May 27, 2022

Chris Everett
Lead Risk Assessment Engineer

Modernizing NASA's Space Flight Safety and Mission Success (S&MS) Assurance Framework

In Line With Evolving Acquisition Strategies and Systems Engineering Practices

Idaho National Laboratory

Purpose of this Presentation

- The purpose of this presentation is to summarize the current effort of the NASA Office of Safety and Mission Assurance (OSMA), supported by INL and others (e.g., JPL), to:
  - Formulate a framework for safety and mission success (S&MS) assurance that is:
    - Applicable to acquisition of products or services from non—NASA providers,
    - Consistent with NASA's governance structure (for example, in its involvement of Technical Authorities),
    - Compatible with existing and anticipated future NASA spaceflight program and project management and systems engineering (SE) practice, and
    - Consistent with NASA's philosophy of risk leadership within an established risk posture
  - Develop a Standard to support implementation of the S&MS Assurance Framework
- Additional discussion of the S&MS assurance framework and implementing standard can be found in the white paper:
  - [1] Dezfuli, H., Everett, H., Youngblood, R., Everline, C. "Modernizing NASA's Space Flight Safety and Mission Success (S&MS) Assurance Framework In Line With Evolving Acquisition Strategies and Systems Engineering Practices," OSMA, June 2021, https://ntrs.nasa.gov/citations/20220003490
- The NASA point of contact for further information is Homayoon Dezfuli, NASA HQ OSMA

Disclaimer

- All opinions presented herein, both verbally and in writing, are the opinions of the presenter and not necessarily of NASA or its official representatives
- The material presented herein is under development and subject to change, and does not represent current NASA process or practice

S&MS Assurance Framework Modernization Groundrules

- **NASA Acquirers have a duty to be assured that the missions they manage will be safe and successful:**
  - **Where what counts as adequate safety and mission success performance is clearly defined for the mission and captured as fundamental S&MS objectives consistent with Agency policy and risk leadership principles**
    - ***"The foundation upon which the ultimate assessment must be made is the acceptable level of risk. In other words—how safe is safe enough?"* – Aerospace Safety Advisory Panel (ASAP) 2011 Annual Report**
  - **Where NASA Acquirers' risk acceptance decisions have technically sound bases that provide justified confidence that Providers' have met, or are on track to meeting, the fundamental S&MS objectives**
- **NASA's framework for S&MS assurance must be applicable to all current and anticipated future NASA and Provider SE processes and practices, e.g.,:**
  - **It should be focused on the fundamental S&MS objectives, i.e., it should be objectives-driven**
  - **It should not over-constrain the Providers, i.e., it should be as process/technology-neutral and acquisition-model-neutral as practicable in order to provide flexibility and promote innovation in Providers' management practices and technical solutions**
  - **It should provide the NASA Acquirer with the information needed for technically sound S&MS risk acceptance decision-making, in a form that is maximally conducive to that decision-making**
  - **It should be consistent with NASA's governance model and system of checks and balances**

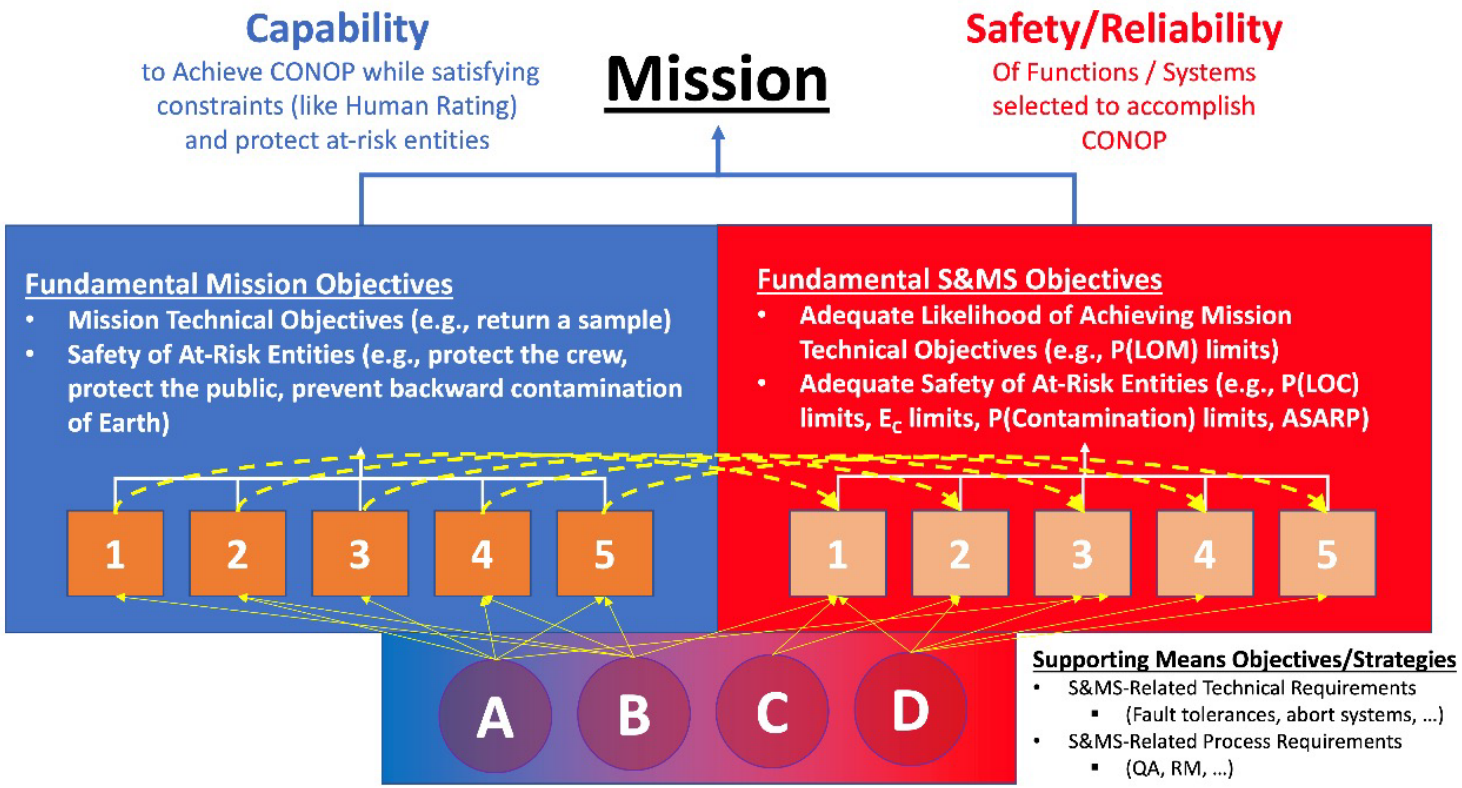
An Objectives-Driven Approach to S&MS (1 of 2)

- NASA has historically taken a largely prescriptive, deliverables-based approach to S&MS, in which adequate S&MS performance is deemed to result from the application of S&MS-related technical and process requirements.
  - E.g., fault tolerance requirements, requirements to use specific S&MS analysis techniques, requirements to implement specific defined S&MS-related processes
- However, the limitations of this approach have become increasingly evident:
  - The possibility of over-constraining the solution space, leading to inefficient processes, unnecessary expenditures, and sub-optimal systems and missions, particularly if the system/mission/acquisition is novel in some respect
  - The absence of explicit articulation and pursuit of what stakeholders fundamentally care about, i.e., mission-specific fundamental S&MS objectives
- In the proposed S&MS Assurance Framework, fundamental S&MS objectives are defined in association with fundamental mission objectives.
  - Below this level (i.e., at the level of means objectives), the Provider has the freedom to develop their own solutions (subject to TA/Acquirer concurrence/approval).
  - Any levying by the Acquirer of prescriptive S&MS-related technical and process requirements should be done judiciously and with clear justification. Prescription should not be the default

An Objectives-Driven Approach to S&MS (2 of 2)

- **Fundamental mission objectives define the desired outcomes of the mission.**
- **Fundamental S&MS objectives define expectations regarding the likelihood that the desired outcomes will be realized.**

Defines the *desired outcomes* (in absolute terms)



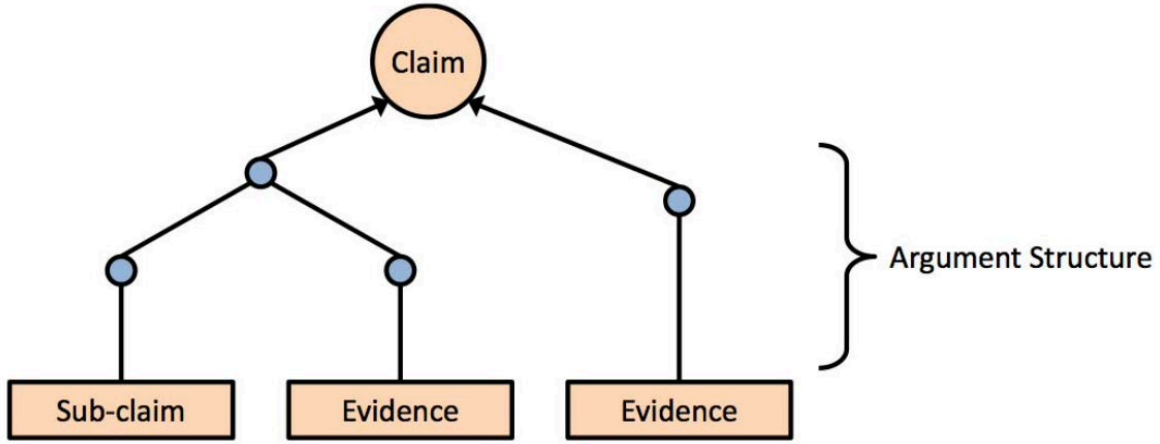
Defines the *risk posture* towards the desired outcomes (in probabilistic terms)

A Case-Based Approach to S&MS Assurance (1 of 3)

- The Provider has an obligation to convince the Acquirer that the fundamental S&MS objectives have been achieved
- However, because the fundamental S&MS objectives (e.g., P(LOC), P(LOM)) are probabilistic and non-observable, their achievement cannot be proven by direct evidence (e.g., in the way that meeting vehicle mass limits can be proven)
  - Unknown and/or underappreciated (UU) sources of S&MS risk have historically been significant causes of mishaps
- Instead, the Provider must make a case (i.e., an S&MS assurance case) that they have been achieved
  - The case for achievement of the fundamental S&MS objectives would be expected to argue the adequacy of all aspects of the program/project upon which S&MS performance significantly depends, over the full scope of its S&MS management system, e.g.,:
    - Design, manufacture, testing, operations, training, inspections, instrumentation, maintenance, continuous improvement, precursor analysis, change control…
  - The argument of the case must then be supported by potentially diverse substantiating evidence, e.g.:
    - Analyses, test results, operational data, internal audit results, independent review results, plans for future activities (e.g., precursor analysis, training, change control), evidence of organizational capability and commitment…
- A valid argument supported by evidence that substantiates its claims provides the Acquirer with a sound technical basis for being assured that the fundamental S&MS objectives have been achieved

A Case-Based Approach to S&MS Assurance (2 of 3)

- An S&MS assurance case is defined in [1] as:
  - 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).
- An S&MS assurance case has two main elements:
  - 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
  - *S&MS Evidence*, which substantiates the base claims



- Formalisms such as Goal Structuring Notation (GSN) or Claims, Arguments, and Evidence (CAE) *may* be used to impose rigor on the S&MS assurance case
- Standards for assurance case development are available, e.g., ISO/IEC 15026, *Systems and Software Engineering – Systems and Software Assurance*

A Case-Based Approach to S&MS Assurance (3 of 3)

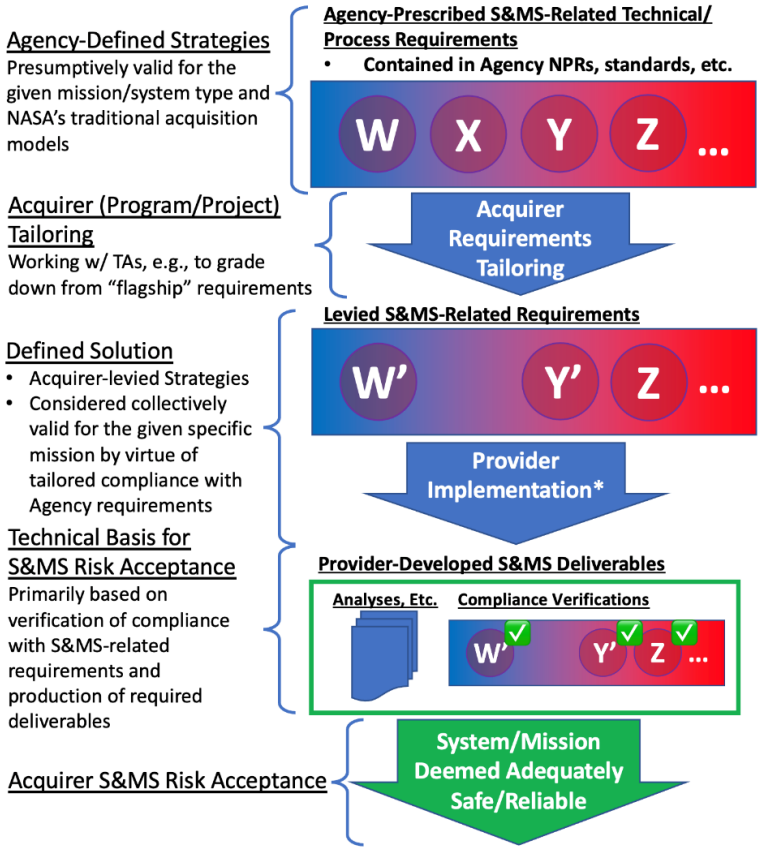
- Although the *Provider* develops the S&MS assurance case, its purpose is to satisfy the *Acquirer's* S&MS assurance needs
- Therefore, the Provider and Acquirer must work together to agree up front what counts at a high level as a valid S&MS argument
- For example, generic elements of S&MS assurance such as those below might be used to define the high-level claims of the S&MS argument*:
  - *Mission S&MS performance is adequately understood*
  - *The boundaries and assumptions (i.e., "normalcy map") within which S&MS performance is acceptable are understood*
  - *Effective S&MS-related management processes and controls are in place to maintain the system within the normalcy map*
  - *Mission S&MS performance meets minimum tolerable levels of mission S&MS performance*
  - *The mission is as safe as reasonably practicable (ASARP)*
  - *The mission complies with all Acquirer-levied S&MS-related requirements*

    **All of the above are maintained throughout the life cycle*
- Each of these claims would then be supported by its own argument structure and substantiating evidence
  - Note: substantiating evidence may be applicable to more than one claim

Objectives-Driven / Case-Based S&MS Assurance vs. Prescriptive / Deliverables-Based S&MS Assurance

Prescriptive

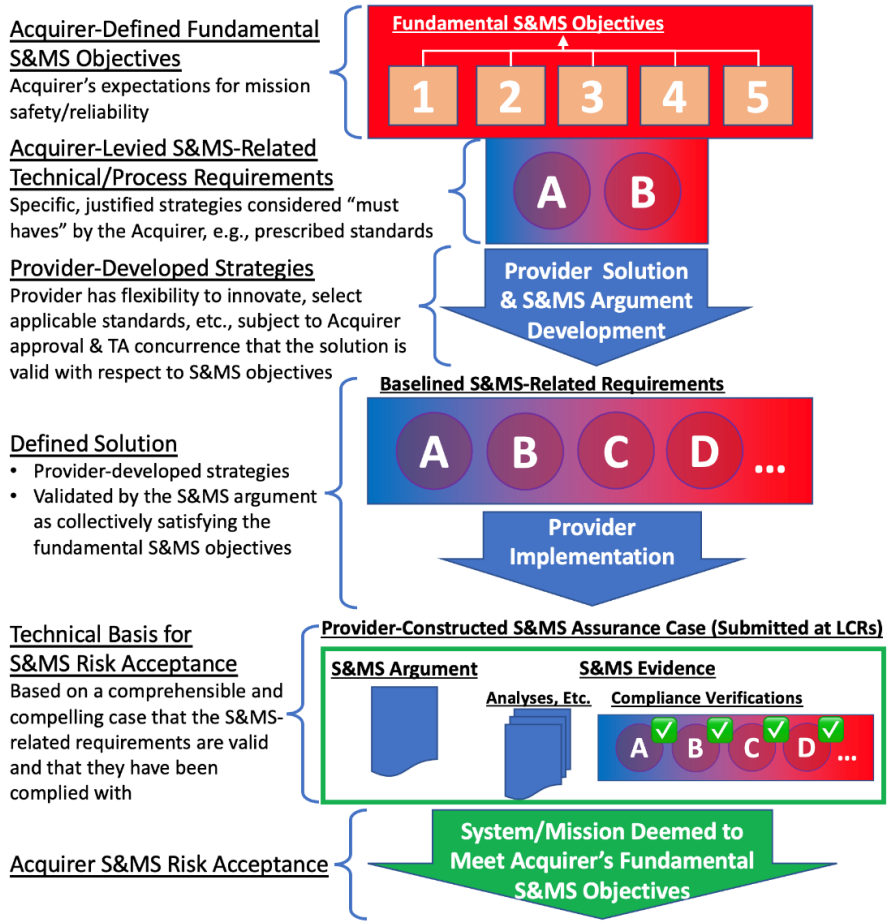
S&MS assurance based on compliance where mandated S&MS activities/deliverables are deemed to produce acceptable S&MS performance



*Subject to possible adjustment of requirements based on iteration with the Provider.

Objectives-Driven / Case-Based

S&MS assurance based on a compelling, comprehensible and valid case that the S&MS objectives have been met



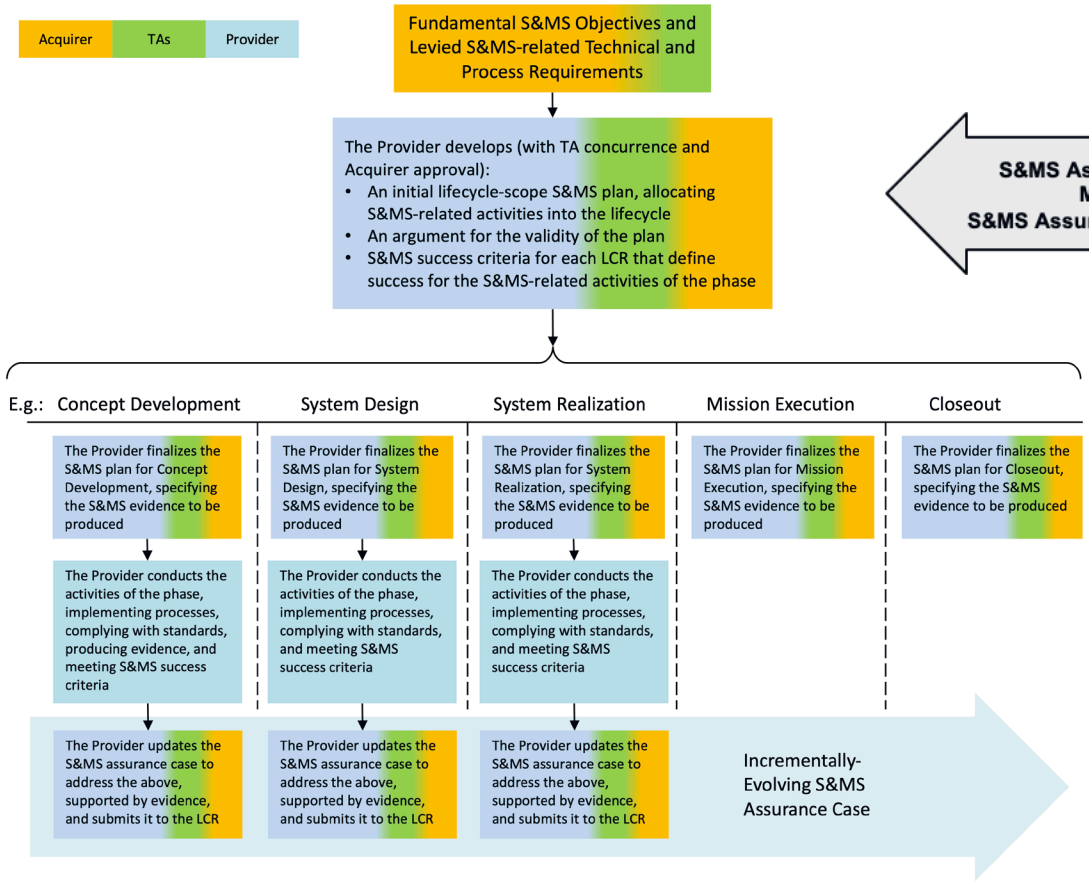
Addressing S&MS Incrementally Over the Program/Project Life Cycle

- Per NPR 7123.1, *NASA Systems Engineering Processes and Requirements*, each LCR has success criteria that define readiness to progress further in the life cycle
- In the S&MS assurance framework, these success criteria must include S&MS success criteria defining what must be accomplished in the phase in order to be deemed on track to meeting the fundamental S&MS objectives*
- S&MS success criteria that indicate the above are valid
- Valid S&MS success criteria enable the Acquirer to be confidently assured of adequate progress toward meeting the fundamental S&MS objectives throughout the program/project life cycle
- The S&MS assurance case is presented at each LCR, incrementally updated to address the S&MS criteria of the review
  - The S&MS assurance case is a living case that evolves over the entire program/project life cycle

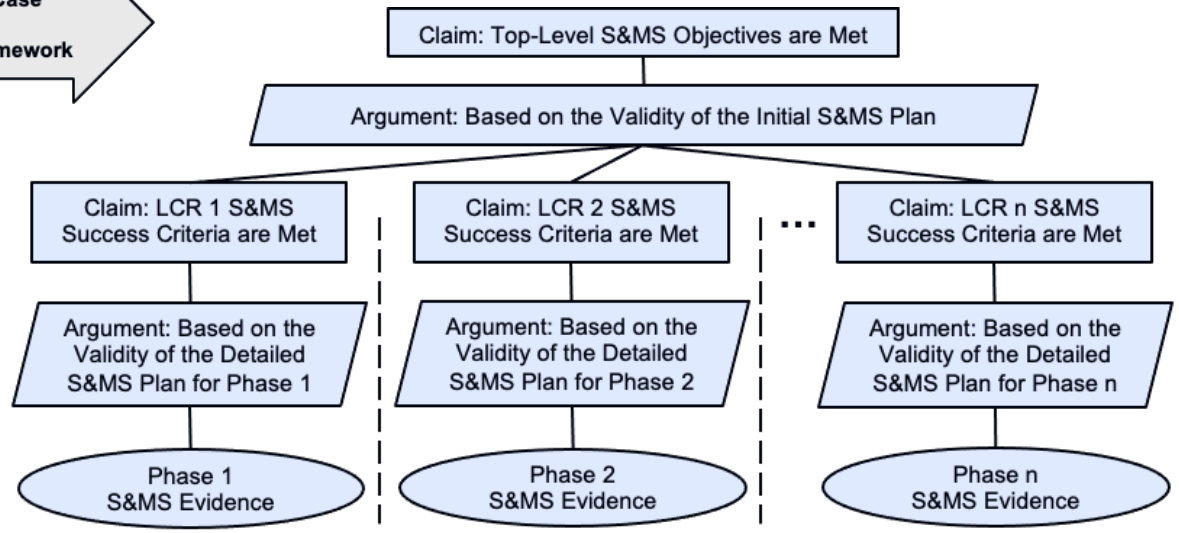
*And any Acquirer-levied S&MS-related technical and process requirements

The S&MS Assurance Case Evolves Over the Program/Project Life Cycle

- **The initial S&MS assurance case, developed early in Formulation, argues the validity of the initial S&MS plan with respect to the S&MS objectives, including the validity of the S&MS success criteria defined for each LCR**



S&MS Assurance Case Mirrors S&MS Assurance Framework



Example S&MS Success Criteria

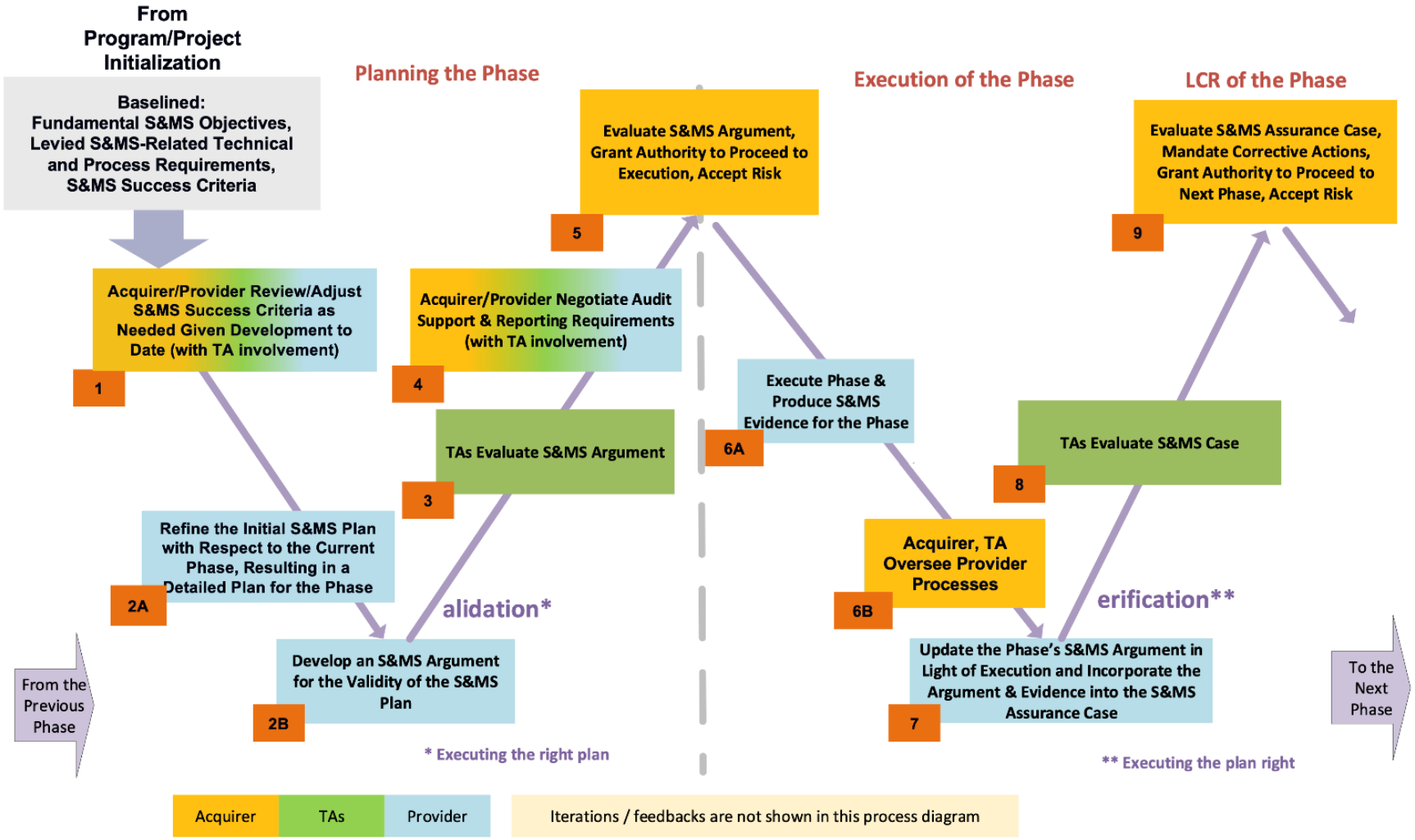
- These are the example S&MS success criteria in the current draft S&MS Assurance Standard:

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 S&MS objectives are 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.
	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	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.
	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	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	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.

The "W-Engine" for S&MS Assurance (1 of 2)

- Within each life cycle phase, Provider S&MS activities are focused on:
  - Meeting the S&MS success criteria of the associated LCR(s) (ensurance)
  - Making the case to the Acquirer that the S&MS success criteria have been met (assurance)
- These activities are codified in the "W-Engine" for S&MS assurance (Illustrated on the next slide). They can be partitioned into:
  - S&MS Planning
    - The Provider develops, and Acquirer approves:
      - A detailed S&MS plan for the phase (as part of overall SE planning for the phase), including specification of the S&MS evidence that will be produced to verify that the S&MS success criteria have been satisfied
      - An S&MS argument for the phase that validates the plan as being responsive to the S&MS criteria
  - S&MS Execution
    - The Provider:
      - Executes the S&MS plan for the phase, producing the agreed-upon S&MS evidence verifying that the S&MS success criteria have been met
      - Updates the S&MS assurance case to address the phase and submits it to the LCR
  - S&MS Risk Acceptance
    - The Acquirer, supported by the Standing Review Board (SRB), evaluates the S&MS assurance case and makes the appropriate S&MS risk acceptance decision
- Technical Authority (TA) concurrences are sought throughout

The "W-Engine" for S&MS Assurance (2 of 2)



Note: The numbered steps in this process correspond to requirements in the draft S&MS Assurance Standard.

Areas of Accountability of Actors in the S&MS Assurance Framework (1 of 3)

- An objectives-driven approach to S&MS places an increased burden on the Provider to validate its solution with respect to the fundamental S&MS objectives
  - The S&MS argument provides the rationale for this validation
  - This is in contrast to a prescriptive approach to S&MS where the Provider's solution is deemed valid by virtue of compliance, potentially without any characterization of mission S&MS performance
- 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, to the degree necessary for informed S&MS risk acceptance
  - For the Acquirer, this results in more effective and informed S&MS risk acceptance
  - For the Independent Technical Review Entities, this results in a more effective system of institutional checks and balances
- Giving providers freedom within the constraints imposed by the fundamental S&MS objectives (as opposed to prescriptive requirements) enhances the potential for technical and process innovation and the adoption of emerging best practices
- An objectives-driven approach to S&MS holds each actor (Provider, Acquirer, and Independent Technical Review Entities) accountable for explicitly understanding the assessed S&MS performance of the Provider's solution

Areas of Accountability of Actors in the S&MS Assurance Framework (2 of 3)

- **Acquirer (NASA entity)**
  - Impose system/mission-level fundamental S&MS objectives on the Provider.
  - Levy, sparingly, 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.

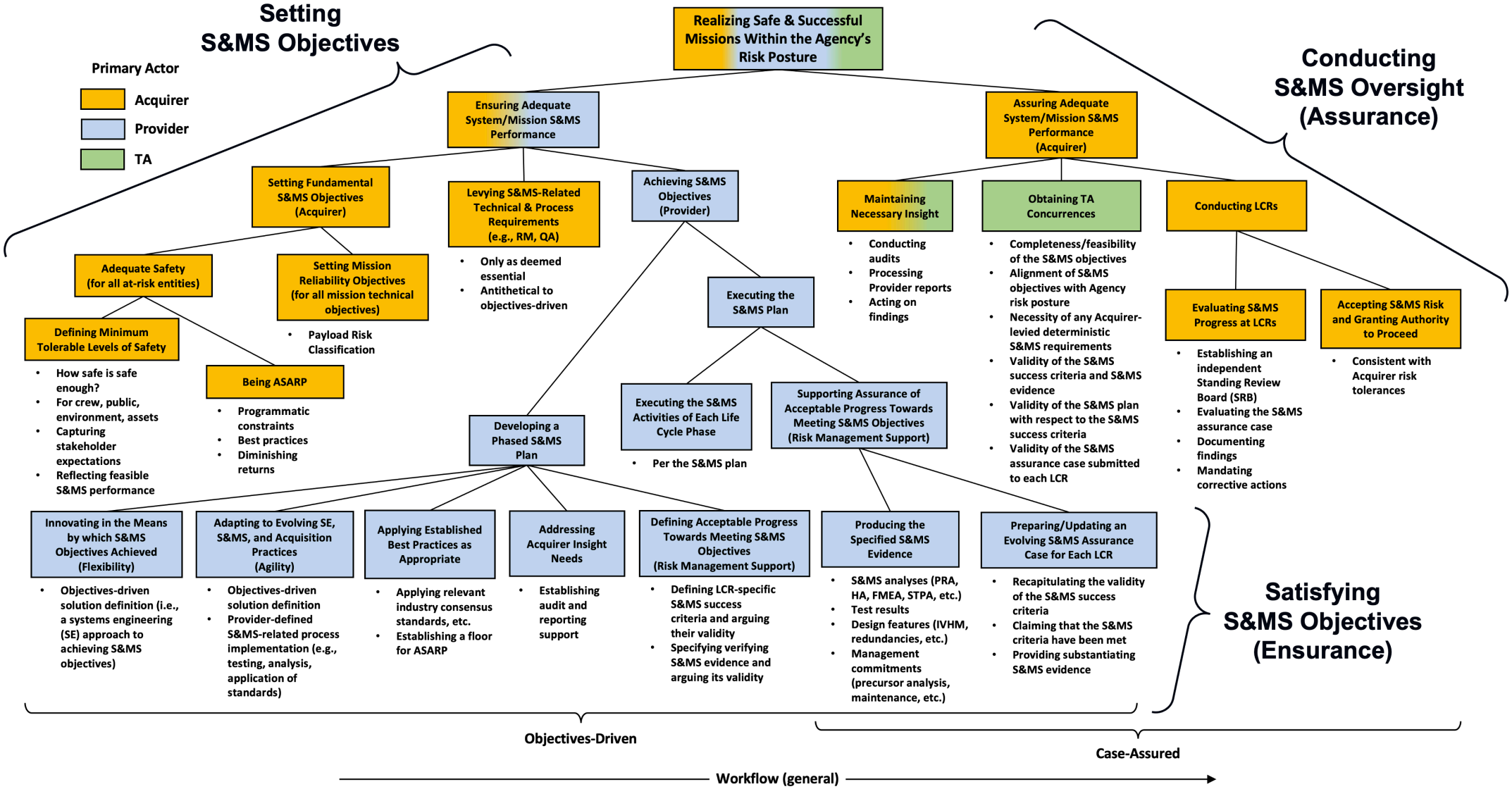
Areas of Accountability of Actors in the S&MS Assurance Framework (3 of 3)

- **Provider** (NASA and/or non-NASA entity)
  - Develop an initial program/project plan, including S&MS success criteria for each LCR, and argue their validity.
  - Develop, for each life cycle phase:
    - A detailed S&MS plan for the phase that nominally meets the corresponding S&MS success criteria, including specification of the S&MS evidence that will be used to verify that the S&MS success criteria have been met.
    - An 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).
- **Independent Technical Review Entities** (NASA entities)
  - Act as independent, critical, and skeptical elements of NASA's system of checks and balances.
  - TAs :
    - Concur or non-concur with the achievability of the fundamental S&MS objectives.
    - Concur or non-concur with the validity of the S&MS success criteria.
    - For each life cycle phase, concur or non-concur with the validity of the Provider's S&MS plan.
    - 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.
  - SRB evaluates the S&MS assurance case at each LCR and presents its findings and recommendations to the Convening Authorities.

Standards-Based Implementation of the Proposed S&MS Assurance Framework (1 of 2)

- 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
- 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
- OSMA is in the process of developing a ***Standard for Assurance of Safety and Mission Success*** (i.e., the S&MS Assurance Standard) that implements the proposed S&MS assurance framework
- 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

Standards-Based Implementation of the Proposed S&MS Assurance Framework (2 of 2)



Summary

- There is an immediate need to modernize NASA's space flight S&MS assurance framework
  - This need is corroborated by NASA-internal analysis and the assessments of external organizations such as ASAP
- An objectives-driven, case-based framework for S&MS assurance
  - Addresses the probabilistic nature of S&MS performance
  - Is responsive to the underlying issues motivating the modernization
- The proposed S&MS assurance framework being developed by OSMA integrates an objectives-driven, case-based framework into:
  - NASA's governance model and system of checks and balances
  - NASA's program/project management framework, utilizing life cycle phases, success criteria, and LCRs
- The proposed S&MS assurance framework provides for ongoing incremental S&MS assurance over the program/project life cycle by:
  - Imposing discipline on the formulation of LCR-specific S&MS success criteria
  - Proactively validating the Provider's S&MS plans with respect to the S&MS success criteria prior to plan execution
  - Verifying the satisfaction of S&MS success criteria using S&MS evidence specified in advance
- Submittal of an S&MS assurance case at LCRs (rather than a document dump) provides a coherent basis for Acquirer S&MS assurance

Acknowledgments

- This activity is consistent with the objectives-driven, case-based approach to system safety promoted in the *NASA Systems Safety Handbook* (expanded to S&MS)
- This activity has been informed by a number of existing case-based standards and other guidance, including:
  - ISO/IEC/IEEE 15026, "Systems and Software Engineering—Systems and Software Assurance"
  - Defence Standard 00-56 (Def Stan 00-56), "Safety Management Requirements for Defence Systems"
  - *Manual of Air System Safety Cases (MASSC)*
  - Regulatory Article 1200 – "Air Safety Management"
- Additional support for the present approach can be found in the NASA OSMA white paper, "Modernizing NASA's Space Flight S&MS Assurance Framework In Line With Evolving Acquisition Strategies and Systems Engineering Practices"
- Further questions should be directed to Homayoon Dezfuli, NASA HQ OSMA