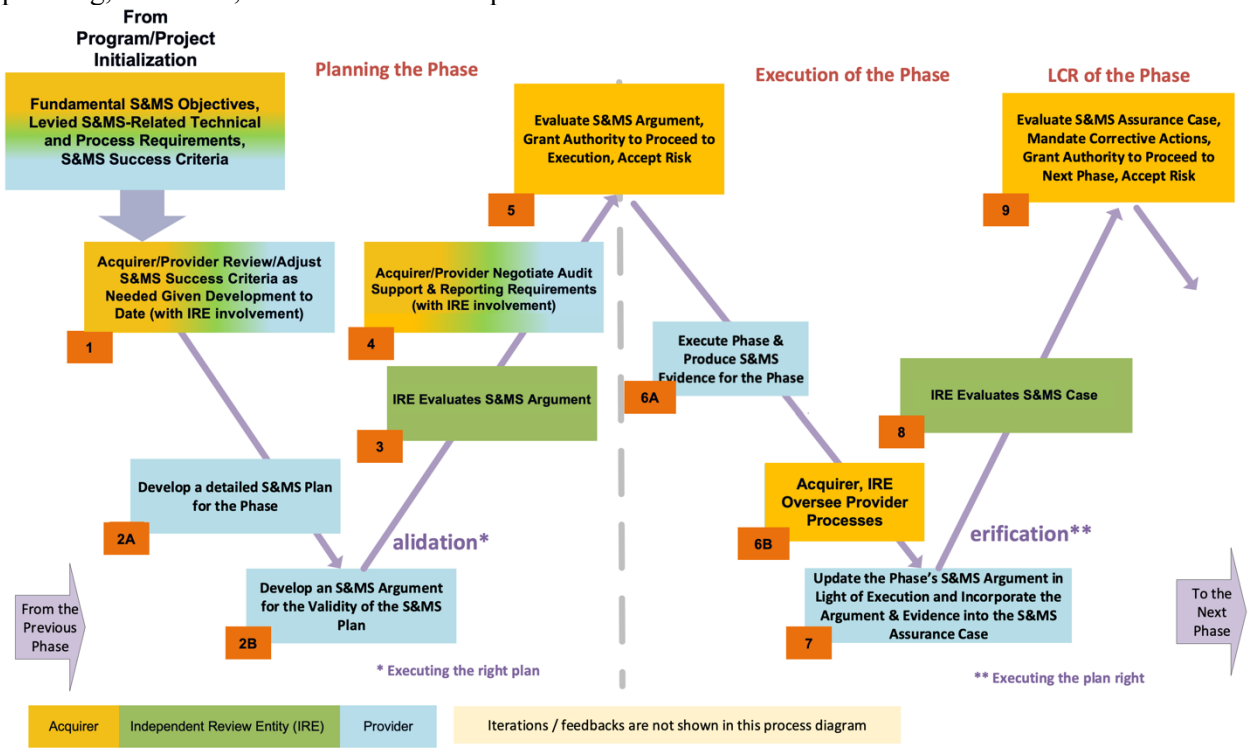

Figure 3. The "W-Engine" for S&MS Assurance in Each Life Cycle Phase

5.1. 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 4. 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. Table 3 illustrates the types of S&MS evidence that might be incorporated into the S&MS assurance case for a program/project life cycle having the S&MS success criteria presented in Table 2.

Table 3: Illustrative Examples of S&MS Evidence

Life Cycle Phase	LCR	LCR-Specific S&MS Evidence
Concept Development	MCR	• List of all at-risk entities (e.g., crew, public, environment, asset, mission objective) • List of S&MS 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	• S&MS 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 S&MS performance objectives • The S&MS analysis plan.
	CDR	• The baselined detailed design specifications and operational requirements • Traceability matrices from Acquirer S&MS objectives to baselined design specifications and operational requirements • S&MS analysis of the baselined design reference mission, 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 • S&MS analysis of the as-is system with respect to mission S&MS objectives.
Mission Execution	MRR	• System status • Mission support status • Training records/certifications.
Closeout	DRR	• System condition/status reports • S&MS analysis with respect to the disposal-related S&MS performance objectives. • Disposal-related training records/certifications.

An Independent Review Entity (IRE) evaluates the S&MS argument for the phase and concurs or non-concurs on its technical soundness (Box 3). Given an acceptable plan, the Acquirer and Provider negotiate audit, reporting, and/or other provisions relating to Acquirer insight/oversight needs (Box 4). 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, Aerospace Safety Advisory Panel (ASAP) findings) in addition to any prescribed audits and inspections. In general, reporting provisions should focus on leading indicators of potentially deteriorating S&MS-related performance. Given satisfaction with these plans among the parties, the Acquirer grants the Provider the authority to execute them (Box 5).

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

5.3. S&MS Risk Acceptance

The IRE evaluates 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.[3] A nominal S&MS assurance case argues, with evidence, that the S&MS success criteria of the phase have been met.[4] The role of the evaluator (Acquirer, IRE, or Standing Review Board) 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 [7], 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).

5.4. Support for Closed-Loop Acquirer S&MS Oversight

The "W-Engine" supports 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 3, and; 2) the S&MS assurance case

[3] 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, for example, [4]). In general, one or more LCRs may be incorporated into a life cycle phase at various points in the phase.

[4] A general concern has been raised that assurance cases are vulnerable to bias; particularly confirmation bias (see, for example, [6]). The 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.

presented at LCRs. Corrective actions can be issued as part of "in-line" oversight (Box 6B of Figure 3) or issued as a condition for Acquirer acceptance of S&MS risk coming out of an LCR (Box 9 of Figure 3). Other information sources may also be used for oversight, such as reports from ASAP, the Government Accountability Office (GAO), other NASA audits, etc. The support for closed-loop Acquirer oversight provided by the S&MS assurance framework is illustrated in Figure 4.

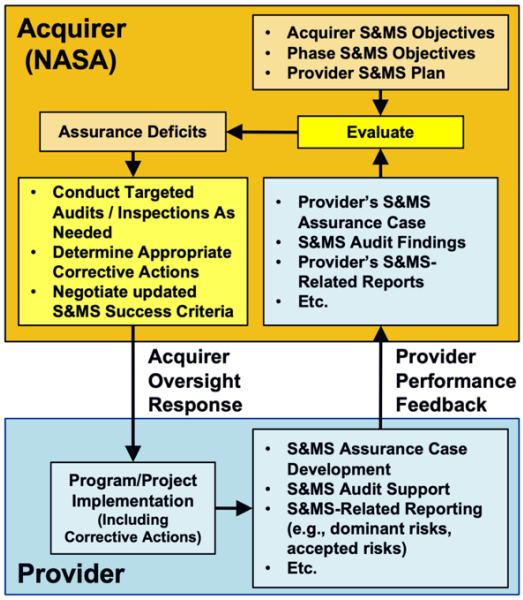

Figure 4. Closed-Loop Acquirer S&MS Oversight

6. STANDARDS-BASED IMPLEMENTATION OF THE PROPOSED S&MS ASSURANCE FRAMEWORK

The proposed S&MS assurance framework could be implemented via an S&MS Assurance Standard. Such a standard would not unilaterally levy technical and process requirements on the Provider (with the possible exception of some limited number of essential requirements, as discussed in Section 3). Instead, the standard would specify that the Acquirer levy on the Provider a set of fundamental S&MS objectives, and it would be 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 adequate confidence that the fundamental S&MS objectives will be met. These requirements would be 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 would be vital resources from which the Provider could draw, as illustrated in Figure 5. These could 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 [8]. Standards could be accepted in their entirety, in part, or as modified to apply to the Provider's potentially novel solution.

The main characteristic of the 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 contrasts with 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.

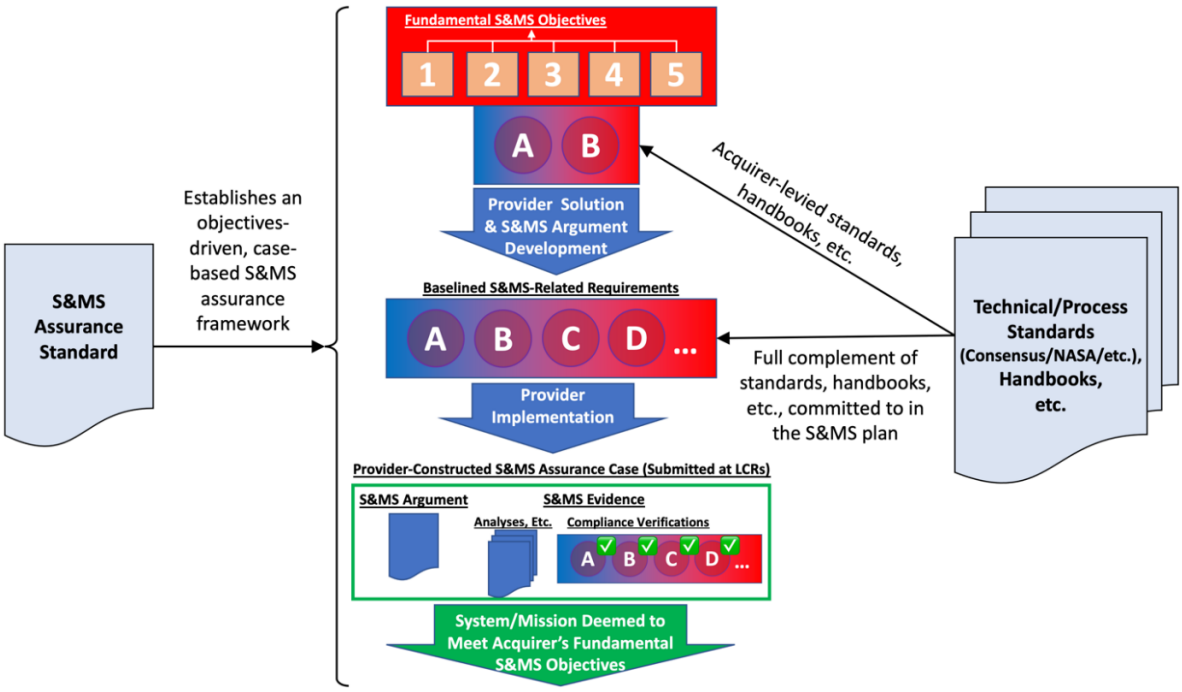

Figure 5. The Role of Technical and Process Standards, Handbooks, Etc., in the S&MS Assurance Framework

7. HIGH-LEVEL VIEW OF THE S&MS ASSURANCE FRAMEWORK

Figure 6 presents a high-level view of the 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, considering 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 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, the IRE provides concurrences.

8. CONCLUSION

The S&MS assurance framework proposed in this paper is responsive to the evolving conditions of NASA's acquisition, systems engineering, and risk management environments. Moreover, it provides the flexibility and agility to accommodate continued evolution in these domains into the future. The objectives-driven and case-assured engineering development and management paradigm is increasingly becoming the norm across a wide variety of industries both domestically and internationally as its benefits become evident. The authors believe that the adoption of an objectives-driven, case-assured approach to S&MS at NASA should be an integral part of the Agency's overall evolution.

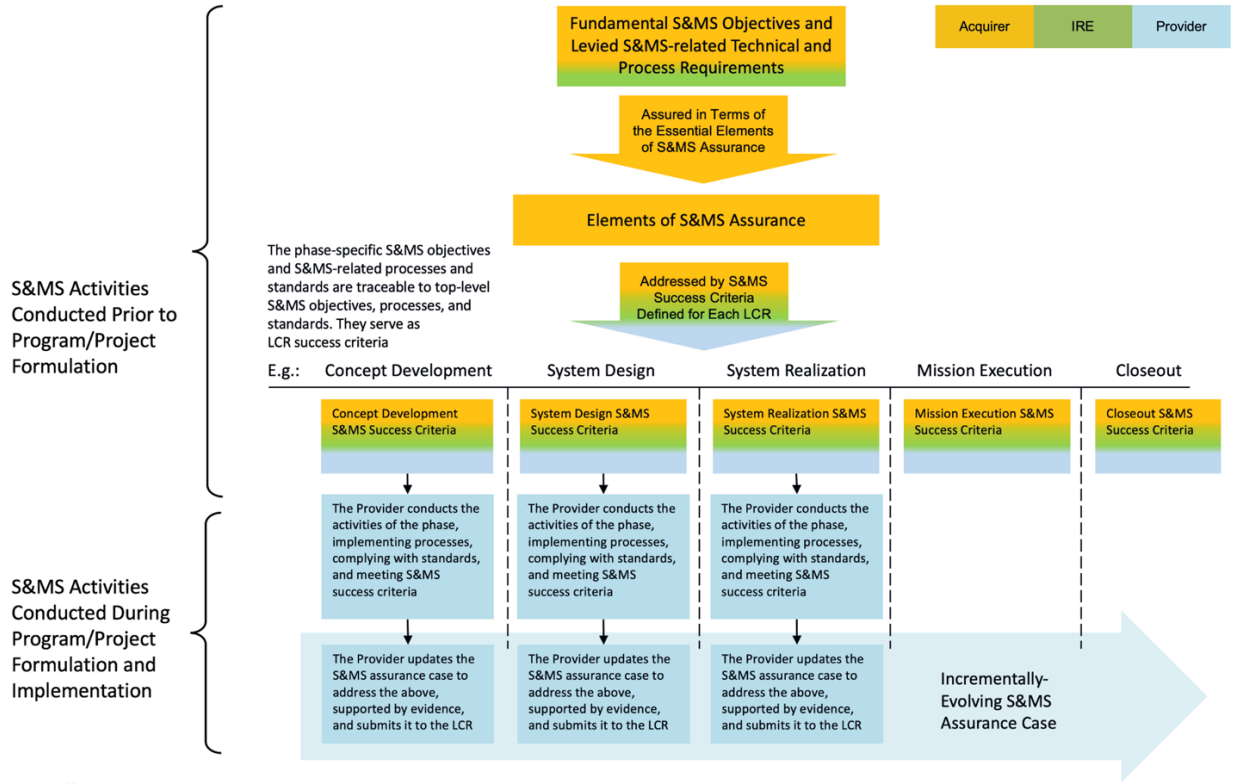

Figure 6. High-Level View of the S&MS Assurance Framework

Acknowledgements

The authors would like to thank the NASA Office of Safety and Mission Assurance (OSMA) for their sponsorship of the work underlying the development of the proposed S&MS assurance framework.

References

[1] H. Dezfuli, C. Everett, R. Youngblood, C. Everline, "*Modernizing NASA's Space Flight Safety and Mission Success (S&MS) Assurance Framework in Line with Evolving Acquisition Strategies and Systems Engineering Practices*", Office of Safety and Mission Assurance, NASA, Washington, DC., June 2021.

[2] NASA, "*NASA General Safety Program Requirements*", NPR 8715.3D, Washington, DC., August 2017.

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

[4] NASA, "*NASA Space Flight Program and Project Management Requirements*", NPR 7120.5F, Washington, DC., August 2012.

[5] NASA, "*NASA Systems Engineering Processes and Requirements*", NPR 7123.1C, Washington, DC., February 2020.

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

[7] ASAP, "*Aerospace Safety Advisory Panel Annual Report for 2014*", Washington, DC., 2015.

[8] NASA, "*Technical Standards for NASA Programs and Projects*", NPR 7120.10A, Washington, DC., February 2017.