EXPLORING DIGITAL TRANSFORMATION FOR NASA NUCLEAR FLIGHT SAFETY

Donald Helton[(1)], Matthew Forsbacka[(1)], Anthony DiVenti[(1)], Steven Cornford[(2)], Mary Bone[(3)], Homayoon Dezfuli[(1)]

[(1)]NASA, 300 E Street SW, Washington, DC 20546, U.S.A., donald.m.helton@nasa.gov
[(2)]Jet Propulsion Laboratory, 4800 Oak Grove Drive, Pasadena, CA, 91190, U.S.A., steven.l.cornford@jpl.nasa.gov
[(2)] NASA Langley Research Center, Hampton VA, 23681, U.S.A, mary.bone@nasa.gov

ABSTRACT

The U.S. National Aeronautics and Space Administration's (NASA)'s Nuclear Flight Safety discipline is exploring opportunities to combine incremental advancements in many contributing areas in a way that produces a transformative change for how work is performed. More specifically, after providing some general NASA and space nuclear policy background, the authors will describe concepts and efforts that enable: (i) the use of objectives-driven approaches (in concert with internal and external constraints) to establish a mission risk posture; (ii) the use of that risk posture in the planning process to risk-inform the selection of Safety and Mission Success (S&MS) methods and models; (iii) use of model-based and machine-assisted techniques to manage the complex and ponderous amount of information and interfaces that typify spaceflight efforts; (iv) the means by which that infrastructure can directly feed an assurance case (including use of systems modelling language, ontological formulation, and semantic web technology) so as to address known weaknesses in our ability to communicate and manage that complexity; and (v) use of that case-assured framework to demonstrate that one did the adequate and sufficient S&MS work and that the S&MS work was done competently.

1. THE CURRENT NASA CONTEXT

The key point in this section is that the U.S. National Aeronautics and Space Administration's (NASA's) Office of Safety and Mission Assurance (OSMA) is embracing the use of objectives-driven, risk-informed, and case-assured approaches to safety and mission success (S&MS) in a manner that harmonizes with NASA's systems engineering approach to life cycle management and execution of programs and projects. The backdrop is that while NASA continues to explore space and perform cutting edge science, missions continue to be more and more complex. This drives the need to rely on computers to do the tasks that they are well-positioned to do, including things like error-checking, cross-comparing design-to-construction and visa versa, and creating traceable representations of the customization of programs and projects (particularly with the rise of evolving acquisition strategies to enable a vibrant commercial space economy).

1.1. Objectives-driven, Risk-informed, and Case-Assured

NASA revised NASA Policy Directive (NPD) 8700.1 [1] in 2022 to, amongst other changes, codify use of objectives-driven, risk-informed, and case assured approaches to S&MS. In describing the three main categories of OSMA policy in Section 1 of NPD 8700.1 (i.e., crew safety and mission success, safety in protecting other entities, and safety culture), OSMA embeds features of objectives-driven, risk-informed, and case-assured throughout.

In doing so, OSMA appropriately anchors these features (e.g., risk informing) in the authorizing NASA policy (e.g., NPD 1000.0's description of the use of risk leadership) [2]. For instance, NPD 8700.1 defines that, for crew safety and mission success, the risk posture will be established and treated as a central element of decision-making during formulation, implementation, and operation. Risk leadership, which has been anecdotally described as leading organizations to taking the right risks as opposed to helping organisations manage the risks right, is a foundational concept in OSMA's current evolution. In a nutshell, risk leadership starts with the candid and succinct articulation of an activity's risk posture. Given that established risk posture, an activity is then able to use standard techniques like goal structured notation to build an objectives hierarchy that provides linkages between goals, strategies, and evidence, along with risk trade (i.e., risk-informing) information, to determine what sub-activities (i.e., tasks that produce evidence) will support established objectives in light of the established risk posture. The act of creating this structure (i.e., the case) and then methodically managing it as a living structure during the course of an overall activity is what makes the outcomes of the activity case-assured.

The use of risk leadership appears most overtly in the policy tenets of Section 1.a of NPD 8700.1, in dealing with crew safety and mission success. However, the underlying concepts of risk leadership also apply in Section 1.b, which deals with other safety aspects (protection of the public, personnel, property, and the environment). The invocation of risk leadership in these other areas is more subtle, in that the core risk posture is often more influenced by external processes (e.g., the Federally-mandated nuclear launch authorization policy in the case of space nuclear systems). However, the more granular concepts of risk-informing, anchoring in objectives, and approaching assurance through cases equally applies. For instance, Section 1.b(1) discusses managing safety as an integral aspect of the objective of the program, project, facility or NASA Center operations and activities (objectives-driven). Section 1.b(3) describes prioritizing performance-based approaches, which is fully in line with use of assurance cases (case-assured). Section 1.b(4) describes the use of subject matter experts to inform decisions about managing risks for unique hazards (risk-informed). Thus, while external constraints may rightfully constrain NASA from having full latitude for risk leadership in these core safety areas, the same underlying tools for establishing and managing the activities' safety standard and risk posture apply. The authors will come back to these NPD 8700.1 policy tenets later in the paper.

1.2. Systems Engineering Approach to Life Cycle Management

Objectives-driven and case-assured approaches are fully compatible with a systems engineering approach to life cycle management, and systems engineering more broadly. In fact, Model-based Mission Assurance (MBMA) often relies on Model-Based Systems Engineering (MBSE) and almost always benefits from it. NASA extensively uses systems engineering in its life cycle management activities, as described in NASA NPR 7123.1 [3] and NPR 7120.5 [4]. In addition, current efforts are underway to develop sysML models of the directives themselves, to further facilitate a systems engineering approach to their implementation.

As the remainder of the paper describes ongoing activities, the authors emphasize here that these activities are being implemented in a way that integrates into this existing NASA way of doing business (i.e., Policy Directives, Policy Requirements, and use of Accepted STDs). For instance, OSMA is developing an S&MS Assurance Standard that establishes the objectives-driven, risk informed, and case-assured framework for S&MS assurance as described in NPD 8700.1F and invoked through S&MS NASA Procedural Requirements documents (e.g., NPR 8705.2 and 8705.4 for crewed and uncrewed missions, respectively). For each respective objective and requirement, corresponding success criteria are defined across the life-cycle phases such that the evolution of the assurance case (i.e., the argument as supported by evidence) can be managed using the same fundamental practices that are used for managing all other aspects of program or project products, including the role of Standing Review Boards and Life Cycle Reviews occurring between Key Decision Points. Further, this assurance case life cycle management methodology will also rely on tools and products described later in this paper to translate the over-arching mission risk posture into the more specific objectives, strategies, and tasks that operationalize that risk posture. The promulgation of the risk through an Assurance Implementation Matrix will harmonize with, rather than interfere with, the traditional steps of performing human-rated or robotic risk classifications, defining the project category, etc. For Nuclear Flight Safety this means that the promulgation of the risk posture will take into account both the external requirements (e.g., the tiering of missions and resulting assignment of the decision-making authority based on Federal policy) while at the same time factoring in the risk-informing and tailoring of mission success requirements that have an indirect effect on nuclear safety.

Finally, the focus on assurance cases maintains the ability and value of explicitly referencing existing standards as means of promoting efficient analysis and review.

1.3. Digital Transformation More Broadly

Throughout this paper the authors will point to enabling work being performed within NASA and elsewhere, with this work sometimes occurring across a broad range of organizations and under the moniker of "digital transformation" or "digital engineering." Digital engineering has been defined as "an integral digital approach that uses authoritative sources of systems data and models as a continuum across disciplines to support lifecycle activities from concept through disposal." [5] Digital engineering is generally an umbrella term that encompasses approaches like MBMA and MBSE, along with concepts like a single-source-of-truth and interoperable systems, to create a digital eco-system. The pointers herein are a very small sample of the overall work being performed within the community.

While the authors are focused on specific aspects of the Nuclear Flight Safety eco-system in this paper, the authors are also aware of the importance that these concepts integrate into the broader eco-system. Some cross-cutting concepts being used at NASA to ensure such cohesion are: (i) establishing interoperable architectures, (ii) transforming critical processes, (iii) maintaining the impact of the data, (iv) adopting common tools, and (v) strengthening inclusive teaming. With that said, these broader initiatives are not the focus of this paper, which instead focuses on Nuclear Flight Safety in an effort to help understand and pilot these broad-reaching themes. More information about NASA's broad Digital Transformation activities can be found elsewhere [6].

1.4. Challenges with the Current Situation

The authors are advocating for evolving this approach to S&MS, including in the Nuclear Flight Safety area, because we perceive weaknesses in the existing situation that are addressable via emerging approaches. In particular, emerging machine-assisted and model-based capabilities, as well as supporting capabilities like ontologies and semantic reasoning are well-suited to address tasks that are currently tedious, error-prone, or outright infeasible, such as:

- Taking vintage information (in this case meaning space nuclear system analysis contained in the tens of thousands of pages of safety analysis documentation spanning seven decades and using varying terminology) and assessing its degree of relevance to related situations – a task that is well-suited for machine-assistance through semantic reasoning supported by discipline-specific ontologies;
- Avoiding the checklist mentality in performing and defending tasks by linking those tasks to their reason for existence and the thing that they are helping to accomplish – a task that is well-suited for objectives hierarchies and assurance cases;
- Treating interdependencies such that the risk you are managing in one area is explicitly linked to the risks and opportunities that it influences in other areas – a task that is well-suited for MBSE and MBMA.

In the latter sections of this paper, the authors will provide examples and discussion that further elaborate on how these different approaches can be developed and implemented in a way that mitigates challenges like those listed above.

2. THE CURRENT SPACE NUCLEAR CONTEXT

The mature nature of the terrestrial nuclear assessment infrastructure, the recently-revised Federal policy for launch of space nuclear systems, and the ground-swell of diverse space nuclear interests has created a unique opportunity to meaningfully advocate for robust and flexible approaches to S&MS in the space nuclear realm.

2.1. Terrestrial Foundation

While the space nuclear realm has benefited from the preceding seven decades of terrestrial nuclear assessment and assurance framework effort, it has also suffered from the relative inconsistency across the small number of initiatives focused on developing and launching space nuclear systems. The authors see clear benefit in more consistent use of the terrestrial precedent as a guide for the space nuclear situation.

In this vein, Fig. 1 provides a notional flowdown of how the terrestrial safety frameworks can readily map to supporting elements, including regulatory pathway determinations, use of accepted standards, and safety activities. All four levels of this notional breakdown exist for terrestrial situations; specific pieces of each exist for space nuclear situations and the degree to which individual documents in each level can be leveraged in space nuclear applications vary.

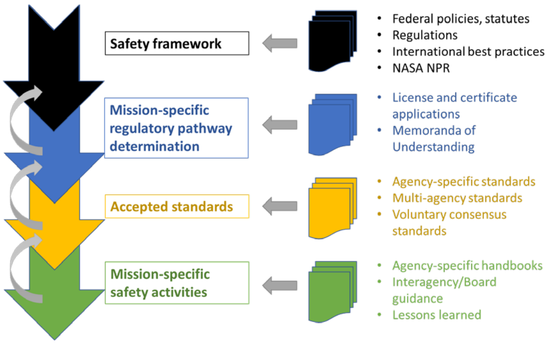

Safety framework
Federal policies, statutes
Regulations
International best practices
NASA NPR
Mission-specific regulatory pathway determination
License and certificate applications
Memoranda of Understanding
Accepted standards
Agency-specific standards
Multi-agency standards
Voluntary consensus standards
Mission-specific safety activities
Agency-specific handbooks
Interagency/Board guidance
Lessons learned

Figure 1. Flow Down of Authorities to Safety Activities

Documents like DOE-STD-1189 [7], DOE-STD-3009 [8], and the Advanced non-Light Water Reactor Probabilistic Risk Assessment Standard [9] were developed specifically with terrestrial situations in mind, however, analysts, evaluators and authorizers could readily extrapolate these documents to a space nuclear application by proactively agreeing on materials that directly apply and adapting the portions that do not.

2.2. Space Nuclear Policy Development

The U.S. Atomic Energy Act addresses nuclear technology use on Earth; there is no equivalent U.S. Law specifically addressing nuclear technology use in space. Rather, a combination of domestic and international policies currently address the space nuclear Safety Framework (i.e., the top box in Fig. 1). Key among these are U.S. National Security Presidential Memorandum No. 20 [10], U.S. Space Policy Directive No. 6 [11], the United Nations (UN) Outer Space Treaty [12], and the Safety Framework for Nuclear Power Source Applications in Outer Space [13] co-developed by the United Nations and the International Atomic Energy Agency (IAEA). These references, along with their scope and context, are described in more detail in other articles (e.g., [14]).

While this framework is not as well-exercised or codified as the terrestrial framework, it does provide many of the needed piece-parts for implementation. NASA and the U.S. Department of Défense have codified the framework at the most fundamental of levels [15, 16]. U.S. stakeholders continue to work on defining and clarifying the permissible mission-specific regulatory pathways, as well as accepted standards and practices (i.e., the 2nd and 3rd boxes in Fig. 1), as will be discussed more in the following sub-section.

Importantly, this framework is fully compatible with an objectives-driven, risk-informed, and case assured approach. Most significantly, NSPM-20 specifically sets a measure of "how safe is safe enough" in establishing its Safety Guidelines, while also creating a risk-informed tiering process that governs the level of review and the degree of elevation of the authorization decision.

2.3. Space Nuclear Standards Development

Space nuclear system developers, evaluators, and decision makers are currently missing a set of accepted standards that would make analysis, review, and authorization more effective, by pre-determining consensus accepted approaches. Historically, space nuclear personnel had less need for such standards because launches of space nuclear systems were infrequent, and often followed the same general pattern (in terms of technology and approval) for multiple decades. However, space nuclear personnel now face a diverse set of projects (from both a technology and partnership perspective) on the horizon, including the potential for the first U.S. commercial launch (as opposed to a government-sponsored launch) of a space nuclear system.

Space nuclear personnel are working on several initiatives that should help to fill in important gaps related to accepted standards. These include both informal guidance and knowledge transfer tools and more formal standards. To the latter, a 2022 Space Reactor Standards Working Group [17] report identified three high-priority gaps that are currently being explored further toward the development of space reactor standards in these topical areas (facilities/testing, safety and risk analysis methods, safe in-space operation). Plutonium-based radioisotope power systems have a significant heritage in terms of their design, analysis, and review, however, novel and commercially-developed radioisotope power systems may also benefit from standards-oriented activities if they continue to see sustained and diverse development.

The authors wish to emphasize that the projected U.S. space nuclear community of the 2030s does not resemble that of the 1960s to 2010s. Rather than one to two U.S. government flagship missions per decade using space nuclear systems, with those always being missions sponsored by NASA or the U.S. Department of Defense and with limited international involvement relative to the nuclear system itself, the future may hold a dramatically more diverse set of sponsors working under substantially different partnership models, akin to what has occurred in other portions of the U.S. space industry. Such a situation would significantly benefit from a strong and clear safety framework, clear delineations of available regulatory pathways, and consensus accepted standards. The following sections will describe how objectives-driven, risk-informed, and case-assured approaches can ensure that a strong framework can co-exist with flexible implementation.

3. CURRENT EFFORTS TO EVOLVE

This section breaks down the ongoing efforts along the lines of the three main features of the desired end-state, that being objectives-driven, risk-informed, and case-assured. The authors are using this breakdown to facilitate the narrative; but in fact, all of these efforts are inter-related with all three of these key features. This is shown pictorially in Fig. 2.

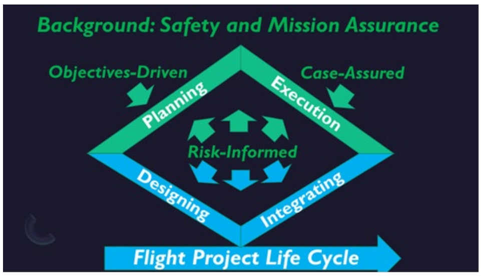


Figure 2 – Illustration of the Three Key SMS Elements

Later in this paper, the authors explore these concepts through the lens of NASA Nuclear Flight Safety. The same concepts are being explored across safety and mission assurance activities in all disciplines and are stepping stones growing out of prior work, such as [18] and [19]. Reference [20] provides a broad and foundational discussion of how and why these concepts grew to be so central to NASA's current activities to evolve S&MS assurance.

3.1. Objectives-driven Tools for Planning Nuclear Flight Safety Activities

Any given spaceflight project will have S&MS elements but will also have other elements (such as scientific goals or acquisition-related constraints) that will be important. While the objectives-driven approach applies to all of these, this paper focuses on the S&MS aspects most relevant to Nuclear Flight Safety. The premise is that the objectives-driven S&MS aspects will build from the objectives-driven program level requirements (science and exploration goals and objectives), the external drivers (e.g., partnership considerations, Congressional direction), and cost considerations (e.g., announcement opportunity criteria, budget realities). Objectives-driven approaches are already utilized in some of these other aspects which facilitates marrying of an objectives-driven S&MS approach into the bigger picture in a way that harmonizes rather than conflicts. Importantly, an objectives-hierarchy governing the programmatic interests and an assurance case governing the S&MS activities would readily be able to share evidence (e.g., system reliability evidence that supports both the availability of a power source for crew habitation and the reduction in potential for an event that causes harmful contamination) in the overall project eco-system.

To ground the discussion in the over-arching S&MS policy for the focus of this paper, Fig. 3 shows an evolving mapping between the most relevant policy tenets in NPD 8700.1 down to high-level Nuclear Flight Safety strategies that are codified in the requirements of NPR 8715.26. (Intervening high-level objectives may be added to a future version of NPR 8705.4 to assist in this translation.)

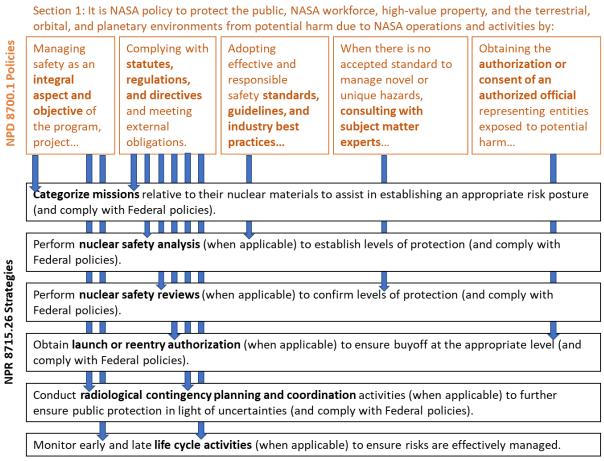

Section 1: It is NASA policy to protect the public, NASA workforce, high-value property, and the terrestrial, orbital, and planetary environments from potential harm due to NASA operations and activities by:
NPD 8700.1 Policies
Managing safety as an integral aspect and objective of the program, project…
Complying with statutes, regulations, and directives and meeting external obligations.
Adopting effective and responsible safety standards, guidelines, and industry best practices…
When there is no accepted standard to manage novel or unique hazards, consulting with subject matter experts…
Obtaining the authorization or consent of an authorized official representing entities exposed to potential harm…
NPR 8715.26 Strategies
Categorize missions relative to their nuclear materials to assist in establishing an appropriate risk posture (and comply with Federal policies).
Perform nuclear safety analysis (when applicable) to establish levels of protection (and comply with Federal policies).
Perform nuclear safety reviews (when applicable) to confirm levels of protection (and comply with Federal policies).
Obtain launch or reentry authorization (when applicable) to ensure buyoff at the appropriate level (and comply with Federal policies).
Conduct radiological contingency planning and coordination activities (when applicable) to further ensure public protection in light of uncertainties (and comply with Federal policies).
Monitor early and late life cycle activities (when applicable) to ensure risks are effectively managed.

Figure 3 – NPD 8700.1 Tenets to NPR 8715.26 Strategies

Figure 3 only addresses those policy tenets most relevant to Nuclear Flight Safety, whereas NPD 8700.1 includes additional tenets under the safety category (Section 1.b), as well as separate tenets under a crew safety and mission success category (as previously described). The crew safety and mission success elements have important interdependencies with Nuclear Flight Safety, while safety culture is the eco-system in which all of these elements operate.

With the basic strategies for Nuclear Flight Safety established, an important task is to risk-inform the activity as a whole, so that the underlying tasks can be appropriately risk-informed (which is the subject of the following sub-section). To do this, we need to overlay the missions risk posture with the National risk posture related to use of space nuclear systems. NASA does this in an integrated fashion as shown in Fig. 4. Mission pre-formulation activities and related or un-related nuclear system development and safety activities contribute to the initial and boundary conditions that drive the transition to mission formulation. Next, a series of "tuning" steps occur that effectively establish the mission's initial risk thread, with these comprising the categorization of the spaceflight project's programmatic risk tolerance, the mission's risk tolerance, the launch vehicle risk tolerance, and the space nuclear system risk tolerance. Some of these determinations are explicitly coupled (e.g., NASA NPR 7120.5 has specific criteria related to both mission cost and nuclear technology) while others are implicitly coupled (e.g., NASA NPR 8715.26 invokes a process where initial mission nuclear tiering is based on the system but final tiering is impacted by the computed mission risk which is in turn affected by launch vehicle reliability).

The outcome of these risk tolerance determinations then becomes the starting point for 4 key documents: the Assurance Implementation Matrix, the Systems Engineering Management Plan, the Safety and Mission Assurance Plan, and the Nuclear Launch Authorization Plan.

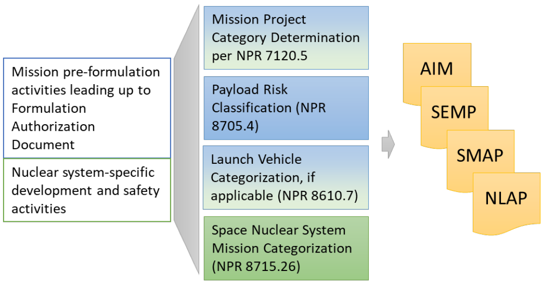

Mission pre-formulation activities leading up to Formulation Authorization Document
Nuclear system-specific development and safety activities
Mission Project Category Determination per NPR 7120.5
Payload Risk Classification (NPR 8705.4)
Launch Vehicle Categorization, if applicable (NPR 8610.7)
Space Nuclear System Mission Categorization (NPR 8715.26)
AIM
SEMP
SMAP
NLAP

Figure 4 – Marrying of Mission and Space Nuclear Technology Risk Postures

This process is most often described by a series of meetings that then lead to the development of plans that are manually generated by refreshing past examples. NASA is working on a tool called the Advanced Program Plan Generator (APPG) that will automate some aspects of this process, including creating a tighter coupling between the subject matter experts that own the relevant policies and the project personnel that are implementing them. APPG will create a digital launching-off point that will further enable model-based activities described later in this paper, including a potential interface with SysML models of the actual over-arching policies.

To set the stage for later discussion, Fig. 5 takes one of the boxes from Fig. 2, the one related to nuclear safety review, and de-composes that strategy into an associated goal and associated subsidiary strategies. These subsidiary strategies are approaching the level of granularity where one can transition from the policy of what constitutes an adequate nuclear safety review (held in a procedural requirements document) to an accepted state-of-practice for the more-detailed features that an adequate effort would produce (held in an accepted standard). For instance, one can imagine an accepted consensus standard for the nuclear safety review supporting launch approval of a space nuclear system that describes the process characteristics and evidence that a project can use to illustrate the five sub-strategies provided in Fig. 5.

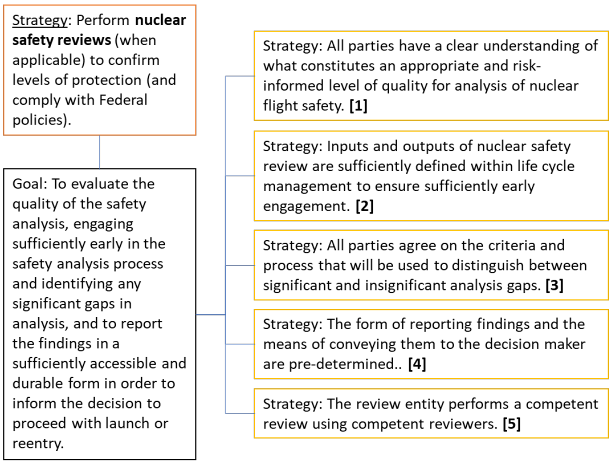

Strategy: Perform nuclear safety reviews (when applicable) to confirm levels of protection (and comply with Federal policies).
Goal: To evaluate the quality of the safety analysis, engaging sufficiently early in the safety analysis process and identifying any significant gaps in analysis, and to report the findings in a sufficiently accessible and durable form in order to inform the decision to proceed with launch or reentry.
Strategy: All parties have a clear understanding of what constitutes an appropriate and risk-informed level of quality for analysis of nuclear flight safety. [1]
Strategy: Inputs and outputs of nuclear safety review are sufficiently defined within life cycle management to ensure sufficiently early engagement. [2]
Strategy: All parties agree on the criteria and process that will be used to distinguish between significant and insignificant analysis gaps. [3]
Strategy: The form of reporting findings and the means of conveying them to the decision maker are pre-determined.. [4]
Strategy: The review entity performs a competent review using competent reviewers. [5]

Figure 5 – De-composition of the Nuclear Safety Review Strategy

This type of objectives hierarchy approach can be tedious to implement and execute, but it engrains four key features:

1. It keeps the dialogue focused on the "what" and not the "how" when it comes to establishing the approaches;
2. It provides traceability between high-level and more-detailed strategies and goals when questions arise about "why" some specific thing is being done;
3. It creates a clearer distinction between the aspects that belong in policy documents (direction setting), procedural requirements (process setting), and accepted standards (where mission-agnostic features meet mission-specific details); and
4. It creates a machine-readable taxonomy that lends itself to machine-assisted planning and semantic reasoning.

3.2. Risk-informed Safety Efforts

All of the activities during Planning and Implementation should be "risk-informed." That is, SMS activities must be responsive to reality; as issues and challenges arise, they are managed as part of the Risk Management process and may result in modifications to details of SMS implementation. This ability to be responsive, and "tailor", is at the heart of SMS.

In this sub-section, the authors focus on one particular aspect of risk-informing at the more detailed level, acknowledging the tie to the high-level risk posture setting that is discussed in the prior sub-section. This aspect is how risk-informing relates to initially picking the modelling and simulation tools and associated empirical evidence that are best suited to the task at hand, and how this should map into decisions about ensuring this information aligns with the as-designed, as-built, and as-operated system through related activities like hardware quality assurance, software assurance, and validation and verification. The starting point for this flow-down is the previously-mentioned Assurance Implementation Matrix, where the payload risk classification is first translated in to the requirements tailoring activities in the related areas (like reliability and maintainability). Work will be done in these other areas irrespective of Nuclear Flight Safety, so the point here is to focus on how the needs of Nuclear Flight Safety should and could interface with the already ongoing work centric to these areas.

Contemporary terrestrial nuclear safety approaches cover a broad range of deterministically-oriented to probabilistically-oriented approaches, and likewise span a range of enveloping-oriented to best-estimate-with-uncertainty approaches. In general, lower intrinsic radiological hazard activities that necessitate highly-consistent use in a broad range of applications lend themselves well to enveloping and deterministic approaches. The IAEA Q-system is an example of this [21], wherein offline analyses are performed using a number of stylized assumptions in order to compute A2 values on a radioisotope-specific basis to generate normalization factors useful in calibrating the degree of hazard in a generic land, sea or air transport situation. Moving in the general direction of higher potential intrinsic hazard and somewhat more case-specific, DOE-STD-3009 provides a largely deterministic approach for performing documented safety analyses for DOE non-reactor facilities, leveraging general features of all facilities (e.g., the existence of a standoff distance to the general public) in creating a robust and quasi-generic approach. Moving in the general direction of lower intrinsic hazard but with the added complexity of space launch, [22] presents a particular example of using low-fidelity scoping risk assessment methods to make an enveloping determination for the categorical relief threshold below which review and approval of radioactive material launch or reentry by NASA headquarters is not required. And finally, moving to the higher hazard and higher-fidelity side of things, the nuclear safety analyses for space nuclear system launches over the past two decades has migrated toward a highly-case-specific simulation-based probabilistic risk assessment approach. As the pedigree and complexity of the analysis increases, so do the required resources. For this reason, it is important to calibrate the scope and fidelity of the analytical approach, and the underlying confirmation of the goodness of the analysis, to the actual risk of the situation.

Assessing this risk calibration is conceptually the same for all space nuclear systems, but the primary factors that will influence the situation do differ between radioisotope power systems and reactors since the likely dominant sources of accident risk differ. It is possible to create general guiderails for steering (i.e., tailoring) up-front decisions about modelling scope and fidelity using primary factors as rating factors, where the primary factors are judged based on past experience and preliminary design. Examples of primary factors could be things like the likelihood of the accident environment defeating all engineered safety barriers given the anticipated accident environments (for radioisotope power systems), the fission product buildup during in-space operation and any subsequent decay prior to Earth reentry (for an Earth-orbiting reactor), or a prescribed standoff distance of potential receptors during launch and ascent phases (for either technology). Doing so would make this decision-making more repeatable and reliable. A standard in the area of safety and risk analysis methods for space reactors has been proposed [17], and that effort may find it worthwhile to include this type of analytical scaling in to such a standard.

Once the needed initial scope and fidelity of the nuclear safety analysis has been determined, the system and mission developers can then focus on how to best pull evidence from the activities in other disciplines (e.g., range safety, hardware quality assurance, etc.) to support the validation and verification of the nuclear safety analysis itself. Clearly this will need to be an iterative process. By its nature, risk assessment leads to an evolving understanding of the key drivers of risk, and the modelling and simulation approach will need to adjust to this evolution by reducing effort in areas that have been shown to not dominate risk and re-focus those resources on emerging contributors to risk. Using MBSE tools to manage modelling and simulation metadata across all disciplines can greatly enable this effort.

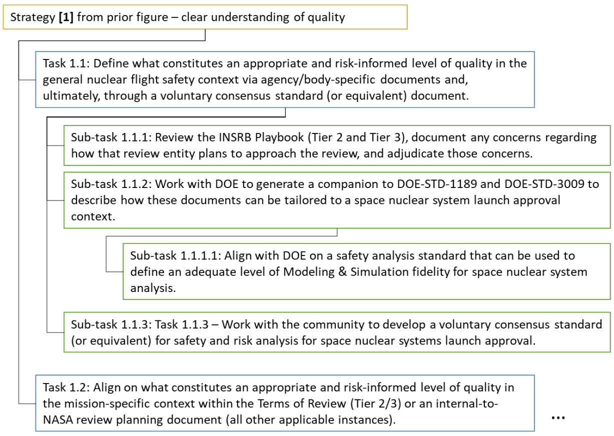
Ultimately, these activities can be better married if they are all leveraging a common standard for the selection and management of the S&MS analysis. Doing so, along with focusing efforts to make the analyses in differing disciplines be as interoperable as possible (e.g., through over-arching analysis framework and interface definitions) would also facilitate an integrated approach to analysis management. Beyond the selection and management of the S&MS analysis approaches, the outputs of that analysis need to be managed within the life cycle. Incorporation of S&MS analysis into the S&MS assurance case in a manner that is fully compatible with NASA's systems engineering approach to requirements and life cycle management is the subject of other ongoing work [20]. Finally, using a common framework for measuring the goodness of the models (such as NASA-STD-7009 [23]) across the varying disciplines would significantly help compatibility.

3.3. Tools for Safety Case Development and Management

The final part of the triad to discuss is the "case assured" component. Assurance cases encompass the safety case and other elements of mission success. Here, we will focus on the Nuclear Flight Safety case as an element within a broader assurance case. We'll also use this opportunity to dive deeper into the model-based interests and the use of ontologies to enable machine-assisted activities. A more general discussion of assurance cases as a philosophical approach to evolving Nuclear Flight Safety is presented in [14]. The use of these techniques in nuclear safety is not novel. For instance, Smith et al. [24] present a survey of the use of artificial intelligence and machine learning exploration in the nuclear community, including a taxonomy of approaches, tasks, applications, and explainability under the machine learning umbrella. The same reference also summarizes ten areas of expected future exploration, of which many apply equally to the space nuclear domain. Nevertheless, the present paper focuses on uses that support S&MS functions.

Fig. 1 provided an overview of how safety frameworks map down to mission-specific activities. Fig. 3 illustrated how S&MS policy tenets map to strategies for Nuclear Flight Safety. Fig. 5 demonstrated an example mapping of the nuclear safety review strategy to a subsidiary goal and 5 supporting strategies. We'll now drill down this leg of the hierarchy / assurance case to a level where actionable tasks produce evidence to support the safety case. Fig. 6 shows this drill-down for the first of the five nuclear safety review strategies, addressing the role of agreements, standards, and tool selection (including aspects that tie back to the previous discussion about S&MS Analysis Management). In this context, the safety analysis tools serve as a type of "digital twin" for how the system will behave under accident conditions, where that twin may be of low or high fidelity depending on what is needed to support the assurance case.

What is exciting about machine learning in this context is that if the standards and tools are developed using common ontologies and interoperable frameworks, then the task of assessing the outcome for correctness and completeness becomes something that semantic reasoning can address. To be clear, the idea is not to remove the human from the assessment loop, but rather to produce machine-generated insights that can guide the human to the areas where there are apparent gaps or errors based on semantic reasoning.



Strategy **[1]** from prior figure – clear understanding of quality

Task 1.1: Define what constitutes an appropriate and risk-informed level of quality in the general nuclear flight safety context via agency/body-specific documents and, ultimately, through a voluntary consensus standard (or equivalent) document.

Sub-task 1.1.1: Review the INSRB Playbook (Tier 2 and Tier 3), document any concerns regarding how that review entity plans to approach the review, and adjudicate those concerns.

Sub-task 1.1.2: Work with DOE to generate a companion to DOE-STD-1189 and DOE-STD-3009 to describe how these documents can be tailored to a space nuclear system launch approval context.

Sub-task 1.1.1.1: Align with DOE on a safety analysis standard that can be used to define an adequate level of Modeling & Simulation fidelity for space nuclear system analysis.

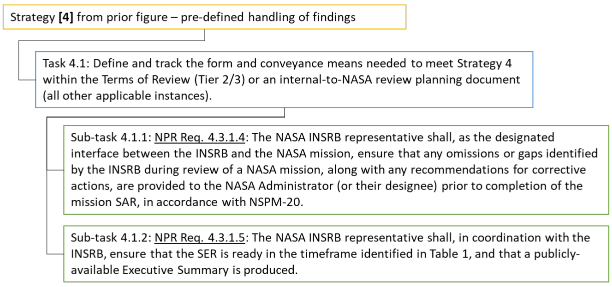
Sub-task 1.1.3: Task 1.1.3 – Work with the community to develop a voluntary consensus standard (or equivalent) for safety and risk analysis for space nuclear systems launch approval.

Task 1.2: Align on what constitutes an appropriate and risk-informed level of quality in the mission-specific context within the Terms of Review (Tier 2/3) or an internal-to-NASA review planning document (all other applicable instances).

…

Figure 6 – Drill-down for Nuclear Safety Review Strategy #1

Fig. 7 shows a partial drill-down of Strategy #4 from Fig. 5 to illustrate how the assurance case can explicitly include requirements, in this case requirements that exist in the current version of NASA NPR 8715.26. This supports a focus area of data representation in the current work and is another area in which a SysML model of the relevant requirements document can interface with the assurance case. Meanwhile, Fig. 8 shows a partial drill-down of Strategy #5 from Fig. 5 to illustrate another specific area where ontologically-enabled and model-based machine learning can directly contribute to the assurance case. In this instance, ontology and semantic reasoners have a particularly strong advantage in being able to parse through decades' worth of past analysis to identify those pieces of information that are most worth a reviewers' time to consume in preparing for and executing a nuclear safety review. The key enabler is the ability to establish pre-defined terminology and relationships such that a machine can make indirect inferences about the context and relevance of this past information. Put simply, a well-crafted data analysis tool leveraging ontologies and semantic reasoning has the ability to take the hundreds of thousands to millions of pages of potentially-relevant past space nuclear system analyses and separate out the useful pieces from the extraneous pieces for a given topic of interest, potentially also leveraging learning algorithms to help deal with the nuances and idiosyncrasies that are resistant to first-order inference. This is equivalent to the use of these same techniques in everyday aspects of our lives, like identifying the three quickest driving routes to present to a driver or identifying the top 100 relevant webpages in a rank-ordered list based on anticipated relevance. Again, the point is not to remove the human from the review, it is to arm the human with the relevant information with less human resources expended.



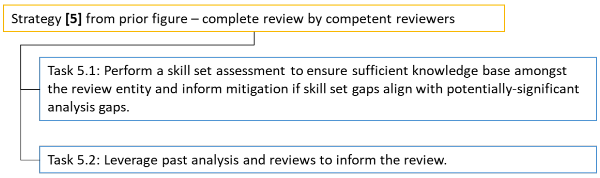
Strategy **[4]** from prior figure – pre-defined handling of findings

Task 4.1: Define and track the form and conveyance means needed to meet Strategy 4 within the Terms of Review (Tier 2/3) or an internal-to-NASA review planning document (all other applicable instances).

Sub-task 4.1.1: NPR Req. 4.3.1.4: The NASA INSRB representative shall, as the designated interface between the INSRB and the NASA mission, ensure that any omissions or gaps identified by the INSRB during review of a NASA mission, along with any recommendations for corrective actions, are provided to the NASA Administrator (or their designee) prior to completion of the mission SAR, in accordance with NSPM-20.

Sub-task 4.1.2: NPR Req. 4.3.1.5: The NASA INSRB representative shall, in coordination with the INSRB, ensure that the SER is ready in the timeframe identified in Table 1, and that a publicly-available Executive Summary is produced.

Figure 7 – Partial Drill-down for Nuclear Safety Review Strategy #4



Strategy **[5]** from prior figure – complete review by competent reviewers

Task 5.1: Perform a skill set assessment to ensure sufficient knowledge base amongst the review entity and inform mitigation if skill set gaps align with potentially-significant analysis gaps.

Task 5.2: Leverage past analysis and reviews to inform the review.

Figure 8 – Partial Drill-down for Nuclear Safety Review Strategy #5

4. ONGOING AND PLANNED WORK

The authors are currently working on a Nuclear Flight Safety case study for ontologically-enabled and model-based approaches in this discipline. This case study will inform broader activities toward evolving the safety and mission success arena to being more objectives-driven, risk-informed, and case-assured, by marrying it with ongoing case studies like the reliability and quality-led exploration of objectives-driven and software (in this case APPG)-enabled approaches and the planetary protection-focused exploration of assurance cases. Fig. 8 illustrates the point that this is one step along an arc that connects the past paper-centric approach to a more digitally-centric future.

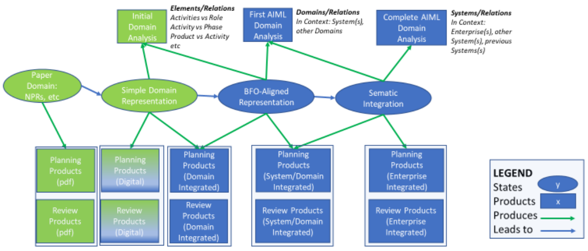

Initial Domain Analysis
Elements/Relations
Activities vs Role
Activity vs Phase
Product vs Activity
etc
First AIML Domain Analysis
Domains/Relations
In Context: System(s), other Domains
Complete AIML Domain Analysis
Systems/Relations
In Context: Enterprise(s), other System(s), previous Systems(s)
Paper Domain: NPRs, etc
Simple Domain Representation
BFO-Aligned Representation
Sematic Integration
Planning Products (pdf)
Review Products (pdf)
Planning Products (Digital)
Review Products (Digital)
Planning Products (Domain Integrated)
Review Products (Domain Integrated)
Planning Products (System/Domain Integrated)
Review Products (System/Domain Integrated)
Planning Products (Enterprise Integrated)
Review Products (Enterprise Integrated)
LEGEND
States
y
Products
x
Produces
Leads to

Figure 9: Representation of Evolution from Paper-centric to Digital

In this Nuclear Flight Safety case study, the drill-down presented earlier in this paper is being leveraged (i.e., the mapping from S&MS policy tenets to Nuclear Flight Safety requirements-oriented strategies to

Nuclear Flight Safety supporting element goals and strategies to nuclear safety review sub-strategies and tasks. This information is being mated with sysML representations of the requirements document(s). From there, the concepts of semantic web technology and basic formal ontology are being introduced. Ontologies are a specification of a conceptualization. Semantic web technology is an evolution past relational databases which uses ontological statements, uniquely-designed query tools, multi-dimensional relationships, and specific formulations of logic and uniqueness to allow for automated checks of correctness, completeness, and consistency across data from multiple sources. Reference [25] presents a useful "stack" illustrating how elements like syntax, data interchange, taxonomies and querying build toward fundamental attributes of proof and trust.

The key identified needs that the authors are attempting to tackle are:

- Data integration and interoperability between tools and organizations (internal and external),, knowing what data to "trust," and understanding data relationships (what aspects are inter-related and how).
- Data representation – viewing data in different ways to inform decisions.
- Data correctness and completeness – checking unit;
- Leveraging knowledge across an organization and across engineering disciplines to achieve better and more consistent decision-making and better context around why a particular decision was made.

These technologies are being approached within the W3C formulation and associated W3C standards, and include Resource Description Framework (RDF), as a general method for describing information; RDF Schema (RDFS); Simple Knowledge Organization System (SKOS); SPARQL, an the RDF query language; Notation3 (N3), designed with human-readability in mind; N-Triples, as a format for storing and transmitting data; Turtle (Terse RDF Triple Language); Web Ontology Language (OWL); and Rule Interchange Format (RIF). It is all those things working together to reason and provide meaning to data that achieves the goal of semantic web technology.

While ontologies have been around for many years the formalization and utilization of systems of ontologies in semantic web technology is a more recent concept that is requiring refactoring and development of ontologies that are aligned with a common upper ontology. Other elements of semantic web technology are generally more mature. Ontologies are not, however, a silver bullet. In some instances they have failed to deliver on expectations due to lack of interoperability, lack of extendibility, or lack of alignment to a Top-Level Ontology. The authors are sensitive to this past experience in the current work. For example, the authors are attentive to establishing workable ontology hierarchies, wherein a Domain (low-level) Ontology is aligned with the Top Domain (mid-level) Ontology, which is in turn aligned with the Top-Level Ontology. Adhering to such a hierarchy is critical to ensuring that what is achieved in the Nuclear Flight Safety domain is ultimately compatible across organizations and across disciplines. The authors have already selected the Basic Formal Ontology [26] as the Top-Level Ontology and are exploring extension of the work in [27] and [28].

Current effort is focused on the goal of demonstrating an ability to usefully employ ontologies and semantic reasoning in the Nuclear Flight Safety domain (as an example S&MS domain), by:

- Further defining the Nuclear Flight Safety use case (i.e., further refining the related assurance case, SysML-oriented requirements representation, etc.);
- Developing the semantic framework to execute the Nuclear Flight Safety use case;
- Developing the domain ontology and supporting ontologies for demonstration, leveraging existing ontologies where possible (e.g., [29]);
- Developing SysML models that facilitate interrogating and understanding the underlying knowledge.

Follow-on work would then embed the above capability within a broader assurance case and objectives hierarchy ontology to enable more extensive reasoning for Nuclear Flight Safety applications, implicate associated tools (e.g., APPG) within this framework, expand computing usage to enable complex reasoning of high-density data, implement robust triple stores to allow capability to execute and reason about more data, develop rules and queries to perform higher level semantic reasoning and enable more capabilities related to this particular use case, and develop tool ontologies to pull in needed data from other tools. A final phase would then be to expand this capability and these formulations and tools to other S&MS disciplines. The above represents the forward work in this area, to be reported on at a later date.

5. REFERENCES

1. NPD 8700.1F, NASA Policy for Safety and Misison Success, July 2022.

2. NPD 1000.0C, NASA Governance and Strategic Management Handbook, Jan. 2020.
3. NPR 7123.1C, NASA Systems Engineering Processes and Requirements, Feb. 2020.
4. NPR 7120.5F, NASA Space Flight Program and Project Management Requirements, Aug. 2021.
5. U.S. Department of Defense, Digital Engineering (DE) Strategy, Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Washington, DC, 2018.
6. NASA Enterprise Digital Transformation Initiative Strategic Framework & Implementation Approach, NASA/TM–20220018538, Dec. 2022.
7. DOE-STD-1189-2016, Integration of Safety into the Design Process, Dec. 2016.
8. DOE-STD-3009-2014, Preparation of Nonreactor Nuclear Facility Documented Safety Analysis, Nov. 2014.
9. ASME/ANS RA-S-1.4-2021, “Probabilistic Risk Assessment Standard for Advanced Non-Light Water Reactor Nuclear Power Plants,” Feb. 2021.
10. National Security Presidential Memorandum No. 20, Presidential Memorandum on Launch of Spacecraft Containing Space Nuclear Systems, Washington D.C., Aug. 20, 2019.
11. Memorandum on the National Strategy for Space Nuclear Power and Propulsion (Space Policy Directive-6), Washington, D.C., Dec. 16, 2020.
12. UN Office of Outer Space Affairs, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, 1967.
13. UN Committee on the Peaceful Uses of Outer Space Scientific and Technical Subcommittee and IAEA, Safety Framework for Nuclear Power Source Applications in Outer Space. United Nations Report A/AC.105/934, Vienna, May, 2009.
14. Forsbacka, M., and D. Helton, “Evolution of NASA's nuclear flight safety program to infuse risk leadership and assurance framework concepts,” Journal of Space Safety Engineering, Volume 10, Issue 1, pg. 95-102, March 2023.
15. NASA NPR 8715.26, Nuclear Flight Safety, Feb. 3, 2022.
16. Department of the Air Force, “Nuclear Safety Review and Launch Approval for Space or Missile Use of Radioactive Material.” DAFMAN-91-110, Feb. 24, 2022.
17. NASA/TM−20220004191, “Report of the Interagency Space Reactor Standards Working Group,” March 2022.
18. F. Groen, J. Evans, and A. Hall, A Vision for Spaceflight Reliability: NASA’s Objectives Based Strategy, IEEE, 2015, Feb. 2015.
19. J. W. Evans, et al., "Enabling Assurance in the MBSE Environment," 2020 Annual Reliability and Maintainability Symposium (RAMS), Palm Springs, CA, USA, 2020, pp. 1-7.
20. H. Dezfuli, et al., Modernizing NASA’s Space Flight Safety and Mission Success (S&MS) Assurance Framework In Line With Evolving Acquisition Strategies and Systems Engineering Practices, NASA/TM-20220003490, June 2021.
21. IAEA, SSG-26, Advisory Material for the IAEA Regulations for the Safe Transport of Radioactive Material (2012 Edition), 2012.
22. D. Helton and M. Witmer, Technical Basis Related to the Posture of NASA’s Office of Safety and Mission Assurance for the Launch of Radioactive Material Other than Space Nuclear Systems: Volume 1–Overview of Analysis and Results, NASA/TM-20230002528, Feb. 22, 2023.
23. NASA-STD-7009, “NASA Standard for Models and Simulations,” Dec. 2016.
24. Smith, C., Rashdan, A., and V. Agarwal, Using the New Math: Artificial Intelligence and Machine Learning Applications for the Nuclear Power Industry, Nuclear News, American Nuclear Society, June 2022.
25. P. Moder, H. Ehm, and E. Jofer, A Holistic Digital Twin Based on Semantic Web Technologies to Accelerate Digitalization, in *Digital Transformation in Semiconductor Manufacturing*, May 2020.
26. ISO/IEC 21838-2:2021, Information technology – Top-level ontologies (TLO) – Part 2: Basic Formal Ontology (BFO), 2021.
27. T. Hagedom et al., Knowledge Representation with Ontologies and Semantic Web Technologies to Promote Augmented and Artificial Intelligence in Systems Engineering, *Insight*, Vol. 23, Issue 1, pg. 15-20, Mar. 2020.
28. M. Bone et al., Toward an Interoperability and Integration Framework to Enable Digital Thread, *Systems,* 2018, 6(4), 46, Dec. 18, 2018.
29. A. Al Rashdan, J. Browning, and C. Ritter, Data Integration Aggregated Model and Ontology for Nuclear Deployment (DIAMOND): Preliminary Model and Ontology, INL/EXT-19-55610, Sept. 2019.