RISK MANAGEMENT FOR DYNAMIC RADIOISOTOPE POWER SYSTEMS

Christopher S. R. Matthes(1), David F. Woerner(2), Terry J. Hendricks(2)

(1,2)NASA Jet Propulsion Laboratory, California Institute of Technology, 4800 Oak Grove Dr., Pasadena, CA, 91109
(1)+1-818-354-3255, cmatthes@jpl.nasa.gov

ABSTRACT

The implementation of dynamic power conversion technology in Radioisotope Power Systems (RPS) for spaceflight has potential for improved specific power and efficiency, compared with existing Radioisotope Thermoelectric Generators (RTGs). This proposed expansion of current RPS technology necessitates a full exploration of the requirements, goals, and concerns related to risks in developing and deploying such systems. The nature of dynamic systems also presents a new set of challenges related to the presence of moving machinery not intrinsic to traditional RTG units.

A general RPS risk management methodology is outlined, which is used to identify and assess the variables and operational scenarios introducing risk throughout the design, fabrication, and system integration processes. This paper will demonstrate how mission requirements for Dynamic RPS concepts (DRPS) drive decisions throughout the development process. This work will define the standard practices for decision making within the scope of the risks associated with DRPS hardware development and deployment in sensitive spacecraft near sensitive payloads. Examples of potential risk areas are analyzed for the proposed dynamic systems, and compared to those associated with traditional RTG technologies. This analysis shows the promise for DRPS systems to elevate and extend the capabilities for power systems used in future NASA missions.

1. INTRODUCTION

For the past several decades, NASA deep space missions have employed Radioisotope Thermoelectric Generators (RTGs) to power spacecraft. These power systems operate using static thermoelectric (TE) designs, which are advantageous in terms of their stability and reliability. RTGs have drawbacks to their effectiveness, however, namely in their conversion efficiency. By contrast, dynamic power conversion in Radioisotope Power Systems (RPS) could achieve up to four times the efficiency of available RTGs[1]. This improvement would offer the ability to produce equal power levels using far less radioisotope fuel, or significantly greater amounts of power per unit fuel. Dynamic RPS (DRPS) would possess additional advantages over RTGs by eliminating sublimation mechanisms within the convertor that result in efficiency degradation.

While a static RTG system converts energy from a heat source into electricity with no moving parts, a dynamic system would involve a heat engine that converts heat into mechanical energy using pistons, dynamic seals, magnetics and linear alternators, and a working fluid, which in turn produces electricity. In recent years, NASA and the Department of Energy (DOE) have pursued dynamic system development with an Advanced Stirling Radioisotope Generator (ASRG), shown in Fig. 1, which would use the Stirling cycle to produce electricity from the radioisotope heat provided by two General Purpose Heat Source (GPHS) modules [2]. The ASRG system design includes two Stirling generators with separate heat sources, which are operated synchronously opposed, in order to significantly minimize vibrations. This effort allowed for substantial testing and research to evaluate reliability and performance, as well as the exploration of other issues related to the development of a dynamic system.

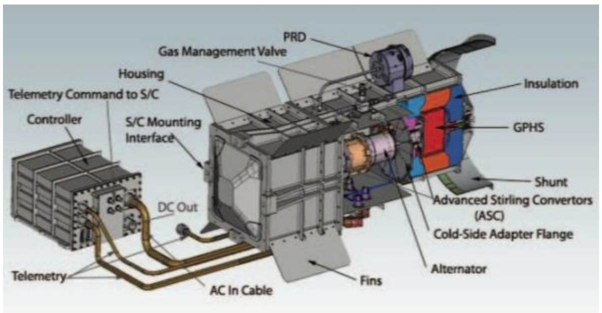

Figure 1. Diagram of the ASRG system

While DRPS technology would offer a number of valuable characteristics, there do exist challenges in qualifying this type of system for spaceflight, arising from its differences with conventional static technology. The fundamental nature of moving parts introduces an entirely new set of variables to a RPS, largely from the resulting vibrations. Electrical integration for a DRPS presents challenges due to an alternating current output from a single, or several generators, as well as the need for a generator controller. New convertor degradation and failure mechanisms also offer further areas to monitor and diagnose[3]. In addition, the desired qualities of these types of systems would come with the need to practically demonstrate their improved efficiency, reliability, performance, and longevity, while proving them to be viable for integration on a spacecraft.

More recently, NASA has partnered with the DOE to further the development of a DRPS system concept, and is currently exploring general concepts for dynamic generators. This proposed implementation of a new type of power system necessitates a robust analysis of associated risks. Effective risk management is critical to mission success, which begins with defining the system requirements and recognizing the constraints related to the power system design. This paper will first provide insight into the design considerations that drive the system requirements, and offer context to the technology development. The Risk Management Plan (RMP) for the RPS Program will then be outlined by describing the components and standards of the Risk Management Process. Lastly, the procedure will be explained for providing conclusions and recommendations resulting from the risk analysis.

2. SYSTEM CONCEPT REQUIREMENTS

2.1 Design Considerations

The Multi-Mission Radioisotope Thermoelectric Generator (MMRTG), used for NASA's Mars Science Laboratory mission, is currently the only space-qualified RPS available for future missions, and in many ways acts as a baseline for future RPS designs. A number of constraints are applied by existing technology. Development of a new heat source would not be feasible or necessary, so a DRPS would utilize the Step 2 GPHS modules used in the MMRTG. For the same reasons, the 9904 shipping cask used for the GPHS RTG would be reused, which applies certain sizing constraints on the system.

Dynamic convertor designs would either produce axial vibrations or rotating imbalances, which must be addressed through one of a number of approaches. One option is the system can be designed to pair convertors such that they are either positioned opposite, or out of phase with one another. In this case, convertor failure may have a greater impact on the system. Another strategy is to employ active dampening or balancing to minimize movement. The generator may also be isolated from the spacecraft so vibrations do not affect operations or other equipment.

Recent work on DRPS following the termination of the ASRG as a flight hardware project in late 2013 has focused on using Stirling convertor technology in a modularized dynamic RPS concept[4]. The proposed design configuration for each individual module involved four convertors evenly positioned around a common GPHS stack. In the case of a convertor failure, less heat would be drawn from the GPHS module, and the remaining convertors would be exposed to elevated temperatures exceeding their given operational limits. Thermal modeling was performed to demonstrate that in the case of a single failed convertor, adjacent converters experienced a rapid increase in temperature before achieving a steady-state elevated temperature level. In this situation, a controller would be needed to detect convertor failure and adjust the remaining convertors to draw a greater amount of heat from the GPHS module and avoid damaging thermal levels. This solution would necessitate running the convertors below their peak power level under nominal conditions in order to accommodate adjustments in the case of convertor failure. The system may also need to be designed to manage elevated temperature levels.

Additional design constraints may be driven by a number of factors, including:

- Power output level of the generator
- Power level of individual convertors
- Quantity and configuration of GPHS modules
- Methods to utilize and reject heat
- Force balancing strategies
- System-level fault tolerance.

These quantities and considerations would be important to analyze within the context of the mission objectives throughout the design process. Similarly, associated risks would need to be extensively explored to support decision-making and to best ensure mission success.

2.2 Envisioned Operational Capabilities

A number of notional design requirements are derived from the generator's generic function of supplying power to the space vehicle. For the design life, the conceptual DRPS shall meet its operating specifications for at least 10 years after Beginning of Mission (BOM), with a goal of 14 years. Related to this requirement, its net electric power degradation shall not exceed a rate of 1.5% per year during the specified lifetime. This degradation figure includes the plutonium dioxide fuel decay of approximately 0.8%. The generator is to provide a steady-state electric DC power output of at least 300 W, with a goal of up to 500 W. The conversion efficiency should reach at least 20% while providing the specified power output. In the case of significant degradation or component failure, a fault-tolerant design should be utilized to allow for graceful degradation levels by adjusting to lower power output levels, without complete failure.

Mission-specific capabilities are also important to consider to accommodate future mission objectives. Potential future missions that could benefit from DRPS technology include those destined for relatively nearby bodies such as Mars and Earth's moon, as well as deep-space ocean and ice worlds such as Titan, Triton, Enceladus, and Europa. There are a number of environmental conditions that must be endured by the DRPS during liftoff, flight, entry, descent, and landing (EDL), and throughout planetary operations. These conditions include thermal transients and disturbance forces such as quasi-static g-loads, parachute deployments, and pyrotechnic actuations, among others. The system must be capable of withstanding launch vibrations and acceleration of particular magnitudes associated with all planned launch vehicles for RPS missions. The DRPS must be designed to operate under peak g-loading during planetary EDL of up to 20 g for a duration on the order of minutes, and up to 5 g for at least five days during spin-stabilization of the space vehicle. Since the DRPS would idealy be able to be mounted in any orientation on the space vehicle, it should have the ability to withstand these acceleration forces along any axis. Flight and operational conditions may require the ability to withstand micrometeorites and dust particles, surface pressure, atmospheric gases, as well as radiation environments.

The DRPS must accommodate requirements relating to its interface with space vehicles. Therefore, the generator would be expected to interface with standard space vehicle communications architectures used for other NASA missions. Fault tolerance for avionics must be admissible by supporting redundant data interfaces between the vehicle and the generator. In addition, the DRPS must minimize disturbance forces transmitted to the host vehicle due to its operation. These forces may include torque, vibration, or angular momentum from moving parts. A maximum housing temperature and/or maximum interface mounting temperatures must also be maintained to prevent excessive thermal loads on instrumentation or other space vehicle systems within close proximity of the DRPS.

2.3 Reliability

For a newly developed power system to be adopted for use in NASA missions, it must be shown to possess the highest degree of reliability that is feasible. Subsystems and their individual components must be rated as highly reliable and configured to last sufficiently long. This way, the power system can be best ensured to provide mission operation and completion of its goals over the course of the mission lifetime.

A dynamic system would possess key differences from static RTG systems, which impact the way reliability is considered. The most obvious distinction lies in the number of convertors, the number of moving components, and their nature of power generation within the RPS configuration. The MMRTG has a total of 768 TE elements, with each contributing a small amount to the entire system power. Performance issues or failure of an individual TE convertor has little impact on the overall power output level. In the case of a DRPS, the entire system may consist of one or several individual convertors, depending on the design. In the first case, degradation or failure of a single convertor may be catastrophic to the ability of the power system to meet mission needs. Losing one DRPS among several could at least represent a large "step" drop in power output, jeopardizing mission power needs, rather than a graceful power degradation.

To achieve a sufficient level of reliability in a mission concept, there are various redundancy and reliability strategies available. A single convertor/controller string may be used within a generator if it is considered to be highly reliable. Alternately, a generator may contain multiple convertor/controller strings if an additional level of reliability is necessary. Generator redundancy may also be employed on a mission if necessary and feasible. Figure 2 shows three different convertor/controller configurations for a four-convertor generator, with each configuration offering different levels of reliability. The converters are labeled 1-4, and the controllers are shown as the empty boxes. According to standard practice, the controllers are implemented redundantly to offer improved reliability.

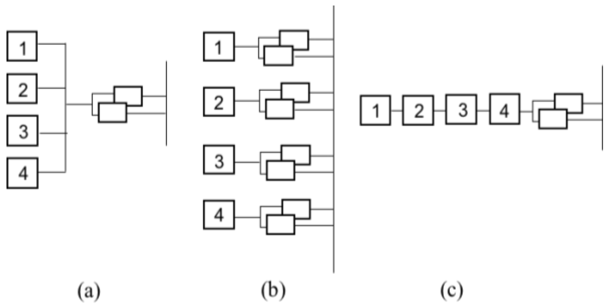

Figure 2. Convertor/Controller Configuration Diagrams

The respective system reliabilities for each of the wiring configurations in Figure 2 are modeled using the following expressions[5]:

$$R_{(a)} = [1-(1-R_{conv})^4] \times [1-(1-R_C)^2] \quad (1)$$

$$R_{(b)} = 1-\{1-R_{conv} \times [1-(1-R_C)^2]\}^4 \quad (2)$$

$$R_{(c)} = {R_{conv}}^4 \times [1-(1-R_C)^2]. \quad (3)$$

Figure 3 shows the modeled reliability behavior characteristic of the three convertor/controller wiring configurations depicted in Fig. 2. Convertor reliability, R_{conv}, is represented across the x-axis, and the system reliability is shown for two different controller reliabilities, R_C=0.5 and R_C=1. These reliability metrics represent the likelihood of each component meeting mission requirements by the end of mission. The top plot (Fig. 3a) corresponds to Fig. 2a for convertors wired in parallel, sharing a common dual controller. Fig. 3b is the same configuration, but with each convertor possessing its own dual controller (Fig. 2b). Fig. 3c is for a single string of converters in series, corresponding to Fig. 2c. The figures show that the most reliable configuration depends on the component reliabilities. For a system with high reliability converters and relatively low reliability controllers, option (b) will clearly result in the highest system reliability. Alternately, when controller reliability is high, there may not be a great difference between the options (a) and (b), and the number of controllers may be limited to a single pair to save weight and cost. The third plot shows the value of parallel wiring compared to series, which exhibits very low system-level reliability overall. The most advantageous configuration will be selected by taking into account cost and weight considerations, among other factors, needed to achieve the necessary system reliability.

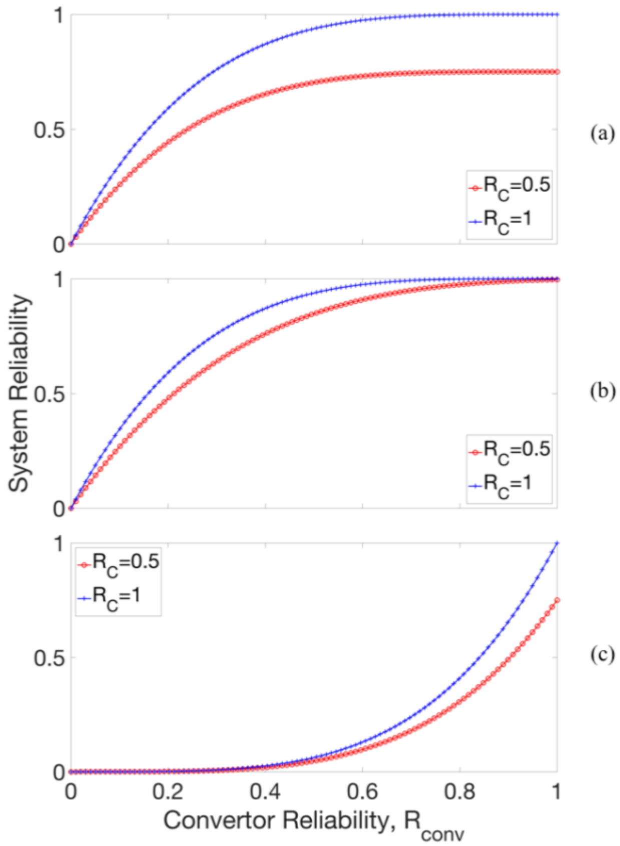

Figure 3. Reliability of Different Convertor/Controller Configurations

3. RISK MANAGEMENT PROCESS

3.1 RIDM and CRM

The Risk Management (RM) process at JPL aims to integrate system requirements, constraints, and design considerations, with an understanding of the associated risks of implementing any new technology. The goal is to minimize or mitigate risks, and when necessary, accept risks responsibly and methodically. This practice uses a complementary combination of two integrated procedures:

a) Risk-Informed Decision Making (RIDM)
b) Continuous Risk Management (CRM).

These processes work together to improve the probability of achieving the RPS Program objectives and goals within the defined schedule and budgetary constraints. The purpose of the RM process is to explicitly address performance shortfalls related to safety, cost, schedule, technical, and programmatic needs.

RIDM initiates the RM process by providing decisions arrived upon through extensive consideration of alternative outcomes. RIDM is comprised of three sequential steps:

1. Identification of Alternatives
2. Risk Analysis of Alternatives
3. Risk-Informed Alternative Selection.

Firstly, "Identification of Alternatives" involves recognizing a range of opportunities and configurations that fit within the context of the program objectives. This stage begins with understanding stakeholder expectations, which are decomposed into distinct performance objectives. Quantifiable performance measures are associated with each individual objective in order to assess all viable alternatives that fit within the imposed constraints. An example of a performance objective may be to minimize cost. The associated performance measure for a particular alternative would be the project cost. Any alternatives that fit within the imposed budgetary constraint may be considered, where the effectiveness of that alternative in achieving the objective is quantified by the performance measure. That is, alternatives with lower cost more effectively fulfil the objective for that particular criterion. In the case of DRPS, performance objectives may lead to consideration of various design configurations that minimize vibrations, or redundancy options in controllers that aim to enhance system reliability. This process results in a compiled set of feasible alternatives, which are obtained through a combination of stakeholder input and evaluation of the various candidate alternatives.

Next, "Risk Analysis of Alternative" requires the development of an integrated perspective, in which the entire scope of the program is taken into account. A technical basis is established for the various options, and deliberation provides further insight into each alternative. Specifically, Risk Analysis of a particular alternative consists of pairing performance assessment, measured according to the previously identified objectives, with probabilistic modeling, which quantifies uncertainties in a specific alternative's effectiveness at achieving program objectives. This practice begins with establishing a methodology for the analysis, followed by a quantification of the established performance measures probabilistically. The result is a technical basis for deliberation and decision making. An example may be the use of a reliability model for various convertor configurations and redundancies. Based on standard practice for reliability estimates based on a convertor's probability of failure, different wiring configurations can be considered relative to associated system considerations such as cost and weight.

Lastly, "Risk-Informed Alternative Selection" refers to the consideration and risk-informed selection of a specific alternative, such as a particular level of controller redundancy. In this process, performance commitments are defined, being informed by, but not solely based on, the aforementioned risk analysis. Consistent levels of risk tolerance are applied across the range of contending alternatives to normalize the field using either a self-consistent quantitative process or a qualitative assessment. Subsequently, the responsible parties deliberate on the existing options and provide a selection with well-documented rationale. This step is iterative, and may require additional analysis or revisions to the chosen performance commitments. The RIDM process culminates in a selected alternative to be inputted into the CRM process.

True to its name, CRM is implemented continuously throughout all program phases to mitigate risks as they become apparent. The purpose of this requirement is to identify risks as they arise so they may be collected and captured. This process is iterative, containing the steps illustrated in Figure 4 and summarized as follows, according to JPL's risk management process:

1. Identify: Identify contributors to risk (shortfalls in performance relative to the baseline performance requirements).
2. Analyze: Estimate the probability and consequence components of the risk through analysis, including uncertainty in the probabilities and consequences and, as appropriate, estimate aggregate risk
3. Plan: Decide on risk disposition and handling,

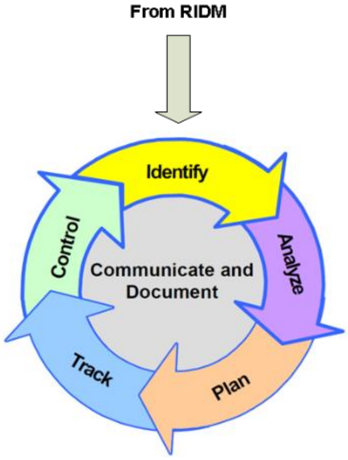

Figure 4. CRM Process Flow, Fed by the Results of the RIDM Process

develop and execute mitigation plans, and decide what will be tracked.
4. Track: Track observables relating to performance measures (e.g., technical performance data, schedule variances).
5. Control: Control risk by evaluating tracking data to verify effectiveness of mitigation plans, making adjustment to the plans as necessary, and executing control measures.

In conjunction with each of these steps, communication and documentation is practiced throughout the lifecycle of the RPS Program and Project.

An example of CRM for a DRPS may be related to assessing risks associated with modularity in the design. The RIDM process may result in a decision to pursue modular layers for the RPS, each with a particular power output, for greater flexibility in its usage for various mission scopes. A higher degree of complexity in the design, and a greater number of interfaces, may be "identified" as contributors to risk. "Analysis" may assign reliability statistics to each interface, and provide an understanding of the increased risk each size level offers to the previous one. That is, if a lower-level assembly is assigned a particular measure of risk, subsequently larger sizes will multiply the number of mating tasks, and the associated risk level. The "planning" phase may result in adjustments and impose design constraints that will minimize the mating tasks, such as prescribing a maximum level of modularity. The effectiveness of these adjustments may be monitored in the "tracking" phase, perhaps by testing the power levels across mating assemblies. Based on these results, certain measures may then be taken to "control" risks through additional adjustments. It is at this point that the risk may either be closed, accepted, or the CRM cycle restarted to mitigate the risk by "identifying" further shortfalls in performance of the assembly mating points.

3.2 Risk Analysis (NASA 5x5 Risk Matrix)

All items on the project risk list will be ranked according to a qualitative risk assessment. This task is accomplished by characterizing the likelihood and consequence of each risk on a scale of 1 to 5. This combined assessment provides the probability of a particular event occurring, and measures the impact in the case of such an event. Table 1 defines the ratings of consequence from both an implementation and mission standpoint. A cost evaluation is also included in Table 1 to approximate the resources necessary to address the risk, as a percentage of remaining project reserves. Resources, as they relate to implementation risk, may refer to performance, contingency, budget, safety, and schedule, among other categories.

Table 1. Risk Consequence Category Definitions

Rating	Consequence	Implementation Risk	Mission Risk
5	Very High	Cannot achieve flight readiness with remaining resources	Mission Failure
4	High	Consume all (100%) of remaining resources	Significant reduction in return
3	Moderate	Consume significant (26-99%) remaining resources	Moderate reduction in return
2	Low	Consume little (10-25%) of remaining resources	Small reduction in return
1	Very Low	Consume minimal (<10%) remaining resources	Minimal reduction in return

The percentage definitions related to the likelihood of a risk occurring, and the associated qualitative rating, are displayed in Table 2.

Table 2. Risk Likelihood Category Definitions

Rating	Likelihood	Definition
5	Very High	Almost Certain (> 90%)
4	High	More Likely than Not (75 < P < 90%)
3	Moderate	Significant but Not Assured (30 < P < 75%)
2	Low	Unlikely (10 < P < 30%)
1	Very Low	Very Unlikely (< 10%)

The likelihood and consequence ratings are tabulated in a traditional 5x5 risk reporting matrix shown in Figure 5. The corresponding rating position on the Risk Matrix categorizes the risk as either "low," positioned in the green section, "moderate" in the yellow, or "high" risk in the red.

3.4 DRPS Concept Risk Mitigation

As part of the communication and documentation for CRM, a Risk Focus Chart is compiled for each risk, which identifies the status of risk mitigation actions. This information includes a risk ID, title, statement, context, and ratings at each status point in the process. From a mission concept perspective, a number of risks associated with using a DRPS may be identified. For example, risk ID "DRPS-M-05" (see Table 3) possesses the title "DRPS Reliability Risk Due to Convertor Failure." The associated risk statement explains that in a DRPS composed of one or more convertor units, there exists a possibility that any of these units may become inoperable, resulting in a loss of power and excess

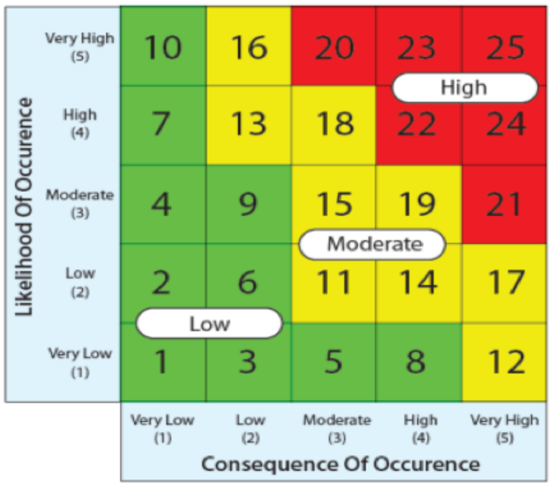

Figure 5. NASA 5x5 Risk Matrix

unused thermal energy input from the GPHS. The context of the risk is such that the power system must meet power output and thermal dissipation requirements over the entire mission. In the event of a single convertor failure in a multi-convertor configuration, the generator needs to meet these minimum requirements while operating with one less converter. A fault-tolerant design must be adopted such that no single credible fault condition renders the entire system inoperable. If the approach for addressing this risk is designated as "mitigate," then steps must be taken to lower the risk rating to an acceptable level such that it can be either accepted or closed. Table 3 shows the mitigation process for the stated risk, in which the rating is reduced from a high-level risk to low-level, to the point where it may be acceptable for flight.

Table 3. Risk Mitigation Process for DRPS-M-05

	Description	L	C	Rating
1	*Initial Rating*	5	5	25
2	Use parallel convertor wiring for improved system reliability rating	2	5	17
3	Initially operate convertors below peak power output	2	2	6
4	Perform reliability tests to improve component reliability rating	1	2	3

For a generator composed of 4 convertor units, the likelihood of convertor failure and the corresponding performance consequence can be tabulated. The initial configuration shown in step 1 of Table 3 corresponds to the series convertor/controller arrangement shown in Figure 2c. The risk likelihood can be quantified using Eqs. 1-3 presented in Section 2.3, initially assigning a conservative reliability estimate of 0.5 for all components. The series arrangement yields a reliability R=0.047, meaning nearly certain failure will occur, corresponding to a likelihood rating of 5 shown in Table 2. This reliability estimate evaluates the probability of each individual component meeting mission requirements by the end of mission. The consequence of a convertor unit outage in a series arrangement would prevent all upstream convertors from successfully contributing to the power output, meaning there exists a higher likelihood of losing each convertor with this design. Assuming that the loss of a single convertor will result in mission failure, the performance consequence in this case is characterized by a 5 rating, for an initial overall "high risk" rating of 25.

To mitigate the risk, the first step is to adopt a different convertor/controller wiring configuration. The arrangement shown in Fig. 2a is selected, resulting in a reliability estimate of R=0.703, lowering the likelihood rating to 2, meaning "low" probability of system failure, and producing an overall rating of 17, within the "moderate risk" regime. The wiring arrangement in Fig. 2b would result in a slightly higher reliability, but the added weight and cost make other risk mitigation options more advantageous. At this point, the likelihood has been lowered to an acceptable level, but the consequence of a convertor failure would result in excessive thermal levels and unacceptable reduction in power output. To address this issue, the convertors used in the DRPS may be rated for a higher power output than utilized during initial operation. In the case of a single convertor failure, the remaining units can ramp up to draw the excess heat from the GPHS and output the required amount of power. In this case, a single failure will have a low performance consequence, limited to a slightly diminished power output and an increased thermal output within reasonable margins. This change reduces that performance consequence rating to a 2, producing an overall risk rating of 6, now in the "low risk" regime. Finally, reliability tests and experimentation can be performed on the convertor units to raise the component reliability rating to a higher level. If the component reliability is raised from 0.5 to 0.7, the overall system reliability reaches R=0.903, allowing the performance consequence rating to drop to 1, for an overall rating of 3. At this point, the risk can be reviewed and closed. Procedurally, if a risk is rated at 4 or above, it may be accepted and watched, whereas if it reaches 3 or below, it may be closed.

4. PLANS & CONCLUSIONS

Dynamic RPS technology offers great potential for revolutionizing the way future NASA planetary missions would be powered. Key characteristics, potential mission constraints, and notional requirements for developing this type of system concept have been presented. A number of key design elements will need to be fully considered and analyzed throughout development to arrive upon a flight-qualified DRPS generator. These considerations include convertor technologies, converter configuration and design, component layout, mission concept needs, budget, and schedule, among many others. As DRPS development proceeds, each of these areas and the associated criteria will need to be well specified and understood. Risk management will be a critical component to decision-making throughout this undertaking.

The JPL Risk Management process was outlined as it relates to DRPS development. The risk management process should be matched to DRPS design considerations and requirements in order to determine viability. There exists great upside to advancing dynamic RPS technology. With this upside comes uncertainty related to generator and spacecraft integration, as well as viability for future use. A full understanding, evaluation, and quantification of the risk associated with implementing these new types of systems will be critical as NASA pursues future decisions about DRPS.

5. ACKNOWLEDGEMENT

The research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.

6. REFERENCES

1. Cataldo, R. L., & Bennett, G. L. (2011). US Space Radioisotope Power Systems and Applications: Past, Present and Future.

In *Radioisotopes-Applications in Physical Sciences*. InTech.

2. Lange, R. G., & Carroll, W. P. (2008). Review of recent advances of radioisotope power systems. *Energy Conversion and Management*, *49*(3), 393-401.

3. Qualls, A. L., Schmitz, P., Rusick, J., Zakrajsek, J. F., Woerner, D. F., & Cairns-Gallimore, D. (2017, March). Dynamic Radioisotope Power System development for space exploration. In *Aerospace Conference, 2017 IEEE* (pp. 1-7). IEEE.

4. Schmitz, P. C., Mason, L. S., & Schifer, N. A. (2016). *Modular Stirling Radioisotope Generator*. National Aeronautics and Space Administration, Glenn Research Center.

5. Ely, N., & O'Brien, T. P. (1995). Space logistics and reliability. *Space mission analysis and design (2nd edition), Dordrecht, Netherlands, Kluwer Academic Publishers*, 693-714.