Overview of Past Space Nuclear Reactor Functional Safety Principles in the Context of Recent Policy Changes

Donald Helton[1], Lee Mason[2], and Matthew Forsbacka[1]

[1]National Aeronautics and Space Administration (NASA) Headquarters, 300 E Street SW, Washington, DC, 20546
[2]NASA Glenn Research Center, 21000 Brookpark Road, Cleveland, OH 44135

Primary Author Contact Information: 202-358-0311, donald.m.helton@nasa.gov

[Placeholder for Digital Object Identifier (DOI) to be added by ANS]

Space nuclear reactor technology development and associated approaches to safety have been ongoing for over 60 years. This paper selects functional safety principles associated with space reactors at several points in time since the early 1980s and provides an overview of their general content, similarities, and differences, as well as how they have evolved. It also reflects, where applicable, on how recent Federal policies in the area of space nuclear systems may affect how these safety principles apply to future activities.

I. BACKGROUND

Safety directives for space nuclear reactor activities, including those found in National Aeronautics and Space Administration (NASA) Procedural Requirements (NPR) 8715.26 (Ref. 1), typically requires that nuclear safety considerations be considered during all phases of system and mission development and execution. However, historically the radiological risk assessment model used to support the safety case for nuclear flight safety and launch authorization has been developed during a period of time spanning 3 to 1 years prior to scheduled launch, though a launch vehicle-focused risk assessment is typically available earlier. This means that a draft of the radiological risk assessment sufficient for providing risk insights related to nuclear flight safety is not typically available until roughly 2 years prior to scheduled launch. Virtually all major design decisions for both the system and the mission have already been made by this time. As such, projects often make these system and mission design decisions based on risk trades that do not directly utilize the radiological risk assessment (though insights from past risk assessments can be used, when applicable). For this reason, deterministic functional safety principles are often used to ensure that broad nuclear flight safety interests are considered at these earlier stages.

As described in the 2015 Nuclear Power Assessment Study[2], "Before the design of a U.S. space nuclear system can proceed in earnest, clear safety criteria must be in place to guide designers and mission planners." Such criteria have been used throughout the decades of development of radioisotope power systems (RPS). Space reactor development efforts have also typically relied on such criteria. A structured approach (adapted from (Ref. 3)) to safety may involve steps like:

1. Establishing a safety philosophy and risk posture for the mission;
2. Establishing the unique safety issues relevant to the mission and a strategy for addressing those issues;
3. Establishing a minimum set of intent-based safety principles that can address those safety issues and promote eventual conformance with the National Security Presidential Memorandum (NSPM)-20 (Ref. 4) Safety Guidelines and the tiering criteria for the intended NSPM-20 tier level, along with other requirements; and
4. Establishing binding design and operational safety specifications to guide effort and assure safety.

The first two items are not addressed here; they are higher-level than this survey paper and would be generally consistent with both NASA's risk leadership philosophy[5] and the approach to terrestrial nuclear safety.[6, 7, 8] Rather, this paper focuses on the third item. The specifications described in the fourth item would ultimately be developed by the performers of a particular project to meet the prescribed principles and objectives. This paper specifically does not deal with purely mission success aspects, such as interoperability with other systems, ease of maintenance, etc. This paper focuses solely on safety topics.

II. PAST RESOURCES SURVEYED

A review of past work[3,9,10,11,12,13] was performed, aided by other recent survey work.[14,15] Consideration of safety principles and design criteria dates back to the 1960s, and some concepts (such as the need to prevent inadvertent criticality and the use of a destruct system to manage this risk) date back to the Rover/Nuclear Engine for Rocket Vehicle Application (NERVA) program. Nevertheless, the current paper primarily focuses on activities since the early 1980s.

A total of 10 categorical areas were defined for dissecting the total material of interest. Each categorical area is discussed in a dedicated sub-section in the following section. In all cases this paper relates to a given topic in the context of the space nuclear system-enabled mission, not the (typically) much broader discipline. For instance, planetary protection is only considered specific to radiological aspects (be it thermal effects or ionizing radiation effects). This survey is not comprehensive. The sources reviewed and further discussed below do cover other topics, such as safeguards in the event of an intact reentry, which are generally not covered here.

III. OBSERVATIONS AND DISCUSSION

III.1 Launch Vehicle Selection

Launch vehicle selection is notably missing from almost all sources reviewed. This is in large part because past space reactor efforts have often not made it from the technology maturation and system development stage to the flight opportunity stage. Yes, of the three mishaps involving U.S. space nuclear systems that occurred between 1964 to 1970, two of the three involved launch vehicle failures (the Transit 5BN-3 navigational satellite failing to reach orbit and subsequently re-entering Earth's atmosphere and the Nimbus B weather satellite launch abort).[16] Later, in the 1980s, concerns over launching space nuclear systems aboard the Space Transportation System (Shuttle) following the Challenger accident caused significant re-evaluation and some design changes prior to launch of the Galileo and Ulysses missions aboard STS.

NASA's process for risk classification for NASA payloads[17] does not tie risk classification to the presence of radioactive or nuclear material, though there is some natural correlation between the other characteristics (e.g., complexity, cost) and the use of a space nuclear system. In other words, there is a large degree of natural harmony between a flight using a space nuclear system and the type of flight that will have less risk tolerance. Meanwhile, NASA's spaceflight program and project management requirements[18] do contain an explicit tie in this regard, in that missions subject to NSPM-20 must be Project Category 1 (the least risk-tolerant category).

Meanwhile, for missions subject to NASA's launch services risk mitigation policy[19] there is an indirect consideration specific to space nuclear systems, and a mission could fly on a Category 2 launch vehicle (the middle risk-tolerant category), if it were Risk Class B or C. For NASA involvement in a commercial launch, the specific language used in the acquisition would apply and its acceptability would be subject to the Federal Aviation Administration's licensing determination.

The characteristics of launch vehicle safety that are relevant for space reactor systems will differ somewhat from those for RPS. For space reactor systems, inadvertent criticality following a launch mishap is traditionally the primary concern for the ascent phase. Nevertheless, the probability of a launch vehicle mishap will have a fairly direct effect on the probability of a radiological release (if it is determined that a radiological release is a credible accident during ascent), and it will directly affect the estimation of exceedance measures for comparison to NSPM-20's Safety Guidelines. For this reason, a safety principle that explicitly considers the vehicle's reliability should be considered.

III.2 Launch Site and Launch Trajectory Selection

Similar to the situation for launch vehicle selection, almost none of the documents reviewed explicitly addressed launch site selection or launch trajectory selection. The selection of these launch characteristics are naturally driven toward areas involving low population densities due to flight safety aspects other than radiological (toxics, over-pressure, and debris). These same drivers will usually serve to reduce radiological safety risks.

Again, for a space reactor system, inadvertent criticality is traditionally the major accident type of concern during the launch and ascent phases, with deformation during land impacts or excess moderator intrusion during water impacts being underlying modes. Due to the degree of natural harmony between radiological and non-radiological drivers in this area, and the likelihood that geopolitical and security risks may be drivers, it isn't clear that a safety principle in this area is warranted. Feasibility of recovering the system after a failed launch may also be a consideration.

III.3 Testing, Assembly, and Launch Operations

Up front, the authors acknowledge that this sub-section blends several sub-topics that it would make sense to separate in a more detailed review, such as nuclear fuel qualification, safety testing (validation), assembly operations, post-assembly system or sub-system testing (verification), and launch operations.

Regarding aspects of ground testing related to fission product build-up, past development efforts have established the practice of explicitly considering the generation of fission products during ground testing as a key means of limiting the radiological release if a launch mishap occurs. These past efforts[9,11,3] used similar terminology to describe the balance between ground testing (typically assumed to be zero-power critical testing), decay time prior to launch, and ensuring further operation doesn't occur until the device is in-space.

These philosophies were later encoded more succinctly as "The reactor shall not be operated prior to space deployment, except for zero-power testing on the ground, for which negligible radioactivity is produced."[15]

At this point it seems unlikely that anyone will propose launching a radiologically "hot" reactor, and so the issue comes down to how much fission product buildup is satisfactory. In the post-NSPM-20 era, a yardstick for this is the contribution of accidents involving dispersal of fission products in the absence of an inadvertent criticality and prior to intentional operation, measured against the NSPM-20 Safety Guidelines. Such an assessment is difficult to perform until other aspects of the system and mission have been defined, and until a system/mission risk assessment has been developed. Additionally, no consensus approach for performing this analysis has been developed. Nevertheless, the means for performing scoping assessments in this area are well understood, and it should be possible to perform coarse accident impact assessments assuming different "cold" reactor source terms. The outputs of such assessments will probably show monotonically increasing individual doses as the fission product inventory is increased, which may make selection of a specific 'tipping point' difficult. However, one can choose a figure-of-merit to constrain this aspect of the trade space, such as 'no credible accident will lead to an individual dose that is more than 25 mrem' (the limit for more frequently-anticipated accidents in the NSPM-20 Safety Guidelines). It may turn out that the launch safety considerations are less constraining than the ground handling and transportation requirements. The amount of time that the fission system is stored prior to transport will have an effect on the inventory of short-lived fission products such as I-131 (8 day half-life), but will have little effect on the inventory of longer-lived fission products such as Cs-137 (30 year half-life).

Regarding criticality safety for ground testing, again, the relevance of this topic has been long-established, with the SP-100 program codifying that, "The reactor systems contractor shall specify in the detailed technical safety specification…the minimum shutdown reactivity during assembly/testing, ground handling/storage, transportation, launch."[9] Criticality safety during ground testing will be dictated by the terrestrial regulatory or authorization process governing the facility used (Department of Energy (DOE), Department of Defense (DoD), or Nuclear Regulatory Commission (NRC)). This process may impose constraints on the system design or test that have both harmonizing and conflicting effects on launch safety. Any competing effects will need to be identified, assessed, and adjudicated within the terrestrial regulatory or authorization process. Exceptions to terrestrial requirements may be possible when properly justified, but the lack of precedents may complicate such efforts.

Regarding sub-system and system verification, terrestrial nuclear and space non-nuclear verification requirements may be readily applied, though some conflicts are possible. Past programs have provided empirical information through full-scale destructive examination for highly-enriched uranium (HEU) designs that may be difficult to reproduce for high-assay low-enriched uranium (HALEU) designs, such as the testing performed during the Systems for Nuclear Auxiliary Power (SNAP) program.[11]

General information and tenets are available in a couple of the reviewed sources[9,11], but this area would particularly benefit from an accepted standard development activity, such as the one recommended recently by an Interagency Space Reactor Standards Working Group.[20]

III.4 Inadvertent Criticality After A Flight Accident

Inadvertent criticality is one of the two primary contributors to flight radiological risk based on past risk assessments (alongside reentry of a "hot" reactor). All past space reactor programs used HEU fuel, which generally relies on "fast" (higher energy than thermal) neutrons to maintain the nuclear chain reaction. Due to this, submersion of the reactor in a fluid (with that fluid serving as a moderator – i.e., a medium that slows down fast neutrons via scattering interactions) does not have a large effect in promoting that chain reaction. This means that HEU-fueled reactors, in general, are less susceptible to inadvertent criticality. HALEU-fueled reactors, on the other hand, rely more heavily on thermal neutrons to support the chain reaction. When submersed, the surrounding fluid tends to slow down neutrons and promote the nuclear chain reaction. For this reason, addressing inadvertent criticality events in HALEU-fueled reactors will differ at the detailed level, relative to addressing inadvertent criticality events for HEU-fueled reactors. Nevertheless, at the functional safety principle level, some of the information translates.

The SP-100 program had several design tenets to address this risk[9] such as "The reactor shall have a significantly effective negative power coefficient of reactivity," and "The reactor shall be designed so that no credible launch pad accident, range safety destruct actions, ascent abort or reentry from space resulting in Earth impact could result in a critical or supercritical geometry."

Later work[11] describes, "Should inadvertent criticality occur, its effects are manifold. Not only does it generate a fission and activation product inventory, it produces a substantial, usually short duration neutron and gamma radiation field. Under certain circumstances, it can also cause thermal or mechanical disassembly of the reactor. An inadvertent criticality therefore has the potential to create and disperse radioactive materials and generate a short-duration, high-intensity radiation field."

The general features considered in past programs to address this risk included: incorporating thermal neutron absorbers into the reactor core (e.g., poison wires); constructing the reactor to limit core deformation during impacts, or during reentry (e.g., inclusion of a reentry aeroshell); and deliberate separation or disassembly of the reactor during a flight abort.

Regarding the latter approach, it is non-intuitive to destruct a nuclear device as part of a safety approach, and this concept relies on the reactor having minimal fission products (as discussed earlier in the context of ground testing). Such a strategy should balance the risks (as opposed to merely the consequences) from human health exposure associated with an inadvertent criticality accident versus dispersal of radioactively "cold" uranium.

Later work[3] went on to summarize the work-to-date as of 2005 to support a conclusion that during launch, ascent and prior to on-orbit operation, the reactor must be radioactively "cold," must be positively shutdown (with adequate shutdown margin provided), and criticality must be precluded for all credible accidents and accident environments that could occur. A more recent study states this more simply by stating that inadvertent criticality shall be avoided for both normal conditions and credible accident conditions.[14]

Using this type of blanket approach for HALEU-fueled space reactors would require careful consideration of how it limits the trade space, given that:

- Natural limitations in criticality control will be less effective for over-moderated conditions;
- Destruct systems will naturally have practical limitations in their engineered reliability;
- Introduction of greater quantities of poison material into the core will generally tend to decrease reliability of the reactor itself once in-space; and
- The transient neutron population during these circumstances can be complex (both analytically and in reality).

Regarding the latter point, it is conceivable for inadvertent criticality events to take three basic forms:

- A quasi-steady critical configuration where the reactor steadily produces fission products and in which competing effects keep reactor k-effective close to 1.0;
- A super-critical or prompt critical configuration that leads to thermal runaway (fuel melt) or mechanical disassembly (energetic break-apart) of the reactor;
- A configuration that results in periodic return-to-power of the reactor as competing effects oscillate between sub-critical, critical, and/or super-critical states.

All three are relevant, and all three have differing impacts on radiological exposures and recovery operations.

Inadvertent criticality events have the potential to create lethal radiation fields to very close-in receptors, and so it can be difficult to conclude that the maximum individual dose will be less than 25 rem in all circumstances. Rather, projects are presently looking to use a range of design options to limit the likelihood of such accidents to levels below those associated with the NSPM-20 Safety Guidelines.[15]

Such an approach, if successful, would illustrate to a decision maker that the design is "safe enough" by the standards of NSPM-20, "the probability of an accident resulting in exposure in excess of 25 rem TED to any member of the public does not exceed 1 in 100,000." (Ref. 4) The lack of a consensus standard for performing safety and risk analyses for comparison against the NSPM-20 Safety Guidelines is a recognized gap.[20] Also, it would be necessary to demonstrate an additional order-of-magnitude reduction in likelihood to avoid triggering elevation of the nuclear launch authorization to the Executive Office of the President, given the 1 in 1,000,000 Tier III criteria in NSPM-20 (Ref. 4). An example of a scoping risk assessment for a generic HEU reactor focused on the risk from inadvertent criticality can be found in (Ref. 21).

Finally, decisions made in this area will have direct effects on payload safety (e.g., the relationship between in-core poison material for flight safety relative to hazard controls for ground safety) and range safety (e.g., introducing complexity into the flight destruct system to ensure reactor breakup). This infers that risk trades may need to be made between payload, range, and flight safety, thus further promoting the benefit of accepted standards in how flight safety is conducted.

III.5 Inadvertent Reentry of a "Hot" Space Reactor

The other primary risk driver (relative to affecting human health on Earth) from past space reactor risk assessments is the inadvertent reentry of the space reactor after it has operated (or inadvertently gone critical) on-orbit. Past programs have established the precedent of not commencing (or planning to commence) reactor operation until the flight system is in a stable orbit, starting with the actual operation of the SNAPSHOT reactor in 1965. The approach for SP-100 evolved, and eventually became[11] "Key safety and design selections that influenced development of the SP-100 safety and safety test program were intact reentry and, for selected missions, retention of reactor geometry for permanent disposal…These selections [aforementioned plus precluding criticality during all credible accidents] and supporting safety analyses led to the inclusion of a reentry cone and internal safety rods that must be retained during accidents. In systems above about 500 kWt, an auxiliary cooling loop is provided if the mission requires high confidence for the retention of core geometry for disposal."

Later work[11,3] carried forward the SP-100 tenets with regard to operation, orbital mechanics, and maintenance/verification of a "Nuclear Safe Orbit." Meanwhile, more recent work[14] proposed that planned radiologically hot reentry be precluded from mission profiles and for any credible radiologically hot reentry accident, the reactor fuel shall reenter essentially intact, or alternatively, shall result in essentially full dispersal at high altitude. For the DRACO program and as of May 2022 (Ref. 15), the following (draft) proposal was made: "GDC-3: The radiological risk to the public from the accidental hot re-entry of a reactor shall be prevented in accordance with the risk criteria in NSPM-20... For hot reentry, the primary method for meeting the risk criteria is through the mission and operational parameters."

As with inadvertent criticality, it will be difficult to preclude the accident altogether, and rather is likely to be framed in terms of determining that the accident is so unlikely as to be non-credible (long-term disposal is discussed later), or that it otherwise meets the NSPM-20 Safety Guidelines. Again, the lack of accepted standards for computing the risk and making comparison to NSPM-20 Safety Guidelines is problematic, and the need for work in this area is recognized.[20]

Also relevant to hot reentry are the requirements in Space Policy Directive 6 (SPD-6) related to the operation and disposition of SNPP systems, and specifying space reactors "may be operated on interplanetary missions, in sufficiently high orbits, and in low-Earth orbits if they are stored in sufficiently high orbits after the operational part of their mission." It goes on to describe what constitutes a "sufficiently high orbit" in broad terms related to fission product decay, orbital debris, and the requirement for a "highly reliable operational system to ensure effective and controlled disposition of the reactor."[22]

This language adapts a tenet in the 1992 United Nations Safety Principles[23] that had similar wording. The Administration has not elaborated on how this passage should be interpreted in technical analysis. Analysts and reviewers are currently left to debate about how terms like "sufficiently high," "comparable to that of uranium-235," and "highly reliable" are to be implemented. For instance, one recent study[24] presents three different interpretations of the radioactive decay aspects arriving at three distinctly different outcomes.

As of this writing, it is the authors' understanding (based in part on discussion with drafters of SPD-6) that the authors of SPD-6 intended that analysis would be performed to estimate how long it would take the fission products (as opposed to actinides) to decay to activity levels where their contribution to the overall system radioactivity is negligible. The key underlying premise is that fission products have shorter half-lives (and therefore their risk can be meaningfully mitigated by delaying reentry), whereas the half-lives of many actinides are too long to lend themselves to risk mitigation in this way. Most fission products have half-lives on the order of hours, days, or a few years. However, some have relatively longer half-lives of tens of year or higher. The premise of the SPD-6 passage was to encourage mission designers and reviewers to seek out disposal orbits whereby the manageable risks would be mitigated, acknowledging that the risks associated with the long-lived actinides are not mitigatable (short of taking the flight system entirely out of orbit, which poses its own challenges for mission design and risk).

With prominent fission products like Cs-137 having half-lives on the order of 30 years, a significant amount of fission product radioactive decay will have occurred after several hundred years. To make a rigorous case in this regard, an assessment would need to estimate fission product abundances and model the relevant controlling exposure accidents (those reentry accident scenarios having a combination of likelihood and consequence that makes them most important to overall risk) to arrive at a time-dependent estimate of risk, where the orbital decay lifetime (the timing of reentry) is the ordinate. Such an estimate would be more meaningful than the more typical assessment performed of looking at the total activity of all fission products and actinides as a function of time because different systems have lesser or greater chances of retaining the radioactive material during reentry and different radioisotopes have lesser or greater impact on radiation dose. Such an assessment would result in a monotonically decreasing risk, and either an accepted threshold would need to be defined or an optimization would need to be constructed that balances this radiological risk mitigation against the orbital mechanics aspects. The "highly reliable" tenet would still need to be addressed through other means, potentially anchoring to state-of-practice reliability and maintainability standards.

III.6 Crew Safety

Past work surveyed typically did not directly address crew safety. NASA's use of space nuclear systems over the last 30 years has all been on robotic missions, but crew interface with RPS was relevant to the Apollo missions, as well as the Galileo and Ulysses missions (those spacecraft were deployed on-orbit from Shuttle).

Safety principles in this area may take two basic forms: those that are designed to protect the crew from excess radiation exposures from the reactor and those that promote good human-system interface practices. The former of these is the subject of NASA-STD-3001 (Ref. 25), while the latter is discussed in several recent studies[26,27,28], and was also recently identified as a part of a broader high-priority gap[20].

For managing radiation exposures from the reactor, NASA-STD-3001, Volume 1, provides the standards for Space Permissible Exposure Levels (PELs) for both background space radiation and human-made nuclear technologies. The standards include astronaut total career exposure limits, short-term acute exposure limits and nuclear technology exposure limits, augmented by the as low as reasonably achievable (ALARA) principle. The standard acknowledges the need to consider tradeoffs for nuclear propulsion systems that shorten transit times (and thus reduce exposure to space radiation).

III.7 Overall Risks from All Potential Accidents

The overall risk from all postulated accidents is estimated as part of the nuclear safety analysis process. That process has evolved over time, and (Ref. 9) provides a good description of the safety analysis process (in Part A), generally describing the situation as it was carried out in the 1980s and 1990s for RPS.

For SP-100, a nuclear safety criteria was that the mission shall be designed such that the risk limits in the "Nuclear Safety Criteria for Space Nuclear Fission Reactors" document are not exceeded. The actual risk limits specified were the outcome of an assessment, as opposed to a specific threshold, with more details provided therein. In effect, the safety analysis was to estimate individual and population risks, and then justify that all reasonable mitigations had been employed. The same source[9], goes on to describe how design margins, postulated accidents, and safety functions would be considered, and translated in to detailed technical safety specification, thematically similar to how this is currently done for terrestrial nuclear safety activities.

After SP-100, the later documents surveyed did not address the topic of managing overall risk from postulated accidents, except one[14], which proposed that the radiological risk and consequences on Earth's surface of a release from an accident shall be insignificant.

With the issuance of NSPM-20 (Ref. 4), and its embedded Safety Guidelines (a stair-step curve of exceedance probability versus maximum individual exposure), it is straight forward to re-word this tenet as: 'The radiological risk and consequences on Earth's surface of a release from an accident shall be compared to the NSPM-20 Safety Guidelines.' Note that this requires a comparison but does not require that the estimated risks necessarily fall below the Safety Guidelines, in keeping with the fact that they are Guidelines and not requirements. This high-level tenet should not be contentious amongst stakeholders, as it is a direct outcome of NSPM-20 itself.

There are, however, three related issues that remain unresolved in the post-NSPM-20 era. The first is what, if any, other measures of risk or consequence should be addressed, beyond those specified in NSPM-20 itself (e.g., the likelihood of an accident resulting in an exposure in excess of 5 rem to any member of the public and the number of individuals who might receive such exposure in an accident scenario). Note that some other measures may be necessary to support radiological contingency planning and range flight safety activities.

The second issue relates to the principle of as safe as reasonably practicable (ASARP). As previously mentioned, SP-100 is an example of a program that built that feature directly into its safety approach, and DOE and NRC also have the similar feature of as low as reasonably achievable (ALARA) or other safety optimizations within some constructs of their safety processes. Implementation can be nuanced, as one should not encumber the trade space beyond what has been established to be "safe enough," while using the ASARP/ALARA principle to address cost-beneficial safety enhancements has a nexus to mitigating uncertainties that may be obscuring the understood level of safety otherwise being achieved.

The third issue is what specific methods should be used for producing the risk estimates. For instance, should a risk assessment that quantitatively estimates uncertainty bounds be required? Should mean values, or a specified percentile value be used? This topic (safety and risk analysis methods) has been identified as a high-priority gap for space reactors[20].

III.8 Planetary Protection

Planetary protection is not addressed in any of the documents surveyed. Forward planetary protection requirements for a nuclear reactor may be largely addressed through the requirements applied to all spacecraft hardware. In terms of carrying biological contamination to other celestial bodies, the reactor may prove to be self-sterilizing if operated prior to reaching a sensitive planetary body. In terms of the effect of the space nuclear system on other planetary bodies, this would require an assessment of the device's radiation and thermal impact, relative to the bodies' established sensitivity. Backward planetary protection is likely not relevant, as it is unlikely that a mission will plan to deliberately return a space nuclear system to Earth. If one were to be returned to Earth orbit, then typical backward planetary protection requirements for non-nuclear components may be enveloping, and again, the self-sterilization feature may be relevant.

The remaining issue in this area is the Outer Space Treaty tenet (Article IX) that: "States Parties to the Treaty shall pursue studies of outer space…and conduct exploration of them so as to avoid their harmful contamination," and conduct "appropriate international consultations" if potential harmful contamination is identified as a possibility. To this end, an assessment would be needed to determine that the nuclear device's operation and (when applicable) in-situ disposal doesn't unduly impact others' access to the planetary body.

III.9 Operation In-Space

In keeping with the scope of the overall paper (dealing with safety aspects, and not dealing with purely mission success aspects such as interoperability with other systems), this section deals with in-space operations from the standpoint of managing risk to Earth's biosphere (and its inhabitants) and crew that are, or may become, proximate to the space nuclear system. Some aspects of ensuring safety in these regards relate back to the system's design while some relate solely to how the system is operated.

Some sources[e.g., 11] relay lessons learned from the Rover/NERVA program regarding safe operation of the space nuclear system based on ground testing. For instance, Rover/NERVA sought to demonstrate an ability to reliably control the rapid start and restart of the nuclear rocket engine. The system had to reliably control the competing effects of the introduction of hydrogen into the core, the manipulation of control elements, and the temperature and power reactivity coefficients during startup, shutdown, and transients. A large portion of the testing focused on developing fuel and core structures that resisted erosive and corrosive effects of the high temperature hydrogen coolant.

The SP-100 program had numerous safety principles related to safe in-space operation and they aren't summarized here solely for the purpose of brevity. A later study[3] synopsized the issues somewhat more succinctly in stating: "Reactor startup(s), operation, and shutdown(s) in space must be performed in a controllable and predictable manner which prevents bulk fuel/clad/core/reactor disruption, and the consequent uncontrolled release of radioactivity, as a result of credible overpower or undercooling conditions or accidents…This means that operation of the reactor (including all startups and shutdowns) must be under positive, predictable control at all times, and that significant fission product containment/confinement barrier damage and consequent uncontrolled release of fission and activation products from the reactor will not occur during normal and off-normal operation, as well as credible overpower and undercooling events or accident situations." That source goes on to identify seven features needed to support this case, such as a reliable, responsive instrumentation and control subsystem; the ability to quickly recognize and respond to threatening overpower and undercooling conditions; and multiple fission product containment/confinement barriers.

NSPM-20 states that "Safety analysis should address launch and any subsequent stages when accidents may result in radiological effects on the public or the environment, for instance, in an unplanned reentry from Earth orbit or during an Earth flyby." SPD-6 states that "The operation and disposition of SNPP systems shall be planned and conducted in a manner that protect human and environmental safety and national security assets." When combined with crew safety standards and planetary protection / Outer Space Treaty tenets, these create the basic framework for what distinguishes safety constraints versus mission success considerations when addressing safe operation in-space. Since there is currently no US regulatory agency that has in-space authorization or oversight authority specifically for space nuclear systems, meeting the tenets of the aforementioned directives and treaties, and obtaining nuclear launch authorization, are the drivers. As such, safety principles in this area, which can be derived on a mission-specific basis using the SP-100 and later program tenets as a starting point, should focus on driving design decisions (including fuel qualification and other fission product barrier qualification) and conduct of operations decisions that will manage the risk to humans and applicable environments by minimizing the potential for the uncontrolled release of radioactive material.

In addition to the question of how the reactor is designed and subsequently operated in-space is the issue of where it is operated. The differences in context are part of what make a mission-specific approach to safety principle development more tenable. Safe operation in Earth orbit is distinctly different than safe operation in interplanetary flight or on another planetary surface, though some aspects are directly applicable to all of these situations. As described earlier, SPD-6 does not prohibit reactor use in any particular Earth orbit, and so the focus becomes on ensuring that the reactor can be operated safely wherever it will be operated.

For reference, NSPM-20 directed that NASA, in coordination with the Secretary of Defense and the Secretary of Energy, submit a report identifying any additional Safety Guidelines needed specifically for safe non-terrestrial operation of nuclear fission reactors, including orbital and planetary surface activities. That effort concluded that no additional policy-level Safety Guidelines were needed at the time.

Meanwhile, safe operation in-space was another high-priority gap identified in the recent NASA-led effort[20] (as a level of technical guidance falling distinctly below policy-level guidelines), and early efforts are underway in this regard.

III.10 Passivation, Long-term Disposal and Orbital Debris Mitigation

Like safe operation, it is somewhat difficult to talk about safe disposal absent the context of where the space reactor is to be disposed (e.g., Earth orbit versus a heliocentric orbit versus another planetary surface).

The SP-100 program had tenets that dealt with maintaining a small fission product inventory prior to launch along with a reboost capability if operated in low Earth orbit. The re-boost capability had a requirement to ensure an orbital lifetime of at least 300 years[9].

A more recent study[3] addressed this area in the following manner: "Final disposal/disposition of the reactor/system must be explicitly addressed in mission planning, operations, and reactor/system design, and must not pose a radiological risk to the Earth's population or environment…This demands projection, assessment, and perhaps real-time verification, of the system's radioactive inventory at the end-of-mission, for any and all disposal/disposition orbits, trajectories, or locations considered, planned, or actually used…This may require the incorporation of a highly-reliable, permanent / irreversible reactor shutdown capability at the end-of-mission…"

Meanwhile, an even more recent study proposed (in the context of the its mission): "In-space disposal shall be limited to sufficiently high orbits in accordance with SPD-6 guidelines."[15] Similarly, NASA NPR 8715.26 states, "For SNS-enabled missions designed to operate in low Earth orbit, the NASA Program or Project Manager shall demonstrate by analysis that the mission design enables for disposal of the SNS in a sufficiently high orbit (as defined in SPD-6), including the incorporation of a highly reliable operational system to ensure effective and controlled disposition of the reactor."

Thus, there is sufficient convergence at the principle level that passivation (permanent reactor shutdown) must occur reliably; Earth-orbiting mission disposal must result in the system being in a sufficiently high orbit; and disposal on other planetary surfaces should address planetary protection considerations.

Both the SP-100 program[9] and more recent work[11] provide useful information on decomposing the above high-level tenets to more actionable elements. Of particular ambiguity at the moment is the issue of what constitutes a "sufficiently high" orbit. While SPD-6 builds off the language in UN Principle 47/68 (Ref. 23) in this regard, there is still a good bit of ambiguity that needs to be addressed through either Administration clarification or adoption of an accepted standard by the interagency. The nature of the ambiguity was previously discussed in this paper relative to "hot" reentry.

REFERENCES

1. NASA, NPR 8715.26, "Nuclear Flight Safety," Feb. 2022.
2. McNutt, R., and P. Ostdiek, NASA TSD-23122, "Nuclear Power Assessment Study," APL, June 1, 2015.
3. Sholtis, J. et al., "Proposed safety guidelines for space reactors," proceedings of the Space Nuclear Conference 2005, San Diego, CA, June 2005.
4. U.S. Gov., "Presidential Memorandum on Launch of Spacecraft Containing Space Nuclear Systems," NSPM-20, Aug. 2019.
5. NASA, NPD 1000.0C, "NASA Governance and Strategic Management Handbook," Jan. 2020.
6. DOE, DOE-STD-1189, "Integration of Safety into the Design Process," Dec. 2016.
7. US NRC, 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities."
8. IAEA, "Safety of Nuclear Power Plants: Design, Specific Safety Requirements," SSR-2/1 (Rev 1), 2016.
9. Bennet, G. et al., "Nuclear safety criteria and specifications for space nuclear reactors," DOE, Aug. 1982.
10. Marshall, A., et al., "Integrated Safety Program for the Nuclear Electric Propulsion Space Test Program," AIP Conf. Proc. 301, 879 (1994); doi: 10.1063/1.2950283.
11. Sholtis, J. et al., "U.S. space nuclear safety: past, present, and future," in: A Critical Review of Space Nuclear Power and Propulsion 1984–1993, American Institute of Physics Publishing, New York, 1994, pp. 269–303.
12. Mehlman, W., "Nuclear space power safety and facility guidelines study," APL, prepared for the DOE (Grant DE-FG01-94NE32180), Sept. 1995.
13. Lipinski, R., "An Approach to Reactor Launch Safety Analysis," SAND2008-6852, Oct. 2008.
14. Camp, A. et al., "NASA Follow-up to Presidential Memorandum on Launch Approval – Emphasis on Fission Reactor Systems," NASA Nuclear Power and Propulsion Technical Discipline Team, Dec. 2019.
15. McClure, P., et al., "Draft General Design Criteria for the DRACO Thermal Nuclear Rocket – Launch Safety Activities," ANS NETS conference, May 2022.
16. DOE, "Atomic Power in Space II," 2015.
17. NASA NPR 8705.4A, "Risk Classification for NASA Payloads," April 2021.
18. NASA NPR 7120.5F, "NASA Space Flight Program and Project Management Requirements," Aug. 2021.
19. NASA NPR 8710.7D, "Launch Services Risk Mitigation Policy for NASA-Owned and/or NASA-Sponsored Payloads/Missions," Jan. 2008.
20. NASA/TM−20220004191, "Report of the Interagency Space Reactor Standards Working Group," March 2022.
21. Weitzberg, A. and S. Wright, "Space Reactor Launch Safety – An Acceptably Low Risk," AIP Conference Proceedings 969, 446, Jan. 2008.
22. US Gov., "Memorandum on the National Strategy for Space Nuclear Power and Propulsion," SPD-6 , Dec. 2020.
23. United Nations, "Principles relevant to the Use of Nuclear Power Sources in Outer Space," UN Principle 47/68, 1992.
24. Alfonsi, A., and M. Eades, "A technical interpretation of the SPD6 radioactivity limited "sufficiently high" disposition orbit lifetime for a space fission reactor," ANS NETS 2022 conference, May, 2022.
25. NASA-STD-3001, "NASA Space Flight Human System Standard," Volume 1, Revision A: Crew Health, Jan. 2022.
26. Klein, A., et al., "Operational Considerations for Space Fission Power and Propulsion Platforms," NASA/CR-2020-220569, 2020.
27. Klein A., et al., "Operational Considerations for Fission Reactors Utilized on Lunar In-Situ Resource Utilization Missions," NASA/CR−20205009307, 2020.
28. Klein, A., et al., "Operational Considerations for Fission Reactors Utilized on Nuclear Thermal Propulsion Missions to Mars," NASA/CR−20210000387, 2021.