KILOWATT ISOTOPE

POWER SYSTEM

PHASE II PLAN

VOLUME V

SAFETY

QUALITY ASSURANCE

RELIABILITY

MASTER

Sundstrand Energy Systems

C00-4299-025

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency Thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

DISCLAIMER

This book was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof nor any of their employees makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

KILOWATT ISOTOPE POWER SYSTEM

PHASE II PLAN

**VOLUME V
SAFETY, QUALITY ASSURANCE AND RELIABILITY**

To

DEPARTMENT OF ENERGY

From

**SUNDSTRAND ENERGY SYSTEMS
4747 HARRISON AVENUE
ROCKFORD, ILLINOIS 61101**

NOTICE

"This document was prepared as an account of work sponsored by the United States Government. Neither the United States nor the United States Department of Energy nor any of their employees, nor any of their contractors, subcontractors, or their employees, make any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness or usefulness of any information, apparatus, product or process disclosed, or represents that its use would not infringe privately-owned rights."

**C00-4299-025
15 MARCH 1978**

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

TABLE OF CONTENTS

<u>Title</u>	<u>Section No.</u>
Safety	6.0
6.1 Conceptual Flight Safety Analysis Report	
6.2 Preliminary Ground Safety Assessment Report	
Quality Assurance	7.0
7.1 Introduction	
7.2 Phase I Quality Assurance Program Plan	
7.3 Phase II Quality Assurance Program Plan	
7.4 NRA-1 Compliance Analysis	
7.5 Fabricability	
7.6 Assembly Procedures	
7.7 Inspectability	
Reliability Plan	8.0
8.1 Phase II Reliability Plan	
8.2 Differences Between Phase I and Phase II Reliability Plans	
8.3 Reliability Estimation	
8.4 Failure Modes, Effects and Criticality Analysis (FMECA)	
8.5 Single Point Failures	

SECTION 6.0

SAFETY

SECTION 6.0

SAFETY

This section presents the results of the safety efforts that were addressed in Phase I. Included are launch and flight safety considerations presented in the Conceptual Flight Safety Analysis Report, Section 6.1 and the ground safety considerations presented in the Ground Safety Analysis Report, Section 6.2.

6.1 CONCEPTUAL FLIGHT SAFETY ANALYSIS REPORT

A preliminary nuclear safety study was conducted which considered the launch of plutonia fueled power conversion systems currently under development by DOE. The probabilities and consequences of potential launch pad and reentry launch aborts were examined for a representative type mission. The launch vehicle used to attain the final orbital mission is the Space Transportation System (STS) with Interim Upper Stage (IUS).

The report describes the study with some specific reference to KIPS attributes. Section I presents the major findings of the study along with brief descriptions of the reference launch, accident definition and associated environments and methods of analysis. Section II provides more information with regard to the critical accident environments and is intended to provide insight into the findings. The final section addresses the major objective of the Conceptual Flight Safety Analysis report: that of quantifying the effects of a specific power conversion system in the risk assessment.

I. STUDY SUMMARY

Summary results of the study are presented in this section. A brief description of the reference launch, scope and limitations of the study, accident definition and associated environments, and methods of analysis are included.

A. Mission, Vehicle and Power Systems Under Study

The preliminary nuclear safety study* was performed for a representative type mission which utilized the Space Transportation System (STS) launched from CCAFB and the Interim Upper Stage (IUS). The mission is that of placing a spacecraft in a high, circular earth orbit (~ 10 day period). To achieve this, the STS vehicle is used to place the orbiter in a low (~ 150 n mi altitude), nearly circular orbit. The IUS/Spacecraft/power conversion system (PCS) is then off-loaded and the two stage IUS is used to achieve the final orbit. The IUS flight involves an initial burn which places the system in a transfer orbit. After coast to near apogee, the second stage motor of the IUS is utilized to achieve the final nominal orbit.

Three plutonia fueled PCS's were considered in the study: two dynamic systems and one RTG (SIG). Analysis specific to these systems reflects the system design concept at the time the study was performed (late 1976 through mid 1977). All three systems employ the Multi Hundred Watt Isotope Heat Source (MHW IHS). Except as noted as follows, the heat source design was that of the MJS mission design.

B. Scope of Study

The study considered failure modes and effects, accident probabilities and consequences in terms of potential nuclear fuel release distributions. A review of documents reporting the status of elements or the various subsystems comprising the STS and IUS was useful for identifying the various failure modes but provided no information concerning failure probabilities. Probability estimates were developed from results of studies performed on previous flight systems. The magnitude of the hazardous environment, which are a consequence of the accident condition were estimated by scaling the results of previous studies according to the STS rocket fuel loadings.

For the accidents analyzed, the study is essentially complete in the sense that the techniques employed were those appropriate to a final safety analysis. The environment and system response models must, however, be considered preliminary because of the preliminary nature of the environment definition and lack of test data to substantiate response modelling.

* A more detailed account of this study will be published as an AFWL Technical Report.

Certain major accident types were not considered in the study: most noticeably (1) orbiter landing accidents (attempt to accomplish a nominal landing of the orbiter with payload following a launch abort) and (2) reentry of an abandoned orbiter with payload from low earth orbit.

C. Accident Definition, Environments

Two major categories of accident types were evaluated: (1) launch pad and (2) IUS aborts resulting in prompt or delayed atmospheric reentry.

The launch pad accidents are those which can occur in the time from launch until impact in the ocean, (approximately 25 seconds after launch). In this time frame, accidents are likely to result in impact of the nuclear system on land or in shallow water near the launch pad. Launch pad accidents are further subdivided as to occurrence before or after the nominal vehicle trajectory clears the pad tower (~ 5 seconds after launch).

Pad accident occurrence probabilities are given in Table 1. All accident types, as referred to in this table, involve an explosion of the liquid rocket fuel contained in the STS external tank (ET). In the tipover and fall back categories, the explosion is assumed to occur at or near ground level; the STS vehicles is assumed essentially intact immediately prior to the explosion. The other types involve an in-flight explosion (OIFE: other in-flight explosions). The destruct type involves a command or automatically triggered vehicle destruct systems designed to substantially reduce the magnitude of subsequent explosions. The OIFE assume no initiation of the destruct system (not triggered or failure to function when triggered).

Estimated representative explosive yields (% TNT equivalence) for the accident types ranged from 1 to 10% for tipover, 10 - 60% for the fall back, 0.1 - 1% for the destruct modes and 4 - 20% for other in-flight explosions. The thermal environment associated with the blast was estimated according to the ET fuel inventory. Fireball duration would range from approximately 0 to 6.5 seconds. Fireball diameter is proportionate to the square of the duration time with a maximum diameter of 870 ft. In the modelling, the fireball parameters were assumed independent of the yield (yield values were used to compute overpressure. High velocity fragments are created as a result of the blast. The primary source of fragments are the ET fuel tank walls. Subsequent to in-flight explosions, the residual structure containing the nuclear fuel would impact at velocities which range from approximately 100 fps to values in excess of the terminal velocity for the configuration. Under certain conditions, fuel released at impact could be vaporized by the fireball environment or by exposure to chunks of burning solid rocket propellant.

Ascent accidents (those occurring after the launch pad phase and prior to attainment of orbit by the STS orbiter) were assessed to have an overall occurrence probability of 4×10^{-2} . About 70% of the time, however, a successful orbiter landing could be accomplished and there would be no nuclear hazard. Probabilities for unsuccessful landing attempt (CCAFB) or uncontrolled reentry during ascent are 1.6×10^{-3} and 1.0×10^{-2} , respectively. The overall probability for African land impact (launch azimuth = 90°) is 2.4×10^{-4} .

TABLE 1
LAUNCH COMPLEX ACCIDENTS AND PROBABILITIES

Time (Relative to Launch) (sec)	Occurrence Probability			
	Accident Type: Tipover	Fall Back	Destruct	OIFE
0 - 5	1.5×10^{-5}	—	8×10^{-7}	6×10^{-6}
5 - 25	—	3.7×10^{-4}	6×10^{-4}	1.4×10^{-4}

Orbiter accidents occurring after attainment of orbit by the orbiter could result in prompt reentry with either a landing attempt accident (3×10^{-4}) or an uncontrolled reentry and sea impact (3×10^{-4}).

Accidents occurring during the IUS phase of the launch were the subject of detailed reentry studies. The assessment postulated three types of accidents: failure of IUS motors to deliver thrust, early termination of thrust while on nominal course or vehicle misorientation during nominal thrust. No-thrust or early termination of thrust have an occurrence probability of 2.4×10^{-2} . Misorientation type accidents were assessed to have an occurrence probability of 7×10^{-6} .

Early termination or no-thrust result in residual configurations left in earth orbit; orbital periods vary. Misorientation accidents can result in an orbiting system or prompt atmospheric reentry with subsequent land or water impact.

D. Methods of Analysis

Although much of the modelling must be considered preliminary, the methods employed for accident analysis are of the form which will be used for final safety assessment. A probabilistic approach is employed; Monte Carlo simulation of the sequence of environments for a given accident and the response of the nuclear systems to that sequence was performed. The analysis results in the production of released fuel source term cumulative distribution functions (CDF's)*. Released fuel is classified as to whether it is in vapor form or particulate matter with a characteristic dimension of less than or greater than 4 microns. The source distributions were used in subsequent analysis (not reported herein) which examines subsequent wind transport effects and biological consequences.

* The probability of exceeding a given source term magnitude.

The Monte Carlo process involves performing a large number of "histories"; each history is a simulation of an accident event. Histories vary due to the random nature of the particular environments and responses (as selected from their respective distributions). Various quantities are scored during each history including the source terms.

Figure 1 illustrates the history process for launch pad accident. One vertical path is followed according to the pre-specified accident type. Separate analyses are performed for each accident type and for pre-specified limits for the time of accident. An indication of the environment sequence considered for the accident is gained by reading down the columns. In this figure, "transitions" refers to reduction of the system or subsystem containing the fuel to some lesser subsystem (e.g., heat source to free FSA's).

The sequence of steps which comprise a history for an accident which effects prompt atmospheric reentry of a substructure containing the nuclear fuel is shown in Figure 2. Heat source release altitude (if released) are randomly selected from preset limits defined by configuration breakup analyses. Nominal critical parameters are then evaluated and subjected to error analysis to determine the consequences of reentry.

The history process for configuration reentering after decay from orbit is similar but simpler in that heat source flight conditions at release (V, γ) are a function of the release height, h , and ballistic coefficient, B only. For orbital decay, initial speed and flight path angle are assumed fixed at 25690 fps and -0.1° .

Impact temperature distribution derived from the reentry analysis are used in a Monte Carlo impact analysis which examines the effect of impact on the worldwide soil type distribution characteristic of the $\pm 40^\circ$ latitude band.

E. Results of Analysis

A summary of results for the launch and reentry accidents is given in Table 2. Respirable source terms are for plutonium dioxide vapor or particles small enough to be inhaled and retained (less than 4 microns). In this table, the designation A or B for launch pad accidents refers to the accident time relative to launch: A (0-5 seconds), B (5 - 25 seconds). The combined probability is the product of the accident probability and the conditional probability of fuel release.

Source terms (excepting the reentry/worldwide) are those resulting from a launch with power conversion system(s) (PCS) utilizing a total of five MHW heat sources. To a first approximation, results may be scaled according to the number of heat sources aboard a launch.

Some perspective of the relative importance of individual accident situations and their related environments may be gained by defining a risk index which is the product of the accident occurrence probability, conditional fuel release probability and the mean or expectation value of the respirable (vapor or fines) source term. Risk factors and more definitive information on the nature of the source term for launch pad are presented in Table 3. Here it is seen that, for the most part, conditional fuel release probabilities are large ($\sim 0.1 \rightarrow 1.0$). Overall risk is relatively large as compared to estimates for prior launches (Titan-Centaur vehicles). The increase is due mainly to the more

FIGURE 1
LAUNCH COMPLEX ACCIDENT SEQUENCES

FIGURE 2
PROMPT REENTRY ATMOSPHERIC
RESPONSE ANALYSIS

TABLE 2

SAFETY ANALYSIS SUMMARY FOR PCS WITH FIVE MIW IHS's

No.	Accident/ Location	Type	Failure Mode /Subsequent Environment	Combined Probability	Mean Value of Respirable Source Term (Ci)	Mean Value of Non-Respirable Source Term (Ci)
1	Launch/ pad area	Tipover	Fragment/ fireball	5.0×10^{-6}	79	69
2	Launch/ pad area	Fallback	Fragment/ fireball	3.6×10^{-4}	142	128
3A	Launch/ pad area	Destruct	Impact/ fireball	2×10^{-6}	1.5	7.9
3B	Launch/ pad area	Destruct	Impact	5.6×10^{-4}	0.48	107
4A	Launch/ pad area	Other in-flight explosions	Impact/ fireball	1.4×10^{-5}	115	265
4B	Launch/ pad area	Other in-flight explosions	Fragment	4.1×10^{-5}	66	57
C*	Reentry/ Worldwide	IUS failure	Impact on land	5.4×10^{-3}	1.7	350

* Source terms for reentry are on a per heat source basis. Fuel is released on ground impact.

TABLE 3

INHALATION RISKS FOR LAUNCH COMPLEX ACCIDENTS
(Five MHW IHS's)

Accident	Probability	Yield Range %	Vapor Source Term		Fines Source Term		Risk Index (C _i)
			Fireball	Solid Propellant			
			Expectation (C _i)	P _C ^[2]	Expectation (C _i)	P _C	
2	3.7 x 10 ⁻⁴	10-60	142 ^[3]	0.95			5 x 10 ⁻²
4B	1.4 x 10 ⁻⁴	4-20	32 ^[3]	0.29		0.66	1 x 10 ⁻³
4A	3.0 x 10 ⁻⁵	4-20	113 ^[4]	0.33	9.8	0.47	1 x 10 ⁻³
3B	5.6 x 10 ⁻⁴	0.1-1.0	1.4 ^[4]	0.13	1.2	0.04	7 x 10 ⁻⁷
1	7.4 x 10 ⁻⁵	1-10	79 ^[3]	0.007			4 x 10 ⁻⁵
3A	4 x 10 ⁻⁶	0.1-1.0	1.4 ^[4]	0.13	1.2	0.04	7 x 10 ⁻⁷

[1] Computed from largest of expectation and conditional probability

[2] Conditional fuel release probability

[3] Fragment/Fireball sequence

[4] Impact/Fireball sequence

severe environments associated with the STS vehicle and certain aspects of the response modelling associated with their environments. Critical environments and effects are the subject of Section II of this report.

II. ANALYSIS OF RESULTS

ACCIDENT ENVIRONMENTS AND RESPONSE

In the assessment of risk for missions utilizing the STS vehicle and the MHW-IHS, the characteristics of several accident environments and system response to these environments play a critical role in the assessment of risks. This section reviews the consequences and response modelling to provide more insight into the results of the study.

A. Launch Pad Accidents

1. Explosive Yield, Overpressures

The center of explosion was assumed to be within the ET as shown in Figure 3. With the possible exception of the in-flight destruct accident, the explosive yields (see Section I, C) and resultant overpressure are severe in the sense that the orbiter skin, HSA (heat source assembly) housing and the heat source aeroshell and sleeve are likely to be destroyed by the blast releasing the collected FSA's. In terms of yield, the destruct ranges are as follows.

<u>Component</u>	<u>Yields to Destruct (%)</u>
Orbiter Skin	0.05
Skin, HSA Housing	0.4 - 0.9
Skin, housing, heat source ablation Sleeve and aeroshell	1.3 - 2.6

The yield variations are attributable in part, to variations in HSA housing material. However, in comparison to the actual yields, it is seen that the difference in the various housings is inconsequential.

Destruct of the GIS by the overpressure was not considered in this limited study (but should be considered in subsequent studies). Hence, for in-flight explosions of this study the impacting configuration is a heat source (destruct) or FSA's (OIFE).

Another aspect of the overpressure was found to be significant: acceleration of the residual nuclear system by the blast. From Figure 3, it is seen that the explosive impulse will deliver a net downward velocity to residual element of the nuclear system when the launch vehicle is vertical. Typical values derived from the current modelling are as follows:

FIGURE 3

HEAT SOURCE LOCATION FROM CENTER OF ET EXPLOSION

<u>Explosive Yield (%)</u>	<u>Reflected Impulse (psi-sec)</u>	<u>Velocity Impulse (ft/sec)</u>
0.1	0.51	18
1.0	2.37	98
10.0	6.37	229
25.0	9.73	349

For early accident times (offsetting effects of vehicle upward motion and atmospheric drag are small), this has a significant effect on impact velocity. Impact velocities well in excess of residual system terminal velocities can occur. Impact velocities as high as 370 fps occurred for FSA's (accident 3-A). Impact occurs for these cases in the near vicinity of the launch pad.

2. Fragmentation

The fragments considered for this study are those generated by a portion of the ET fuel tank within the solid angle intercepted by the heat source relative to the COE. A probabilistic model was formulated for fragments assumed to be circular disks with diameters ranging from 0.2 to 3 inches. The fragment size distribution shows a decrease in size with increasing blast yield. The variance of the fragment speed distribution decreases with increasing yield: for higher yields, the tendency is toward nearly uniform breakup of the tank wall into small, high velocity particles.

Modelling assumed that penetration could only occur for nearly edge on impact (larger discs). Penetration modelling was according to the Recht-Ipson experiments (cylindrical pellets). Speeds required to completely penetrate the fuel and PICS and all other intervening structure ranged from 2.4×10^4 fps (0.2 inch diameter) to 1200 fps (3 inch diameter).

The expected number of penetrating fragments varies dramatically with blast yield. Typical values are as follows:

<u>% Yield</u>	<u>Expected Number of Penetrating Fragments</u>
0.1	7×10^{-6}
1.0	5×10^{-3}
10.0	0.4
25.0	3
50.0	13

Since the modelling is for complete penetration of the FSA, a significant amount of fuel is expelled ahead of the fragment and is therefore subjected to the severe thermal environment (fireball) which is essentially coincident with fragment arrival. The result is the large vapor source terms (see Tables 2 and 3).

3. Impact

As previously noted, for this analysis the impacting configurations were either heat sources* or collections of free flying FSA's. Impact modelling was based, in part, on results of impact tests performed on MHW IHS's and FSA's. Test data was used to formulate the basic failure probabilities for a specific reference condition: namely, impact on granite at 280 fps with a PICS temperature of 1300°F. Basic failure probabilities as derived from test data were modified in an attempt to account for the apparent improvement with units which would employ doped irridium PICS. Failure probabilities for the reference condition were assessed as follows:

<u>Unit</u>	<u>Expectation or Failure Probability</u>	
	<u>Non Doped Irridium PICS</u>	<u>Doped Irridium PICS (used for study)</u>
Heat Source	3 PICS failures out of 24 units per heat source	3 PICS failures out of 24
FSA	$P_{fail} = 0.5$	$P_{fail} = 0.16$

Launch pad impacts involve a variety of target materials, velocities and a range of temperatures. Since the bulk of the testing was done under conditions in the very near vicinity of the reference condition, modelling with respect to the above variables remains to be substantiated. Failure probability was assumed linear with respect to velocity with the expected number of failures or failure probability tending toward zero as v approached 100 fps. Target correction factors based on acoustic impedance model were applied to adjust the actual impact velocity to an effective velocity used in assessing failures.

For PICS temperatures exceeding 1250°C failure probabilities are as stated above. A linear relationship with elongation between 1250°C and 950°C was used to adjust

* For very low yields, the configuration released by the blast could have been a heat source within its primary containment. For impact analysis, it was assumed that this configuration behaved as a heat source on impact.

failure probabilities. For temperatures less than 950°C, failure probabilities (or expected number of failures) were as derived from test results for non-doped iridium PICS.

Given failure, source terms are derived by first selecting a crack size from a distribution which was derived from consideration of the data of several test failures. Released fines (particles < 4 microns) and particles of greater size are then estimated from an empirical model relating crack area to radioactivity released.

For accidents in the early time frame, the consequences of impact are particularly important when the blast thermal environment (fireball) is considered.

4. Fireball

As previously indicated, a maximum fireball liftoff time of 6.5 seconds was postulated. In the Monte Carlo modelling, this fireball liftoff time was chosen from a uniform random distribution over the range from 0 to 6.5 seconds based on a limited amount of test and launch accident data. Maximum fireball diameter varies as the square of the liftoff time, t_{lo} : namely, $d_{max} = 20.5 t_{lo}$ for a maximum diameter of approximately 870 ft. Given the event of exposed nuclear fuel (released by fragmentation and/or impact), fuel vaporization is computed according to the time in the residual (time dependent) fireball environment assuming radiative heat transfer to the fuel particles.

The fireball, coupled with fragment and impact consequences, has a dominant effect on the vapor source terms. The thermal environment is essentially in coincidence with the arrival of and damage caused by fragments. A significant amount of fuel may be released directly as a result of the penetrating fragments (see accidents 1, 2, 4-B, Table 2). For other accidents, impacts and impact related fuel release can occur prior to the effective end of the fireball. For early accident times, with explosion center altitudes less than 870 ft, the fireball is postulated to touchdown, the residual heat could then cause significant vaporization of impact released fuel. (See accidents 3-A, 4-A, Table 2).

5. Burning Solid Rocket Propellant

Solid propellant fuel loading of each STS Solid Rocket Booster (SRB) is about 2.5 times that of a Titan "strapon" Solid Rocket Motor. Modelling postulated that a condition for explosion of an SRB on impact severe enough to cause rupture of the steel casing, breakup and dispersion of chunks of burning solid rocket propellant over large "throw" areas was near end on impact of the SRB. The conditional probability of end on impact is approximately 3×10^{-3} . Given impact, the explosive yield is a function of impact velocity. Impact velocities of SRB's are likely to be relatively high. Terminal velocity estimates range from 600 to 1200 ft/sec (depending on motion); an average of 900 ft/sec was used in the ballistic flight calculation to compute the actual impact velocity.

High yields result in large chunk dispersion areas with a continuous spectrum of sizes ranging from very small to a maximum characteristic dimension of 3 ft. (For consideration of thermal effects in nuclear fuel, the minimum dimensions of the chunk is the

critical dimension since it determines the burn time). Fuel released by other mechanisms and being in the proximity of a chunk can suffer extensive vaporization.

The relative importance of this environment depends, to a large part, on the assumed requirement for end-on impact (probability is about 3×10^{-3}) and on the dependence of chunk size on the impact speed of the SRB.

B. Accidents Involving Reentry, Impact

The overall accident probability leading to atmospheric reentry is second order (10^{-2}) Parametric reentry thermal analysis for heat source released at varying altitudes and flight conditions showed that the MHW heat source is relatively insensitive to the atmospheric heating environment. The probability of a PICS melt danger during reentry is very small (nominal maximum temperatures were about 3000°F whereas the irridium-graphite eutectic temperature is about 3800°F).

PICS impact temperatures do show a significant dependence on initial temperature. Some relatively weak dependence of impact temperatures on release altitudes is shown for prompt reentries. Generally, however, as the release altitude decreases toward 100,000 ft, impact temperatures tend toward initial temperatures (net heating and cooling effect of the atmosphere is small).

The probability of an aeroshell failure by thermal stress then releasing FSA's for subsequent flight is about 3×10^{-8} (accident probability of prompt reentry 7×10^{-6} , conditional failure probability, 4×10^{-3}). FSA flight and impact was not analyzed during this study.

Graphite ablation during reentry is inconsequential. Under the most severe reentry conditions, the ablation sleeve could be burned through, but the aeroshell would suffer no significant damage prior to impact.

Results with respect to fuel release at ground impact are significant. Heat source impact response modelling was essentially the same as for launch pad impacts except as follows:

1. Impact velocities were selected from a distribution appropriate to the heat source terminal velocities.
2. PICS impact temperature distributions were those derived from the reentry studies.
3. A worldwide averaged (+ 30 to -30° latitude) soil distribution was assumed for the target material.

The soil distribution included eight types. According to the "target correction factor" the effective impact speed would exceed 100 fps* for seven of the nine types which constitute 83% of the land mass. Since 100 fps is the threshold of failure leading to fuel

* The target correction factor, derived from an acoustic impedance model, is used to estimate an equivalent impact speed on granite.

release of an impacting heat source, fuel release is possible following impact on 83% of the land mass. Previous analyses assumed a fuel release potential in only 7 percent of the impacts (frequency at occurrence of azonal - hard or granite-like surface).

III. IMPLICATION WITH RESPECT TO THE POWER CONVERSION SYSTEM

One of the stated objectives of the CFSAR is to investigate those system design aspects which would create environments different from those that the MHW IHS has previously seen. In accordance with the information already presented, it is apparent that any power conversion system launched aboard the STS is subject to accident environments which are more severe than those postulated for previous launches which employed the Titan-Centaur vehicles. Many aspects of prior safety analyses are adjudged inapplicable since response analysis was provided over limited and much less severe environment distributions or not provided at all. In particular, the launch pad explosion with its resultant overpressure, fragment environment, fireball and Δv impulse effects is cited. For accidents resulting in atmospheric reentry, consequences of heat source release are not vehicle-sensitive and results of prior analysis may be applicable. However, the IUS is currently in the development stage and future studies should critically examine the potential failure modes to provide better estimates of abort probabilities and ascertain that all abort situations with relatively high probabilities and/or particularly severe consequences in terms of fuel release are included in safety analysis.

The remainder of this section will attempt to examine the implication of the study with respect to the KIPS. The question addressed is: does the inclusion of the MHW IHS in the KIPS increase or decrease the capability of the IHS to survive launch abort environments? For the most part, the question remains unanswered because of the preliminary nature of the accident environment definition. However, some information was gained and is presented as follows.

1. Overpressure Environment

Stress analyses showed some variation with respect to the tendency of the primary heat source containment to breakup and release the heat source. However, differences are small and essentially inconsequential with respect to the projected overpressure environments. For most launch pad accidents heat source release or even aeroshell destruction is a virtual certainty.

2. Fragmentation

Here again, the retarding effects on ET fragments of primary heat source containment members show minor variations.

3. Atmospheric Reentry

(a) Initial temperatures - Initial heat source temperature at release to the atmosphere were selected at random from a range of temperatures which were characteristic of all power systems under study. This range was characteristic of initial temperatures with the possible exception of loss of nominal cooling prior to reentry. (information was not available at the time of the study.) Loss of coolant in the dynamic systems or loss of fluid from heat pipes on the RTG via micrometeoroid

damage or other failure mechanisms would tend to increase nominal heat source temperatures prior to reentry. Given sufficiently high initial temperatures, atmospheric heating could then possibly result in local PICS melting during reentry or high temperature on impact. Both of these effects would tend to further impair the capability of the PICS containment to survive impact.

However, the KIPS employs a multifoil emergency heat dump system (EHDS) intended to limit the increase of heat source temperature given a loss of coolant event. A recent test has verified the satisfactory response of this system. The EHDS will limit heat source temperature to essentially preclude the above mentioned detrimental effects.

(b) Atmospheric breakup - Breakup studies (breakup of reentry subsystems leading to heat source release) were performed for the specific power systems under study. The specific breakup requirement was attainment of the "zero strength" temperature of the 6061-T6 aluminum housing (heat source can) of 800° F. Depending on the reentry motion and initial flight conditions, release altitudes varied from an upper limit of 285000 ft to no release prior to impact. A review of these results indicates heat source release is a strong function of the motion of the residual reentering configuration. Reentering configurations varied from a spacecraft/PCS to configurations with residual IUS components plus spacecraft/PCS. The resultant motion (tendency to stabilize or not stabilize during atmospheric flight) was not significantly influenced by a particular PCS. Given Heat source release, temperature conditions of impact are only weakly dependent on release altitude. The MHW IHS is relatively insensitive to atmospheric heating and cooling effects.

According to the findings of this study, a tentative conclusion is that the possible detrimental effects of launch accidents are a strong function of the ability of the MHW heat source to survive the STS, IUS abort environments. At present, the power system tends neither to increase or decrease the inherent ability of the heat source to survive the environments.

1.0 PURPOSE AND SCOPE

The purpose of this report is to present a ground safety assessment, during Phase I of the KIPS program, of the KIPS conceptual flight system. Since much is yet unknown about the exact equipment, facilities and spacecraft, the safety aspects are scoped in concept rather than detailed specifications and procedures.

2.0 OBJECTIVE

The objective is to conduct a safety assessment to insure that all operations which must be performed on the heat source and power system prior to launch can be safely performed and are feasible for the selected KIPS flight concept.

3.0 CONCLUSIONS

The transportation, storage and handling of the KIPS IHS is expected to be accomplished in a manner similar to other MHW heat source programs. No additional risks should be expected in the KIPS program.

4.0 GROUND FLOW PLAN

A ground flow plan, shown in Figure 1, has been selected to serve as the basis for evaluating the safety aspects and feasibility of the flight concept. Selection of the ground flow plan followed a logical process in which many flow paths were considered. The flow paths receiving consideration (See Appendix A, Figure A-1)

FIGURE 1 - GROUND FLOW PLAN

GROUND FLOW PLAN - (Continued)

were limited to those in which the heat source and power system are shipped separately to the launch site (KSC) for assembly with the spacecraft. Most of the paths were disregarded as being unnecessarily complicated. Fueling in space seems the least desirable approach because of the additional launch weight due to support/fueling equipment and fueling personnel. Fueling in the orbiter bay before launch was considered undesirably time consuming, considering the probable restriction on activities in the shuttle. The most desirable approach appeared to be to load the IHS into the power system prior to installation in the orbiter.

The only consideration that remained was whether loading the IHS into the power system should come before or after the power system is mated to the spacecraft. At this point the discussion becomes somewhat less distinct since the Phase I KIPS radiator baseline design (4 ft. diameter x 9 ft. length) may not be optimum for use in the shuttle orbiter where a shorter, large diameter KIPS may be better suited. In the interest of limiting radiation exposure for spacecraft assembly personnel, loading the IHS after

KIPS is mated with the spacecraft appears to be the more desirable approach. This approach would allow mating the PCS to the spacecraft well in advance of the launch date, while the IHS may be installed some time later for final system checkout before spacecraft installation into the orbiter. However, due to the design of the baseline KIPS, fueling KIPS after mating with the spacecraft would be somewhat difficult and would probably require a more costly fueling facility. The baseline KIPS design, with the heat source assemblies located at the spacecraft end of the 4 x 9 radiator, is more accessible for fueling prior to mating with the spacecraft. Moving the heat source assemblies to the open end of the radiator, to allow fueling after mating with the spacecraft, would result in a significant weight penalty. However, it may be expected that a KIPS packaged for the space shuttle would use a large diameter radiator which would allow easy access to the heat source assemblies for fueling after being mated with the spacecraft. The proper sequence of events in a final GSAR is thus currently hampered by lack of definition of the spacecraft and the optimum radiator dimensions for the particular mission. The fueling scheme for the baseline design presented in this report, therefore, is to fuel prior to mating with the spacecraft.

5.0

HEAT SOURCE CONTAINERS

It is expected that the IHS would be shipped, from the fueling agency to the launch site, contained in the same or similar manner currently in use for the MHW heat source. The heat source would be contained in a Storage Protection Container (SPC) which provides mechanical and environmental protection for the heat source. The SPC would be used as an integral part of the Isotope Heat Source Shipping Container (IHS-SC) for transportation of the IHS. The SPC is shown in Figure A-2 of the Appendix. Figure A-3 (Appendix) is a pictorial of the IHS-SC. The SPC and IHS-SC are described in Reference 1.

6.0

HEAT SOURCE LOADING SEQUENCE AND FACILITY

Figure 2 presents a generalized loading sequence for KIPS. The loading sequence outlines the operations which must be performed for installing the IHS's into the power conversion system.

The KIPS loading facility, which is referred to as the loading and assembly station (LAS) in this report is shown pictorially in Figure 3. The LAS will provide for handling the IHS's; provide controls to maintain an inert environment during IHS installation; and provide radiation and thermal shielding for personnel

FIGURE 2

KIPS LOADING SEQUENCE

Step Number

1. Install Loading and Assembly Station (LAS) to Heat Source Assembly (HSA) No. 1.
2. Remove Electrical Heat Source (EHS) power cables.
3. Remove HSA end cover and Min-k insulation. (Stow in LAS)
4. Remove EHS from HSA using loading mechanism.
5. Remove EHS from LAS.
6. Inspect HSA prior to Isotopic Heat Source (IHS) loading.
7. Transfer IHS in shipping container to fueling area.
8. Remove Storage Protection Container (SPC) from IHS shipping container.
9. Disassemble SPC.
10. Remove Environmental Protection Container (EPC) from SPC and transfer EPC to LAS.
11. Install EPC into LAS; close and lock LAS hatch.
12. Evacuate and back fill LAS with inert gas.
13. Disassemble EPC.
14. Remove IHS from EPC using loading mechanism and perform visual examination of IHS.
15. Initiate HSA cooling.
16. Load IHS into HSA using loading mechanism.
17. Install HSA Min-k insulation and end cover.
18. Pressurize HSA and leak check.
19. Remove LAS from HSA No. 1 and install to HSA No. 2.
- 20 - 35. Repeat Steps 2 thru 18 (except Step 15) for IHS/HSA No. 2.
36. Remove LAS from HSA No. 2 and install to HSA No. 3.
- 37 - 52. Repeat Steps 2 thru 18 (except Step 15) for IHS/HSA No. 3.
53. Remove LAS from HSA No. 3.

FIGURE 3

CONCEPTUAL KIPS LOADING AND ASSEMBLY STATION (LAS)

6.0 HEAT SOURCE LOADING SEQUENCE AND FACILITY (Continued)

protection. Glove ports, view ports and tool locks will be incorporated to allow access to the components.

After disassembly of the IHS shipping container, the SPC would be disassembled near the loading station. The IHS, in its environmental protection container, would then be installed in the loading station.

7.0 PERSONNEL RADIATION EXPOSURE

Radiation dose rate measurements have been made on the HPG MOD 3 generator employing MHW heat source IHS HPF-2. This data, shown in Table I, was used for estimating personnel radiation exposure levels during IHS installation into the power system. Details of the personnel radiation exposure estimation are shown in Table A-I in the Appendix. The analysis assumes no radiation shielding is provided by the power system or the loading chamber. Exposures are whole body exposure. Exposure of hands and forearms would exceed the Table A-I values but are expected to be within established exposure limits. Fueling times and distances from the radiation sources were estimated based on expected maneuvers needed to accomplish the fueling operations. The radiation

TABLE I
APPROXIMATE RADIATION LEVELS
MHW IHS

<u>Distance from IHS center- inches</u>	<u>Neutron mrem/hr</u>	<u>Gamma mrem/hr</u>	<u>Total mrem/hr</u>
15	200	33	233
17	156	26	182
20	115	19	134
25	74	12	86
30	51	8.5	60
35	37	6.2	43
40	29	4.8	34
45	23	3.7	27

Notes

- (1) Total dose rate in the radial midplane of the cylindrical heat source - distance R measured from geometric center of heat source.
- (2) Dose rates are based on actual measurements performed on the HPG MOD 3 RTG employing heat source IHS HPF-2.

7.0 PERSONNEL RADIATION EXPOSURE (Continued)

exposure estimate should be considered preliminary.

The radiation exposure estimate uses two fueling technician positions, each position estimated to be exposed to slightly more than three rems during the fueling process. This indicates that more than two workers may be required to function as fueling technicians during a complete loading sequence. Also, depending on the number of fuelings scheduled for the quarter and year, additional fueling technicians may be desirable in order to minimize the number of workers for the year. Appropriate shielding would also limit the dosage.

8.0 REFERENCES

1. "Mult-Hundred Watt Radioisotope Program Final Safety Analysis Report", Volume I - Reference Design Document for LES 8/9, GEMS - 419, General Electric Company, March 1975

FIGURE A-1 - POTENTIAL GROUND FLOW PATHS

Figure A-2. Storage Protection Container (EPC not shown)
(Figure is from Reference 1)

Figure A-3. Isotope Heat Source Shipping Container

(Figure is from Reference 1)

TASK NO.	TASK DESCRIPTION	PERSONNEL RADIATION EXPOSURE (WITHOUT SHIELDING)														
		FUELING TECHNICIAN			FUELING TECHNICIAN			HEALTH PHYSICIST			QC REPRESENTATIVE					
		Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem
7	Transfer Isotope Heat Source Shipping Container (IHS-SC) No. 1 to fueling area.	0.4	86	34	0.4	86	34	0.2	86	17						
8	Remove Storage Protection Container (SPC) No. 1 from IHS-SC	0.5	233	116	0.5	233	116	0.2	233	47						
9	Disassemble SPC	0.6	233	140	0.6	233	140	0.2	233	47						
10	Remove Environmental Protection Container (EPC) from SPC and transfer EPC to LAS using overhead trolley.	0.5	233	116	0.5	233	116	0.1	233	23						
11	Install EPC into LAS; close and lock LAS hatch.	0.3	233	70	0.3	233	70	0.1	233	23						
12	Evacuate and backfill LAS with inert gas.	0.5	<10	<10	0.5	<10	<10									
13	Disassemble EPC	0.5	233	116	0.5	233	116	0.2	233	47						
14	Remove IHS from EPC using loading mechanism and perform visual examination of IHS.	0.3	233	70	0.3	233	70	0.1	233	23	0.2	233	47			
15	Activate HEA cooling.	0.1	---			---										

TASK NO.	TASK DESCRIPTION	PERSONNEL RADIATION EXPOSURE																	
		FUELING TECHNICIAN			FUELING TECHNICIAN			HEALTH PHYSICIST			QC REPRESENTATIVE			Min-K Technician					
		Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem
16	Load IHS into HSA using loading mechanism.	0.2	233	47	0.2	233	47												
17	Install HSA Min-K insulation and end cover.	0.2	233	47	0.2	233	47				0.1	233	23	0.4	233	93			
18	Pressurize HSA and leak check.	0.2	233	47	0.2	233	47	0.2	233	47	0.1	233	23						
19	Remove LAS from HSA No. 1 and install to HSA No. 2	0.7	134	94	0.7	134	94												
20	Remove EHS power cables.	0.2	70	14	0.2	70	14												
21	Remove HSA No. 2 end cover and Min-K insulation.	0.3	70	21	0.3	70	21												
22	Remove EHS from HSA No. 2 using loading mechanism.	0.2	70	14	0.2	70	14												
23	Remove EHS from LAS.	0.2	70	14	0.2	70	14												
24	Inspect HSA No. 2 prior to IHS loading.	0.2	70	14	0.2	70	14				0.2	70	14						
25	Transfer IHS No. 2 in shipping container to fueling area.	0.4	86	34	0.4	86	34	0.2	86	17									

TASK NO.	TASK DESCRIPTION	PERSONNEL RADIATION EXPOSURE																	
		FUELING TECHNICIAN			FUELING TECHNICIAN			HEALTH PHYSICIST			QC REPRESENTATIVE			Min-K Technician					
		Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem
26	Remove SPC from IHS No. 2 shipping container.	0.5	233	116	0.5	233	116	0.2	233	47									
27	Disassemble SPC	0.6	233	140	0.6	233	140	0.2	233	47									
28	Remove EPC from SPC and transfer EPC to LAS	0.5	233	116	0.5	233	116	0.1	233	23									
29	Install EPC into LAS; close and lock LAS hatch.	0.3	300	90	0.3	300	90	0.1	300	30									
30	Evacuate and backfill LAS with inert gas.	0.5	<10	<10	0.5	<10	<10												
31	Disassemble EPC	0.5	300	150	0.5	300	150	0.2	300	60									
32	Remove IHS No. 2 from EPC using loading mechanism and perform visual examination of IHS.	0.3	300	90	0.3	300	90	0.1	300	30	0.2	300	60						
33	Load IHS No. 2 into HSA using loading mechanism.	0.2	300	60	0.2	300	60												
34	Install HSA Min-K insulation and end cover.	0.2	300	60	0.2	300	60				0.1	300	30	0.4	300	120			
35	Pressurize HSA and leak check.	0.2	300	60	0.2	300	60	0.2	300	60	0.1	300	30						
36	Remove LAS from HSA No. 2 and install to HSA No. 3.	0.7	204	143	0.7	204	143												

[illegible]

TASK NO.	TASK DESCRIPTION	PERSONNEL RADIATION EXPOSURE																	
		FUELING TECHNICIAN			FUELING TECHNICIAN			HEALTH PHYSICIST			QC REPRESENTATIVE			Min-K Technician					
		Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem	Time hrs.	Rate mrem/hr	Dose mrem
46	Install EPC into LAS; close and lock LAS hatch.	0.3	396	89	0.3	396	89	0.1	396	40									
47	Evacuate and back fill LAS with inert gas.	0.5	< 10	<10	0.5	<10	<10												
48	Disassemble EPC.	0.5	396	198	0.5	396	198	0.2	396	79									
49	Remove IHS No. 2 from EPC using loading mechanism and perform visual examination of IHS.	0.3	396	119	0.3	396	119	0.1	396	40	0.2	396	79						
50	Load IHS No. 3 into HSA using loading mechanism.	0.2	396	79	0.2	396	79												
51	Install HSA Min-K insulation and end cover.	0.2	396	79	0.2	396	79				0.1	396	40	0.4	396	158			
52	Pressurize HSA and leak check.	0.2	396	79	0.2	396	79	0.2	396	79	0.1	396	40						
53	Remove LAS from HSA No. 3.	0.3	292	88	0.3	292	88												
	Total	16.6		3376	16.6		3376			881			418			371			

SECTION 7.0

QUALITY ASSURANCE

SECTION 7.0

QUALITY ASSURANCE

7.1 INTRODUCTION

For the Phase I KIPS program, extensive quality controls were imposed by the DOE. To accomplishing these controls, Sundstrand established many of the control techniques and procedures necessary for the Phase II Program. These techniques and procedures will form the base for the Phase II Quality Program Plan. This section contains (1) the Phase I Program Plan, (2) additions or redefinitions that will be made in the Phase II plan, (3) fabricability plan, (4) assembly procedures, and (5) inspectability plan.

7.2 PHASE I QUALITY ASSURANCE PROGRAM PLAN

The Phase I Quality Assurance Program Plan, N.R.A. 3071-012, Rev. B, is included as an appendix to this section of the report.

7.3 PHASE II QUALITY ASSURANCE PROGRAM PLAN

The Quality Plan for the KIPS Phase II effort will be consistent with the objectives of the U. S. Department of Energy NRA-1, Quality Assurance Program Requirements, dated July 1, 1977. The plan will be prepared and submitted for approval by DOE within sixty days after receiving the contract for Phase II.

The Sundstrand KIPS Phase I Quality Plan, N.R.A. 3071-012, Rev. B, will be used as baseline for the Phase II plan. The following concepts will be defined and added or redefined to upgrade the initial plan to a level commensurate with flight system requirements:

- Sundstrand Vendor Quality Assurance Pre-award Vendor Surveys will be required on all major and critical procurements. The survey emphasis will be an evaluation of facility and personnel capability in relation to the particular KIPS component being considered for placement. This requirement will include special nondestructive testing evaluation as well as the normal quality survey.
- Periodic audits by Sundstrand Vendor Quality Assurance will be performed on all major and critical procurements.
- KIPS test equipment design, fabrication and installation will be verified and monitored by the appropriate Sundstrand Quality section. This will include documentation and verification of existing and new facilities, station proofing, test engineering drawing approvals, and provisions for a "Break of Entry" system.
- Failure Review Board requirements will be added and defined.
- Indoctrination training of office personnel as well as floor personnel to unique KIPS requirements will be required.
- A section defining ground support equipment controls will be incorporated.
- A Quality Assurance Director "Statement of Authority" will be incorporated.
- Documentation control will be redefined to include the requirement that KIPS original data felt to be critical for program support will be maintained on file in one accessible area.
- Traceability requirements will be defined on the applicable engineering drawings.
- A separate section for NDT consistent with requirements of MIL-I-6870D will be incorporated. The NDT section will include Materials Laboratory analysis considerations.
- Configuration control requirements will be imposed to record the actual revision letter of the part used in the assembly operations.

7.4 NRA-1 COMPLIANCE ANALYSIS

A summary of the compliance to Document NRA-1 is listed below.

		*A	B	C
1.	Introduction			
1.1	Scope			
1.2	Applicability			
1.3	Relation to other contract requirements			
1.4	Actions and prerogatives of the Government	✓		
1.5	Appendix A, "Data Package"	✓		
2.	Management and Planning			
2.1	Quality Assurance program		✓	
2.2	Organization		✓	
2.3	Planning		✓	
2.3.1	Quality Program Plan contents		✓	
2.4	Training		✓	
2.5	Certification of personnel		✓	
2.6	Records	✓		
2.7	Documentation		✓	
2.7.1	Policies and Procedures		✓	
2.7.2	Quality Records		✓	
2.7.3	Quality Status reports		✓	
2.7.4	Audits and Reviews		✓	
3.	Quality Assurance personnel program participation and technical document review		✓	
3.1	Technical Documents		✓	
3.2	Quality Reviews		✓	
3.3	Quality Support to Design Reviews		✓	
3.4	Technical Document Control		✓	
3.4.1	Effectivity		✓	
4.	Traceability and Identification		✓	
4.1	Technical Documentation		✓	
4.2	Traceability		✓	
4.3	Identification		✓	
5.	Procurement		✓	
5.1	General		✓	
5.2	Selection of Contractor Procurement Source		✓	
5.3	Procurement documents		✓	

*A. We presently comply with this requirement as standard practice in our compliance to MIL-Q-9858A.

B. We will comply and implement full requirements in Phase II KIPS. Most of these elements were implemented and developed in Phase I.

C. We feel this requirement is not applicable due to small quantities, type processes or other related requirements which will perform the same job.

COMPLIANCE ANALYSIS OF QA DOC. NRA-1 FOR KIPS (cont'd)

		*A	B	C
5.3.1	Review		✓	
5.3.2	Contents		✓	
5.4	Contractor Quality Assurance personnel at source		✓	
5.5	Government Source Inspection	✓		
5.6	Receiving Inspection	✓		
5.7	Receiving Records		✓	
5.8	Coordination of Contractor-Supplier Inspections and Tests		✓	
5.9	Nonconforming of Procured Articles and Materials		✓	
5.10	Control of Procured Articles and Materials	✓		
6.	Fabrication and Assembly			
6.1	Planning		✓	
6.2	Article and Material controls	✓		
6.3	Fabrication and Assembly processes		✓	
6.4	Process Qualification		✓	
6.5	Cleanliness and Contamination control	✓		
6.6	Completed End Items	✓		
6.6.1	Modifications, Repairs or Replacements	✓		
6.7	Workmanship Standards			✓
7.	Inspections and Tests			
7.1	Inspection and Test Planning		✓	
7.2	Inspections and Tests		✓	
7.2.1	General requirements		✓	
7.2.2	Documentation		✓	
7.2.3	Records		✓	
7.2.4	Inspection and Test of major deliverable systems		✓	
7.2.5	Contractor Quality Assurance actions		✓	
8.	Nonconforming Articles and Materials			
8.1	Controls	✓		
8.2	Initial Review dispositions	✓		
8.3	Material Review Board	✓		
8.3.1	Membership	✓		
8.3.2	Responsibility	✓		
8.3.3	MRB Dispositions	✓		
8.4	Nonconformance reporting and Corrective Action (NOTE: It will be our discretion to determine when corrective action is required due to the small quantities.)	✓		
8.4.1	Nonconformance reporting	✓		
8.4.2	Corrective Action	✓		
8.4.3	Quality Trend Visibility	✓		

COMPLIANCE ANALYSIS OF QA DOC. NRA-1 FOR KIPS (cont'd)

		*A	B	C
9.	Calibration and Standards			
9.1	General	✓		
9.2	Equipment Evaluation	✓		
9.3	Equipment Control	✓		
9.4	Calibration Standards	✓		
9.5	Discrepant Equipment	✓		
10.	Stamps			
10.1	Stamp Control system	✓		
10.2	Stamp Restriction	✓		
11.	Handling, Preservation, Packaging, Storage, Shipping			
11.1	Handling	✓		
11.2	Preservation, Packaging and Storage	✓		
11.3	Shipping	✓		
12.	Statistical Quality Control Analysis			
12.1	General			✓
	(NOTE: We don't feel this section is applicable with the small quantities and type of processes involved.)			
12.2	Critical parts, Materials and Processes			✓
	(NOTE: We don't feel this section is applicable with the small quantities and type of processes involved.)			
Appendix A: Data Package			✓	

7.5 FABRICABILITY

The KIPS Phase II system has been designed such that the system can be manufactured within current state-of-the-art standards. All processes and procedures will be in accordance with existing DOE, ASTM, NASA, and Sundstrand standards.

To assure that the design meets established manufacturing processes and procedures, Sundstrand has assigned a producibility engineer to follow the FSCD through design, engineering, and detail drafting. During the design phase, the producibility engineer is involved with design reviews to ascertain that the design is cost effective and can be manufactured using established procedures. Redesign is performed where necessary. Any questionable manufacturing process is resolved through research or experimentation before approval of detail prints.

The manufacturing cycle begins with the preparation of processing and job instruction sheets coordinated with the responsible producibility engineer. All pertinent manufacturing information from the design phase is incorporated into these sheets.

The processing and job instruction sheets are reviewed by Quality Assurance Engineering to insure compliance with engineering requirements prior to adding inspection criteria and planning.

Critical manufacturing processes are controlled by Sundstrand or Military Standard procedures. All vendor sources must be certified before source approval is given. After approval, vendors are monitored by the Sundstrand Quality Assurance Department.

New contract awards are reviewed for existing production procedures; new requirements may require additional or revised procedures.

Processing sketches and job instruction sheets will be used in the manufacturing cycle with tolerances and dimensions maintained by quality controlled tooling. Manufacturing test specimens will be used for destructive testing prior to piece part manufacture, especially in the areas of welding, brazing, and heat treat.

The fabrication integrity designed into Sundstrand's ground demonstration unit is the basis of our criteria for the flight system. Additional controls and procedures may be imposed, as required, to be consistent with the Phase II requirements.

Special processes and procedures which will be used throughout the manufacture of the FSCD are listed in Table 7-A. Copies of these documents are available upon request.

Table 7-A Manufacturing Standards

<u>Process or Procedure</u>	<u>Sundstrand Document Number</u>	<u>MIL Spec.</u>
Cleanliness	PN14.57-01 PN14.50	
Manufacture	PN02.01 PN02.02 PN02.04	
Identify & Revise	PN17.50	
Anodize		MIL-A-8625
Passivation	PN14.10	
Chemical Film		MIL-C-5541
Electron Beam Welding	PN05.17	
Manual/Machine Welding	PN05.15	
Heat Treat	PN09	
Silver Plate		QQ-S-365
Brazing		MIL-B-7883
Tubing		MS 33611
Electric Soldering	PN05.06	
Conformal Coating	PN17.31	
Electrical Construction	PN17.21	
Electrical Varnish	PN17.28-05	
Lamination Bonding	PN17.26-10	
Torque of Threaded Fasteners	PN17.36	

7.6 ASSEMBLY PROCEDURES

The assembly of the KIPS will be controlled by a route card, a test procedure, and a job instruction sheet (JIS).

A route card is generated at the time each component design is completed. It details the operations step by step for assembly, inspection, test, special processes, and planning required. Each operation, as it is completed, is signed and dated by the individual performing the operation. This route card is maintained with the hardware until it has shipped or stocked at which time the route card is removed and retained in a central file.

Job Instruction Sheets (JIS) are issued for assembly operations that require extensive descriptions. The JIS breaks down the operation into single task steps, complemented with pictures where required. The JIS references all special gaging or tooling required to perform the operation. Signoff by the assembler and an inspection verification, on steps containing dimensional studies or hidden parts in subsequent steps, are required for each step.

After assembly and inspection, the system is transported to the test area. In the test area, in addition to the route card, test procedures are used to provide detailed sequences. A log book is provided to sign off completed sequences and inspection verification.

Table 7-B summarizes the assembly and pretest sequence for the KIPS.

Table 7-B KIPS Assembly/Test Sequence

7.7 INSPECTABILITY

Quality Assurance Engineering and Quality Special Process (NDE) Engineering have been and will continue to be participants in the KIPS Design Reviews in order to provide quality overview inputs and be certain detail and assembly integrity is capable of being verified.

Following completion of the design reviews, Sundstrand Quality Assurance Engineering, Quality Special Process Engineering, and Vendor Quality Assurance will provide a continuing quality effort by reviewing all KIPS engineering drawings prior to their release for production. The review will assure specifications, tolerances, classification of characteristics and unique requirements are adequately defined and can be realistically inspected. Experience gained on Phase I details and assemblies will be applied to the review.

Sundstrand vendors considered for participation in the KIPS Phase II effort will be reviewed by Sundstrand Vendor Quality Assurance and Quality Special Process Engineering (as required) prior to release of the subcontract. This review will evaluate facility and personnel capability in relation to inspectability requirements of the component being considered. Sundstrand Quality Special Process Engineering will be in attendance during first article inspections to establish and proof detail fabrication and NDT test procedures.

In-house fabrication procedures are controlled and defined by Manufacturing and Inspection Job Instruction Sheets to ensure that the intended inspectability is reduced to practice. Only personnel indoctrinated to KIPS requirements will be allowed to establish and define manufacturing and inspection efforts. In addition, in-house fabrication will be under KIPS Quality Assurance Engineering surveillance.

Plan No. QA5-107335

Revision B

Date July 22, 1977

SUNDSTRAND CORPORATION
QUALITY ASSURANCE PROGRAM PLAN
APPLICABLE TO
KIPS

REVISION B

DATE: July 22, 1977

APPROVAL SHEET

ENERGY SYSTEMS,
KIPS PROGRAM MANAGER

E. KRUEGER

QUALITY ASSURANCE MANAGER -
ROCKFORD

J. R. BOASE

QUALITY ASSURANCE ENGINEERING
SECTION MANAGER

W. M. SLOTA

ENERGY SYSTEMS, KIPS
PROJECT ENGINEERING MANAGER

G. SORENSON

REVISED BY: W. WALTON, KIPS Q.A. ENGINEER

TABLE OF CONTENTS

	<u>PAGE</u>	
1.	INTRODUCTION	1
1.1	SCOPE	1
1.2	APPLICABILITY	1
1.3	RELATION TO OTHER CONTRACT REQUIREMENTS	1
1.4	ACTIONS AND PREROGATIVES OF THE GOVERNMENT	1
1.5	APPENDIX A, "DATA PACKAGE"	1
2.	MANAGEMENT AND PLANNING	1
2.1	QUALITY ASSURANCE PROGRAM	1
2.2	ORGANIZATION	2
2.3	PLANNING	3
2.3.1	QUALITY PROGRAM PLAN CONTENTS	3
2.4	TRAINING	4
2.5	CERTIFICATION OF PERSONNEL	4
2.6	RECORDS	4
2.7	DOCUMENTATION	5
2.7.1	POLICIES AND PROCEDURES	5
2.7.2	QUALITY RECORDS	5
2.7.3	QUALITY STATUS REPORTS	5
2.7.4	AUDITS AND REVIEWS	5
3.	QUALITY ASSURANCE PERSONNEL PROGRAM	6
	PARTICIPATION AND TECHNICAL DOCUMENT	
	REVIEW	
3.1	TECHNICAL DOCUMENTS	6
3.2	QUALITY REVIEWS	6
3.3	QUALITY SUPPORT TO DESIGN REVIEWS	6
3.4	TECHNICAL DOCUMENT CONTROL	6
3.4.1	EFFECTIVITY	6
4.	TRACEABILITY AND IDENTIFICATION	6
4.1	TECHNICAL DOCUMENTATION	6
4.2	TRACEABILITY	7
4.3	IDENTIFICATION METHODS	7
5.	PROCUREMENT	7
5.1	GENERAL	7
5.2	SELECTION OF CONTRACTOR PROCUREMENT SOURCES	7
5.3	PROCUREMENT DOCUMENTS	7
5.3.1	REVIEW	7
5.3.2	CONTENTS	7
5.4	CONTRACTOR QUALITY ASSURANCE PERSONNEL AT	8
	SOURCE	
5.5	GOVERNMENT SOURCE INSPECTION	8
5.6	RECEIVING INSPECTION	8
5.7	RECEIVING RECORDS	8
5.8	COORDINATION OF CONTRACTOR-SUPPLIER	9
	INSPECTIONS AND TESTS	

TABLE OF CONTENTS
(Continued)

		<u>PAGE</u>
5.9	NONCONFORMING PROCURED ITEMS	9
5.10	CONTROL OF PROCURED ARTICLES & MATERIALS	9
6.	FABRICATION AND ASSEMBLY	9
6.1	PLANNING	9
6.2	ARTICLE AND MATERIAL CONTROLS	9
6.3	FABRICATION AND ASSEMBLY PROCESSES	9
6.4	PROCESS QUALIFICATION	10
6.5	CLEANLINESS AND CONTAMINATION CONTROL	10
6.6	COMPLETED END ITEMS	10
6.6.1	MODIFICATIONS, REPAIRS OR REPLACEMENTS	10
6.7	WORKMANSHIP STANDARDS	10
7.	INSPECTIONS AND TESTS	10
7.1	INSPECTION AND TEST PLANNING	10
7.2	INSPECTIONS AND TESTS	11
7.2.1	GENERAL REQUIREMENTS	11
7.2.2	DOCUMENTATION	11
7.2.3	RECORDS	11
7.2.4	INSPECTION AND TEST OF MAJOR DELIVERABLE SYSTEMS	11
7.2.5	CONTRACTOR QUALITY ASSURANCE ACTIONS	11
8.	NONCONFORMING ARTICLES AND MATERIALS	12
8.1	CONTROLS	12
8.2	INITIAL REVIEW DISPOSITIONS	12
8.3	MATERIAL REVIEW BOARD	12
8.3.1	MEMBERSHIP	13
8.3.2	RESPONSIBILITY	13
8.3.3	MRB DISPOSITIONS	13
8.4	NONCONFORMANCE REPORTING AND CORRECTIVE ACTION	13
8.4.1	NONCONFORMANCE REPORTING	13
8.4.2	CORRECTIVE ACTION	13
9.	CALIBRATION AND STANDARDS	13
9.1	GENERAL	13
9.2	EQUIPMENT EVALUATION	13
9.3	EQUIPMENT CONTROL	13
9.4	CALIBRATION STANDARDS	13
9.5	DISCREPANT EQUIPMENT	14
10.	STAMPS	14
10.1	STAMP CONTROL SYSTEM	14
10.2	STAMP RESTRICTION	14

TABLE OF CONTENTS
(Continued)

	<u>PAGE</u>
11. HANDLING, PRESERVATION, PACKAGING, STORAGE SHIPPING	14
11.1 HANDLING	14
11.2 PRESERVATION, PACKAGING AND STORAGE	15
12. STATISTICAL QUALITY CONTROL AND ANALYSIS	15
12.1 GENERAL	15
TABLE I DATA PACKAGE	16
KIPS Organization	17
MATRIX - KIPS QA5-107335	

KIPS QUALITY PROGRAM PLAN

1. INTRODUCTION

1.1 SCOPE

(B) This Quality Program Plan describes the manner in which the Energy Systems Unit of the Advanced Technology Group Division of Sundstrand Corporation applies its Quality Assurance Program and Systems to control and assure compliance to the Quality requirements imposed by SNS-1, Rev. 1, dated February 28, 1975 in support of the Kilowatt Isotope Power Systems (KIPS) Program (Phase I). Elements of the Sundstrand Quality Systems not in full compliance with the SNS-1 specification will be denoted by an asterisk (*).

The format of SNS-1, Rev. 1, has been employed in Quality Program Plan to allow for ease of cross referencing.

(B) A Matrix cross referencing paragraphs of this Plan to the Sundstrand Quality Assurance Manual is included herein.

1.2 APPLICABILITY

The applicability of this plan will be as defined herein.

1.3 RELATION TO OTHER CONTRACT REQUIREMENTS

The KIPS Quality Program Plan is to complement other contract requirements. This plan is constructed to be cost effective by utilizing existing organizational controls. Duplication of effort is avoided.

* 1.4 ACTIONS AND PEROGATIVES OF THE GOVERNMENT

ERDA's right to source inspection at Sundstrand or at major sub-contractors is acknowledged.

* 1.5 APPENDIX A, "DATA PACKAGE"

A suitable data package will be provided at the termination of contract as defined by Table I (attached).

2. MANAGEMENT AND PLANNING

(B) * 2.1 QUALITY ASSURANCE PROGRAM

The quality effort concerning the design phase, hardware procurement, fabrication, assembly and test will be a positive effort to establish a viable quality program.

Quality Assurance Engineering activities will include but not be limited to the following:

- a) Evaluate design compatibility with fabrication and inspection capabilities. Instigate corrective actions as necessary.
- b) Evaluate/audit vendor activity as applied to unique program requirements.
- c) Review component and GDS testing procedures. Monitor testing.
- d) Assure documentation of procurement, fabrication, assembly and test is sufficient for program evaluation requirements.
- e) Verify that procedures established are of sufficient detail to ensure reproducibility.
- f) Coordinate corrective actions.
- g) Document the above to Management.

The Quality Assurance Engineering involvement in the GDS design shall begin with the first design review. Quality Assurance Engineering shall be available to advise during conceptual design phase. Quality Assurance Engineering shall monitor design subsequent to the first GDS Design Review.

Quality Assurance Engineering shall review all items defined by Reliability Engineering as critical and shall require additional material and/or process controls where appropriate.

(B)

2.2 ORGANIZATION

The Quality Assurance Manager, Rockford, has complete responsibility for the administration and direction of the Quality Assurance efforts on the KIPS Program. He shall regularly report directly to high management.

The primary manufacturing facility for this program will be located at Plant 6, Rockford, Illinois. The responsibility of the implementation of the Standards, Procedures and Policies developed rests with the Rockford Quality Assurance Manager, Operations Division.

The organization of the Energy Systems Division and the Operations Division is depicted on the chart herein.

The major responsibilities of the Rockford Quality Assurance Manager are as follows:

- a. Proposal/Contract Review
- b. Quality Program Plan Development
- c. Customer Coordination
- d. Special System Audits
- e. Drawing and procedure review for specific program requirements
- f. Reports
- g. Program Q.A. Management
- h. Purchase Order Review
- i. Vendor Control
- j. Audits
- k. Drawing Review
- l. Procedure Approval
- m. Inspection Planning
- n. Gage Design and Procurement
- o. Change Board
- p. Record Retention
- q. NDE Engineering
- r. Process Control
- s. Nonconforming Material Review
- t. All other functions relating to part fabrication, assembly and tests.

2.3 PLANNING

The planning effort defined in this plan shall be supplemented by procedures, instructions, job instruction sheets and other appropriate documents as applicable.

This plan and subsequent revisions shall be submitted to ERDA for formal review and approval.

2.3.1 Quality Program Plan content is as follows:

- 2.3.1.1 Applicable sections of the Sundstrand Quality Assurance Manual are referenced herein by Section, Procedure, and/or Instruction number.
- 2.3.1.2 Departmental responsibilities will be as defined by this plan, referenced procedures and organizational charts.
- 2.3.1.3 Quality task descriptions, policies, and procedures are included in Section 2.2.
- 2.3.1.4 The Sundstrand coordinators for interface on matters concerning quality are:

ERDA-Sundstrand	Quality Assurance Engr. Mgr.
Sundstrand-Suppliers	Vendor Quality Assurance
Sundstrand-Sundstrand	Quality Assurance Engr. Mgr.

ERDA - Sundstrand's Suppliers - Not anticipated except on major subcontract with Teledyne in which case ERDA shall have direct access for routine matters. Quality problems should be coordinated with the Quality Assurance Engineering Manager.

(B)

- * 2.3.1.5 The flow of fabrication and assembly will be controlled by Route Cards prepared by Manufacturing Engineering with inspection point requirements verified by Quality Planning and Quality Assurance Engineering.

Details of fabrication and assembly will be described in Job Instruction Sheets and in referenced Process Procedures. Quality Planning and Quality Assurance Engineering review Route Cards, JIS's and subsequent revisions for approval. From these documents, and the print Quality Planning prepares an inspection JIS. The inspection JIS does not require approval outside of the Quality rganization.

(B)

2.4 TRAINING

All NDE personnel shall be qualified and certified in accordance with Q.A. Procedure 7.09.

All Welding personnel shall be qualified and certified in accordance with Q.A. Procedures and Q.A. Instructions.

Welding Inspection shall be accomplished in accordance with Q.A. Procedure 7.08 and suitable Q.A. Instructions.

Soldering personnel shall be trained and certified in accordance with Q. A. Instruction 4.04.15.

All personnel performing helium leak checks shall be qualified and certified in accordance with Q.A. Procedures and Q.A. Instructions to be developed by Sundstrand Aviation Quality Assurance.

Assembly & Test personnel will be indoctrinated to unique requirements applicable to the KIPS Program.

(B)

2.5 CERTIFICATION OF PERSONNEL

Included in 2.4 of this Quality Plan.

(B)

2.6 RECORDS

Records of training and certification shall be maintained by Sundstrand Quality Assurance.

Recertification shall be as required in 2.4.

2.7 DOCUMENTATION

2.7.1 POLICIES AND PROCEDURES

This quality plan is augmented by Standard Policy Documents, Instructions and other technical documents.

2.7.2 QUALITY RECORDS

Sundstrand Aviation Quality Assurance shall be responsible for the maintenance of quality records applicable to program requirements. Quality records shall be presented to ERDA for review upon request.

(B)

* 2.7.3 QUALITY STATUS REPORTS

Sundstrand Quality Assurance Engineering shall submit monthly reports of all quality activities to program management for incorporation into monthly reports to ERDA. The reports shall include a brief narrative of all Quality Program accomplishments, progress and action item objectives. MRB files shall be audited monthly to determine trends. MRB statistics and trends shall be incorporated into a monthly report. Copies of Sundstrand Malfunction & Trouble Report/Event Record (Form 6811) will be included in the Monthly Report. Summaries of unique program audits shall be incorporated into the appropriate monthly reports.

(B)

2.7.4 AUDITS & REVIEWS

* 2.7.4.1 Quality Audits

Routine company wide audits will be conducted in accordance Q.A. Procedure 1.07 and Q.A. Instruction 1.07.01 by Sundstrand Quality Assurance on a frequency of no less than once a year. Summaries of these audits will be available for on site review.

Unscheduled and/or special audits shall be conducted in a manner similar to the above mentioned routine audits as directed by the Q.A. Manager. To avoid duplication of effort only program unique features must be audited on at least an annual basis. Summaries shall be provided to ERDA.

* 2.7.4.2 Management Reviews

Quality documentation and reports shall provide management visibility into the overall quality effort. Formal Quality Program reviews will be held when deemed necessary by management.

3. QUALITY ASSURANCE PERSONNEL PROGRAM PARTICIPATION AND TECHNICAL DOCUMENT REVIEW

(B) 3.1 TECHNICAL DOCUMENTS

The required documents are prepared as standard operating practice. Sundstrand specifications and standards shall require the review and approval of Sundstrand Quality Assurance.

(B) * 3.2 QUALITY REVIEWS

The Quality Assurance Engineering objectives described in Para. 2.1 apply. Quality Assurance Engineering will participate in all phases of the KIPS Program activity including review and documentation (i.e. Engr. Dwg. review and sign-off, MTR review, etc.).

(B) 3.3 QUALITY SUPPORT TO DESIGN REVIEWS

Quality Assurance Engineering shall participate in all design and change review activity related to KIPS and shall have responsibility to notify the Program Manager and Quality Assurance Manager of proposed changes which affect interface characteristics.

Drawings and changes shall require Quality Assurance approval. Compliance to Q.A. Procedure 2.02 and Q.A. Instruction 2.02.06 shall be required.

(B) * 3.4 TECHNICAL DOCUMENT CONTROL

Each department which maintains a controlled drawing file is charged with the responsibility for filing new drawings distributed to them and removing obsolete ones. Sundstrand Quality Assurance audits controlled drawing files for conformance to current requirements. Audits are conducted on a random basis at an interval not to exceed one year. Where a file is found deficient, additional follow up audits are made.

(B) 3.4.1 EFFECTIVITY

Shall comply with Sundstrand Policy 4-02, 4-3, 4-05 and 4-06.

4. TRACEABILITY AND IDENTIFICATION

(B) 4.1 TECHNICAL DOCUMENTATION

Methods, location and information to be employed in marking shall be defined on the engineering print per Sundstrand PN 17.50.

* 4.2 TRACEABILITY

Records for articles and materials shall indicate applicable part or type numbers and detailed identification. Records shall provide the capability of tracing the material from which the fabrication originated to determine the location of like articles or raw materials within a level of process or assembly.

GDS non-critical hardware may not have full material traceability.

4.3 IDENTIFICATION METHODS

Identification methods will be as defined by engineering print.

5. PROCUREMENT

5.1 GENERAL

Sundstrand accepts the responsibility for the adequacy and quality of all contractor purchased articles, materials and services.

(B) * 5.2 SELECTION OF CONTRACTOR PROCUREMENT SOURCES

Sources shall be selected in accordance with Sundstrand Q.A. Procedure 3.01.

5.3 PROCUREMENT DOCUMENTS

(B) * 5.3.1 REVIEW

Quality Assurance Engineering shall review purchase requests and purchase orders. Revisions to the quality requirements imposed on purchase requests will require Quality Assurance approval.

(B) * 5.3.2 CONTENTS

Review of procurement contents will be in accordance with Sundstrand Q.A. Procedure 3.01. Government Source Inspection (GSI) is not contemplated except on the major sub-contract to Teledyne. All applicable program requirements shall be imposed on the Teledyne contract. Subcontractor exceptions will require ERDA approval prior to Sundstrand acceptance.

It is assumed that 5.3.2c (12) applies to other than standard commercial or off-the-shelf procurements.

Control of age sensitive materials depends on many factors but at a minimum material is dated upon receiving. Material drawn from stock is examined to assure useful life prior to use. Out of date materials are scrapped.

Sundstrand's proprietary processes shall be open for ERDA review where required. Use of vendor proprietary products and/or processes will be discouraged. Where requirements exist for proprietary products and/or processes and where a high degree of Quality cannot be assured by examination and testing, then Sundstrand shall attempt to secure one of the modes of assurance in, SNS-1, Rev. 1, paragraph 5.3.2c. (14), a. through 3., if such can be achieved with minimal impact on cost, schedule, and other program requirements.

(B) 5.4 CONTRACTOR QUALITY ASSURANCE PERSONNEL AT SOURCE

As defined by Sundstrand Q.A. Procedure 3.01 and Sundstrand Q.A. Instruction 3.01.05.

5.5 GOVERNMENT SOURCE INSPECTION

It is acknowledged that GSI does not relieve Sundstrand of the responsibility for inspection. Reference Section 5.3.2 for additional information.

(B) * 5.6 RECEIVING INSPECTION

Receiving Inspection shall be performed in accordance with Sundstrand Q.A. Procedure 3.02. Periodic disassembly per Section 5.6 (4) will not be performed unless specific purchased assemblies requiring such inspection are identified by Sundstrand Engineering.

Receiving Inspection shall at a minimum require that age sensitive materials be marked with cure date and discard date.

Raw material random samples shall be periodically obtained to allow for verification of reported chemical and mechanical properties prior to material release.

(B) * 5.7 RECEIVING RECORDS

Records as required in Section 5.6 are maintained, however, traceability to unserialized non-critical components when more than one lot is received is not maintained once acceptance is assured.

5.8 COORDINATION OF CONTRACTOR - SUPPLIER INSPECTION AND TESTS

Supplier coordination will be as defined in Section 5.4.

(B) * 5.9 NONCONFORMING PROCURED ITEMS

Nonconforming items shall be handled in accordance with Sundstrand Q.A. Procedure 6.01. Resubmittal of rejected items requires the supplier to identify the reject tag number. Only items for which acceptable rework is possible are eligible for resubmittal. Receiving Inspection verification shall be by reinspection (physical characteristics) and/or vendor documentation as applicable.

Should a supplier wish to use nonconforming items, the supplier must submit a "Vendor's Request for Material Review Action", Form 6197B.

Due to the limited quantities, supplier corrective action may not always be required.

(B) 5.10 CONTROL OF PROCURED ARTICLES AND MATERIALS

Procured items shall be controlled in accordance with Sundstrand Q.C. Procedure 4.05 and Sundstrand Q.C. Instruction 4.05.01.

6. FABRICATIONS AND ASSEMBLY

(B) 6.1 PLANNING

Planning shall be performed in accordance with the standard route card and job instruction sheet (JIS) system which shall provide sequence and instruction for fabrication, assembly and test inspection operations. Quality Assurance Engineering will monitor Planning efforts for completeness and compliance to program objectives.

6.2 ARTICLE AND MATERIAL CONTROLS

Items shall be controlled by Route Cards with identification control as defined by Engineering prints being specified.

(B) * 6.3 FABRICATION AND ASSEMBLY PROCESSES

Fabrication and assembly processes shall be controlled as defined by Section 6.1. Processes and Testing shall be performed to written procedures which shall be reviewed by Quality Assurance. Approval for use shall require that environmental considerations be controlled and that special fixtures be identified.

Process flow charts shall not be utilized due to hardware lot sizes.

(B) * 6.4 PROCESS QUALIFICATION

Standard manufacturing practices are controlled by Sundstrand Production Procedures (PN's). Formal rehearsal of process with ERDA acceptance is not applicable to KIPS (Phase I) program.

Use of new processes that are developed for KIP's application and where high quality cannot be verified after completion, shall be qualified and require the approval of Q.A. Engineering and Project Engineering. A list of these processes shall be maintained by Q.A. Engineering and reported in status report.

(B) 6.5 CLEANLINESS AND CONTAMINATION CONTROL

Sundstrand Quality Assurance shall require facilities cleanliness and related cleanliness operations as required to obtain cleanliness requirements as specified on the engineering prints per CPL4.57-01, the KIPS General Precision Cleaning Document, or the Supplements thereof. Should problems related to cleanliness arise during the course of the program Quality Assurance shall impose such additional requirements as experience indicates is required.

6.6 COMPLETED END ITEMS

Test and inspection of end items prior to delivery shall be performed in accordance with Engineering prints and design specifications.

(B) 6.6.1 Modification, Repairs or Replacements

Modification, repair shall be performed in accordance with written instructions. Quality Assurance shall inspect and shall verify acceptance of the activity. Retest shall be as determined by Project Engineering and shall require Quality Assurance concurrence.

* 6.7 WORKMANSHIP STANDARDS

Samples and visual aids are not applicable to KIPS (Phase I) Program unless specified on Engineering prints or design specification. Use of samples and visual aids is not anticipated. Workmanship is controlled by drawings, process procedures and formal inspection instructions.

7. INSPECTION AND TESTS

(B) * 7.1 INSPECTION AND TEST PLANNING

Test Engineering prepares test plans which require the review and approval of Sundstrand Quality Assurance prior to use. Inspection Planning is the responsibility of Sundstrand Quality Planning.

7.2 INSPECTIONS AND TESTS

7.2.1 General Requirements

Sundstrand Quality Assurance Engineering shall verify that testing is in accordance with approved procedures, that calibrated instrumentation is employed and that nonconformances are documented. Cause and corrective action investigation will be made for all nonconformities occurring during GDS qual tests.

7.2.2 Documentation

Procedures shall include accept/reject criteria and the documentation requirements. Sundstrand Quality Assurance shall review procedures and conformance.

Nonconformities and events (other than problems) encountered during assembly and test of hardware in-house will be documented per QA Instruction 5.01.08 utilizing the Malfunction Trouble Report/Event Record (Form 6811).

7.2.3 Records

Applicable quality records shall be maintained in accordance with the standard record retention system.

* 7.2.4 Inspection and Test of Major Deliverable Systems

Sundstrand Quality Assurance shall review proposed procedures for compliance to contract requirements.

Project Engineering shall coordinate test operations which incur abnormal risk with the Quality Assurance Manager. The applicable tests may be subject to formal rehearsal with ERDA's surveillance prior to proceeding with actual test as determined by Sundstrand Project Engineering and Quality Assurance Engineering.

* 7.2.5 Contractor Quality Assurance Actions

Prior to Testing:

- a. Sundstrand Quality Assurance (SQA) Engineering shall verify that applicable inspection and test documents are complete, available and unambiguous.
- b. SQA shall verify that requirements for control of test articles are met and that test constraints are resolved.
- c. SQA shall ensure test articles are properly identified.

- d. SQA shall verify configuration of test articles.
- e. SQA shall verify GSE and article configuration consistency.
- f. SQA shall verify that test equipment is calibrated.

During Testing:

- a. SQA shall ensure that testing is accomplished in accordance with test procedures.
- b. SQA shall verify accurate and complete data is recorded.
- c. SQA shall document repair and/or rework.
- d. SQA shall document nonconformances and shall participate in their disposition.

Subsequent to Testing:

- a. SQA shall ensure proper disposition of articles.
- b. SQA shall document any additional nonconformances and participate in their disposition.
- c. SQA shall ensure remedial and preventive action relative to nonconformances is in effect.
- d. SQA shall verify that test results are accurate, complete and traceable to the unit tested.

8. NONCONFORMING ARTICLES AND MATERIALS

8.1 CONTROLS

Control, review and disposition of nonconforming material shall be performed in accordance with Sundstrand Q.A. Procedure 6.01.

8.2 INITIAL REVIEW DISPOSITIONS

Initial review is covered in Section 3.3 of Sundstrand Q.A. Procedure 6.01.

* 8.3 MATERIAL REVIEW BOARD

MRB shall conform to Sundstrand Q.A. Procedure 6.01. ERDA review will not be required prior to implementing MRB actions.

All Class I MRB's will be reported to ERDA for information purposes within 24 hours of disposition.

* 8.3.1 Membership

Sundstrand reserves the right to change MRB membership without prior ERDA approval.

ERDA representation on MRB is accepted only if a representative is available for timely disposition.

* 8.3.2 Responsibility

Responsibility is as defined in Section 8.1.

8.3.3 MRB Disposition

Disposition is as defined in Section 8.1.

8.4 NONCONFORMANCE REPORTING AS CORRECTIVE ACTION

* 8.4.1 Nonconformance Reporting

Reporting shall be in accordance with Sundstrand Q.A. Instruction 6.01.01. Detailed MRB action shall be provided for ERDA on site review. Formal summaries will be transmitted as part of quality status reports.

8.4.2 Corrective Action

Corrective Action is as defined in Section 8.4.1.

9. CALIBRATION AND STANDARDS

(B)

9.1 GENERAL

Sundstrand Quality Assurance shall be active in the selection, calibration, adjustment, maintenance and control of inspection, measuring and test equipment per applicable policies and instructions in Section 8 of the Sundstrand Quality Assurance Manual.

9.2 EQUIPMENT EVALUATION

Special test equipment such as checkout consoles shall be tested to assure that the objective of the test procedure is obtainable.

9.3 EQUIPMENT CONTROL

Control shall conform to Sundstrand Q.A. Procedure 8.01.

9.4 CALIBRATION STANDARDS

Sundstrand or outside calibration standards may be used and shall be traceable to NBS. Environmental controls shall be exercised as necessary.

(B)

* 9.5 DISCREPANT EQUIPMENT

In order to provide cost effectivity only those gages and/or test equipment which are special equipment assigned to the KIPS Program for end item acceptance will be controlled for the purpose of identifying possible discrepant items due to out of calibration conditions. When discrepancies in inspection, measuring and test equipment are found at calibration, a Malfunction Trouble Report/Event Record (Form 6811) will be initiated to document and determine what corrective action and/or retesting is required.

10. STAMPS

* 10.1 STAMP CONTROL

Sundstrand Quality Assurance shall control stamps in accordance with Sundstrand Q.A. Procedure 1.04 and Sundstrand Q.A. Instruction 1.01.01 and 1.04.02.

It is the obligation of inspection supervisors to determine inspector qualifications and to allow only qualified personnel to perform inspection.

The qualifications and training of all personnel, to whom stamps are issued, are not necessarily documented. Documentation is required for certain skills (see 2.4 of this plan) and is available for ERDA review on site. Much training is on the job. Close supervision is maintained on the job to assure proper training, qualification and performance. This process gives the supervisor insight to skills and allows proper job assignment.

Special training is conducted from time to time as required without formal documentation, to insure the concerned supervisor that the skills required are available. As an example when new and complex equipment is purchased the vendor would conduct training classes.

10.2 STAMP RESTRICTION

Sundstrand Q.A. Instruction 1.04.01, Appendix I for illustration of typical Sundstrand stamps. "ERDA" designation is not utilized.

11. HANDLING, PRESERVATION, PACKAGING, STORAGE AND SHIPPING

11.1 HANDLING

Requirements for special handling shall be at the direction of Project Engineering, Manufacturing Engineering and Quality Assurance. Sundstrand Quality Assurance Engineering shall have ultimate responsibility for verifying that acceptable handling procedures are implemented. Quality shall review and approve all special handling procedures prior to use.

11.2 PRESERVATION, PACKAGING AND STORAGE

Special requirements for preservation, packaging and storage shall be denoted on the engineering drawing.

When not specified, standard requirements shall apply.

Quality Assurance shall verify compliance to special and standard requirements.

12. STATISTICAL QUALITY CONTROL AND ANALYSIS

* 12.1 GENERAL

Sampling plans used by Sundstrand are described in Sundstrand Q.A. Instruction 3.02.08, 4.01.02 and 4.02.03.

Statistical analysis to evaluate trends and shifts in critical processes is not applicable to KIPS (Phase I).

TABLE I

DATA PACKAGE REQUIREMENTS

The Data Package shall consist of the following:

1. Title Page
2. Operating Log
3. Bill of Materials
4. Record of As-Built-Configuration
5. Replacement Record - See Operating Log
6. Weight and Balance - See Engineering Report
7. Test Data and Procedures
8. MRB Records
9. Drawings - Top and first tier only with product specifications
10. Operating Instructions for GDS
11. MTR and Event Records

KIPS ORGANIZATION

The accompanying chart is presented to show the Sundstrand organization elements which are directly involved in the KIPS program.

The KIPS program is in the Energy Systems Unit of the Sundstrand Corporation. The Program Manager is directly responsible to the Energy Systems General Manager for the successful operation of all aspects of the program.

The three product line units, Aviation Mechanical, Electric Power and Energy Systems, in the Advanced Technology Group are shown along with the Operations unit. The Operations unit supports the three product line units in the functional areas of Engineering (Research, Test Design), Production (Material, Quality Assurance, Manufacturing) and Administration (Data Control, Management, Accounting, Pricing).

For specific programs such as KIPS, it is the responsibility of the Reliability, Quality Assurance and Hardware Managers to assign individuals to support the program and functionally report to the Program Manager. For major subcontractors such as Teledyne, the Materials Department of the Operations unit is responsible for assigning an individual to the program to perform the contractual interface function with the subcontractor.

In the Operations unit, the Vice President of Engineering is responsible for the research, test and design functions. Due to the nature of the KIPS program, a Research Engineering Manager has been assigned to functionally work within the program organization. The test and design functions are directed by task assignment originating from the KIPS Project or Research Engineering Managers.

Likewise, the Contracts Manager in the Energy Systems section has assigned Program Control and Cost Control personnel to functionally report to the KIPS Program Manager.

Figure 1 KIPS Program Organization

QUALITY ASSURANCE PROGRAM MATRIX

DATES

ORIGINAL:

REVISION:

EFFECTIVE:

NUMBER:

REVISION:

PAGE 1 OF 7

ORIGINATED BY:

PROGRAM:

KIPS

PROGRAM REQUIREMENT

SUNDSTRAND DOCUMENT NUMBER

O.A. Inst. &/or Proc.

1.

1.1 thru 1.5

2.

2.1

2.2

2.3

1.01

2.3.1

2.3.1.1 thru
2.3.1.5

1.01.01

2.4

4.04.15 7.08
7.09.01 1.02
7.09.02 7.08.01

7.09.01 Denver
7.09.02 Denver

2.5

Same as 2.4

2.6

Same as 2.4

2.7

2.7.1

1.01

N/R = Not Required

NAD = Not Applicable Denver

NOT IN 19

FOR EXTERNAL DISTRIBUTION

Form 65-729A

QUALITY ASSURANCE PROGRAM MATRIX

DATES

ORIGINAL:

REVISION:

EFFECTIVE:

NUMBER:

REVISION:

PAGE 2 OF 7

ORIGINATED BY:

PROGRAM:

KIPS

PROGRAM REQUIREMENT

SUNDSTRAND DOCUMENT NUMBER

	Q.A. Inst &/or Proc.		
2.7.2	1.06		
2.7.3	6.01 5.01.08		
2.7.4	1.07		
2.7.4.1	1.07 1.07.06 Denver 1.07.01		
2.7.4.2	1.07		
3.1			
3.2			
3.3	2.02 2.02.06 2.02.01 Denver		
3.4	2.02.03 2.02.01 Denver 2.02.02 Denver		
3.4.1	2.02.01 2.02.01 Denver 2.02.02 Denver		
4.			
4.1			
4.2	1.06		

N/R = Not Required

NAD = Not Applicable Denver

NOT INTENDED FOR

INTERNAL DISTRIBUTION

Form 65-729A

QUALITY ASSURANCE PROGRAM MATRIX

DATES**ORIGINAL:****REVISION:****EFFECTIVE:****NUMBER:****REVISION:**PAGE 3 OF 7**ORIGINATED BY:****PROGRAM:**

KIPS

PROGRAM REQUIREMENT**SUNDSTRAND DOCUMENT NUMBER**

	Q.A. Inst &/or Proc.		
4.3	.		
5.			
5.1			
5.2	3.01.03 3.01.06 Denver 3.01 3.01.06		
5.3			
5.3.1	002-1		
5.3.2	3.01 002-1	3.02.02 Denver	
5.4	3.01.05 3.01.06 Denver 3.01		
5.5			
5.6	3.02 3.02.01 Denver 002-14	3.02.02 Denver	
5.7			
5.8	3.01.10 3.01.08 3.01.06 Denver 3.01 3.01.05		
5.9	6.01	Directive (New) 6.01.--	

N/R = Not Required

NAD = Not Applicable Denver

NOT INTENDI 21 OR EXTERNAL DISTRIBUTION

Form 65-729A

QUALITY ASSURANCE PROGRAM MATRIX

DATES

ORIGINAL:

REVISION:

EFFECTIVE:

NUMBER:

REVISION:

PAGE 4 OF 7

ORIGINATED BY:

PROGRAM:

KIPS

PROGRAM REQUIREMENT

SUNDSTRAND DOCUMENT NUMBER

5.10

4.05
4.05.01, Denver
4.05.01

6.

6.1

4.01

6.2

5.01

6.3

4.01
5.01

6.4

6.5

6.6

5.01

6.6.1

6.7

7.

7.1

5.02

7.2

N/R = Not Required

NAD = Not Applicable Denver

NOT INTL 22 D FOR EXTERNAL DISTRIBUTION

Form 65-729A

QUALITY ASSURANCE PROGRAM MATRIX

DATES

ORIGINAL:

REVISION:

EFFECTIVE:

NUMBER:

REVISION:

PAGE 5 OF 7

ORIGINATED BY:

PROGRAM:

KIPS

PROGRAM REQUIREMENT

SUNDSTRAND DOCUMENT NUMBER

	Q.A. Proc &/Or Inst		
7.2.1			
7.2.2			
7.2.3	1.06 1.06.01 Denver		
7.2.4			
7.2.5			
8.	Section 6 of Q.A.I.		
8.1	6.01	6.01.02 Denver	
8.2	6.01	6.01.01 Denver	
8.3	6.01	6.01.02 Denver	
8.3.1	6.01		
8.3.2	6.01		
8.3.3	6.01		
8.4	6.01.03 Denver		

N/R = Not Required

NAD = Not Applicable Denver

NOT INTEND 23 OR EXTERNAL DISTRIBUTION

Form 65-729A

QUALITY ASSURANCE PROGRAM MATRIX

DATES

ORIGINAL:

REVISION:

EFFECTIVE:

NUMBER:

REVISION:

PAGE 6 OF 7

ORIGINATED BY:

PROGRAM:

KIPS

PROGRAM REQUIREMENT

SUNDSTRAND DOCUMENT NUMBER

	Q.A. Inst &/or Proc.		
8.4.1	6.01.03. Denver	6.01.03, Appendices I thru XI Denver	
8.4.2	Same as 8.4.1		
9.	Section 8 of Q.A. Manual		
9.1			
9.2			
9.3	8.01		
9.4	8.01.01 Denver		
9.5			
10.			
10.1	1.04.01, 1.04.02 & 1.04.03 Denver		
10.2	1.04.01, 1.04.02 & 1.04.03 Denver		
11.			
11.	4.05	4.05.01	

N/R = Not Required

NAD = Not Applicable Denver

NOT INT 24 ID FOR EXTERNAL DISTRIBUTION

Form 65-729A

SECTION 8.0
RELIABILITY PLAN

SECTION 8.0

RELIABILITY PLAN

This section contains the KIPS preliminary reliability program for Phase II; the difference between the Phase I and Phase II plans; the reliability prediction analysis; the failure modes, effects, and criticality analysis (FMECA); and a preliminary single point failure evaluation.

The preliminary Phase II reliability program plan (subsection 8.1) is substantially unchanged from the Phase I plan. Significant changes from the Phase I plan are presented in subsection 8.2.

Subsection 8.3 presents the results of the reliability prediction estimation. The rationale and data base for the failure rate estimation are included on the tabular prediction sheets. The reliability goal for KIPS is 0.93 for seven years.

The FMECA tabulation is presented in subsection 8.4. Credible failure modes together with possible failure effects are discussed. Based on the results of the FMECA, a single point failure listing is presented in subsection 8.5.

The material presented in this section is intended to serve as a starting point for defining the Phase II reliability program.

8.1 PHASE II RELIABILITY PLAN

A preliminary reliability program plan for Phase II is included in this subsection of the report. This plan evolved from the Phase I plan.

Sundstrand Corporation
Advanced Technology Group

- SUNDSTRAND AVIATION ELECTRIC POWER
- SUNDSTRAND AVIATION MECHANICAL
- SUNDSTRAND ENERGY SYSTEMS
- SUNDSTRAND OPERATIONS
- SUNDSTRAND MACHINE TOOL

4747 HARRISON AVENUE • ROCKFORD, ILLINOIS 61101
(815) 226-6000 • TWX 910-631 4255 • TELEX 257-440

PRELIMINARY
RELIABILITY PROGRAM PLAN
FOR THE
KILOWATT ISOTOPE POWER SYSTEM (KIPS)
PHASE II

Sundstrand Report Number RE-3475

Prepared by *Don J. Nonneman* Date 2-24-78
Reliability Engineer

Approved by *William F. Carpenter* Date 3-1-78
Group Engineer, Reliability and Qualification

Approved by *Bob Key* Date 3-1-78
Section Mgr., Qualification Test and
Reliability Engineering

Approved by *Earl Kuegel* Date 3-1-78
KIPS Program Manager

TABLE OF CONTENTS

	<u>PAGE</u>
1.0 INTRODUCTION	2
1.1 Scope	2
2.0 GENERAL PROGRAM REQUIREMENTS	2
2.1 Purpose	2
2.2 Plan Preparation	3
2.2.1 Revisions	3
2.2.2 Implementation	3
3.0 ORGANIZATION AND DOCUMENTATION	3
3.1 Organization and Management	3
3.1.1 Reliability Organization	3
3.1.2 Reliability Manager	4
3.1.3 Interface with Other Organizations	4
3.1.4 Personnel and Training	4
3.2 Program Documentation	5
3.2.1 Reliability Milestones	5
3.2.2 Program Reviews	5
3.2.3 Facilities Reports	5
3.2.4 Progress Reports	5
3.2.4.1 Progress Report Content	5
3.2.4.2 Reports of Meetings	6

	<u>PAGE</u>
4.0 DESIGN RELIABILITY ELEMENTS	6
4.1 Design Specification	6
4.2 Reliability Design	7
4.2.1 Expected Environments	7
4.3 Systems Variables Analysis	7
5.0 RELIABILITY ENGINEERING PROGRAM ELEMENTS	8
5.1 Reliability Goal	8
5.2 Demonstrated Reliability	8
5.3 Reliability Participation and Analysis	8
5.4 Failure Modes, Effects and Criticality Analyses (FMECA)	8
5.4.1 Failure Modes and Ranking	8
5.4.2 Failure Effects and Ranking	9
5.4.3 Criticality	10
5.4.4 Failure Mode Elimination	10
5.4.5 FMECA Reporting	10
5.5 System Logic Synthesis	10
5.5.1 Logic Diagrams	11
5.5.2 Probability Equations	11
5.5.2.1 Allocations	11
5.5.2.2 Assessment	11

	<u>PAGE</u>
5.5.2.3 Sensitivity Analysis	12
6.0 TEST PROGRAM	12
6.1 Purpose	12
6.2 Requirements	12
6.3 Data Sources	13
6.4 Failures and Corrective Action	13
6.4.1 Failure Definition	13
6.4.2 Failure Reporting	13
6.4.2.1 Description and Analysis	13
6.4.3 Failure Review Board	13
7.0 MAINTAINABILITY	16
7.1 Maintenance Free Design	16
7.2 Tolerance Control	16
7.3 Maintenance and Operation Analysis	16
8.0 HUMAN FACTORS ANALYSIS	16
8.1 Human Problems and Failures	16
8.2 Reports	16
FIGURE 1 KIPS Program Organization	17
FIGURE 2 TASK AND MILESTONE SCHEDULE	18
FIGURE 3 FMECA FORM	19

KIPS PHASE II RELIABILITY PROGRAM PLAN

1.0 INTRODUCTION

1.1 Scope

This document is an integral part of the Kilowatt Isotope Power System (KIPS) Program Plan. This document defines the KIPS Reliability Program Plan for Phase II and is referenced in the KIPS Phase II Program Plan as Task 5.0. This document delineates the reliability assurance tasks that are to be accomplished by Sundstrand and its suppliers during the design, fabrication and testing of the KIPS flight system.

2.0 GENERAL PROGRAM REQUIREMENTS

2.1 Purpose

The reliability program is established and will be implemented to assure that reliability is considered in the design, fabrication, and testing of the KIPS. The reliability program plan is based on DOE Specification NRA-2 "Reliability Engineering Program Requirements" dated June 17, 1974.

2.2 Plan Preparation

The plan defined herein is the KIPS reliability program plan. The plan format follows the format of DOE Specification NRA-2. The reliability program defined herein complements and supports functions required by the KIPS program plan.

2.2.1 Revisions

This document shall be updated as necessary if the work effort or contract is modified and any revisions and deviations shall be submitted to DOE for approval.

2.2.2 Implementation

The reliability program plan presented herein defines the total reliability effort for Phase II of the KIPS program without further reference to DOE Specification NRA-2. The approved program plan shall be the standard used by DOE to evaluate Sundstrand's reliability performance.

3.0 ORGANIZATION AND DOCUMENTATION

3.1 Organization and Management

3.1.1 Reliability Organization

The Reliability Manager reports functionally to the KIPS Program Manager.

The formal reliability organization consists of technical experts, engineers, and statisticians reporting to the Test and Reliability Engineering Department Manager, responsible directly to the Vice President of Engineering. The reliability organization acts as director of reliability efforts, interprets specifications, gathers and analyzes results, critiques and publishes performance data, coordinates supplier reliability efforts where necessary, and participates in design analysis and testing.

The KIPS program organization is shown in Figure 1.

3.1.2 Reliability Manager

The Reliability Manager is responsible for the planning implementation and management of the reliability program. The Reliability Manager has the necessary authority and resources to discharge reliability program responsibilities. Direct liaison between DOE personnel and the Reliability Manager is authorized.

3.1.3 Interface with Other Organizations

Direct liaison between the Reliability Manager and technical and support groups is to be accomplished through participation in component analysis design and test; system design tradeoffs and reviews; system testing and data reduction, etc.

3.1.4 Personnel and Training

Trained and competent reliability engineering personnel are assigned to implement the reliability program. Indoctrination of the program managers and personnel from technical and support groups with reliability disciplines, techniques and procedures will be conducted. If unique circumstances dictate, a special training program for reliability, technical and support personnel will be initiated.

3.2 Program Documentation

Formal written reports covering the program and results obtained during the performance of the reliability tasks will be prepared and submitted.

3.2.1 Reliability Milestones

The reliability program is planned and implemented to meet the KIPS program milestones scheduled in Task 1.0 of the KIPS program plan. The reliability task/milestone schedule is presented in Figure 2.

3.2.2 Program Reviews

The progress and significant accomplishments of the reliability program will be documented and reported at the formal design reviews scheduled in Task 1.0. Reliability reviews, informal design reviews and working meetings will be held as needed in conjunction with and preparation for the regularly scheduled Design Reviews.

3.2.3 Facilities Review

Quality Assurance may conduct surveys of suppliers' facilities as provided in the Quality Program Plan.

3.2.4 Progress Reports

Progress and accomplishments of the reliability program will be included in the monthly Program Technical Report of Task 10.0. Formal reliability reports will be distributed with the monthly Technical Report. The overall results of the reliability program will be summarized and presented in the Annual Technical Report.

3.2.4.1 Progress Report Content

Progress reports will in general include the following:

- a. Progress of each reliability task including significant accomplishments and milestones during the reporting period.

3.2.4.1 Progress Report Content (Continued)

- b. Reliability problem areas and proposed corrective action.
- c. Failures that occurred during the reporting period and the corrective action taken.
- d. Further action of unresolved failures.
- e. Decisions and actions during the reporting period having impact on the reliability effort and descriptions of their anticipated effect on reliability.
- f. Anticipated reliability program changes, their effects, and corrective action taken.
- g. A description of formal or informal reliability recommendations, an evaluation of the effect of the change on the system, and the action taken.

3.2.4.2 Reports of Meetings

Sundstrand will submit the minutes of each Sundstrand/DOE reliability meeting within ten days.

4.0 DESIGN RELIABILITY ELEMENTS

4.1 Design Specification

Design specifications will be prepared by Design Engineering to describe the requirements of special purpose, non-standard and off-the-shelf components. These design specifications will include, as appropriate, functional, environmental, physical, reliability, and performance requirements against which purchase can be made and operational characteristics assessed. Reliability will review all design specifications to insure compatibility with reliability requirements.

4.2 Reliability Design

The use of stress derating, tolerance studies, redundancy, stress strength analysis, materials analysis, variables analysis, design trade-off studies and similar reliability oriented design techniques will be practiced in designing equipment to reduce the likelihood of critical failure modes and early wearout.

4.2.1 Expected Environments

An expected environments study will be conducted based on inputs from DOE and Sundstrand generated data. The expected environments study will develop a Manufacturer to Use Sequence (MUS) and table of environments. The MUS is a flow diagram which describes the various possible logistic sequences involved in moving a device from the time it is accepted to its end use environment. The environments table will describe the magnitudes of all expected environmental inputs to the system during MUS.

4.3 System Variables Analyses

During Phase I of the KIPS Program, a system optimization program was used to examine the effect of component design variables on the performance of other system components and on the thermal performance of the entire system. The optimization program consists of a computerized mathematical model of the system incorporating both cycle analysis and component design. The system performance analysis will be updated during the KIPS flight system design phase to ascertain the effect of design and parameter changes on system requirements. Results of the system performance analysis will be considered and included in the FMECA of Paragraph 5.4 herein.

5.0 RELIABILITY ENGINEERING PROGRAM ELEMENTS

5.1 Reliability Goal

The reliability objective for the flight system is established by DOE as .93 for 7 years.

5.2 Demonstrated Reliability

A minimum acceptable level of reliability will be established by DOE.

5.3 Reliability Participation and Analysis

Reliability organization participation began with the Phase I request-for-proposal and will continue throughout the KIPS program.

5.4 Failure Modes, Effects and Criticality Analyses (FMECA)

The FMECA provides a systematic, detailed, and continuous review of all system components and functions at the earliest possible phase of design. The FMECA will be performed to identify potential failure modes and ascertain the effects of such failure modes upon mission requirements. An FMECA was prepared for subassemblies and major components during Phase I. During Phase II, the FMECA will be continued incorporating changes in the KIPS baseline design.

5.4.1 Failure Modes and Ranking

All credible failure modes will be identified to include relationships with single or multiple components. Worst case environments will be assumed. Failure modes will be ranked on a relative scale of likelihood from 1 to 100 with 100 the most likely.

5.4.2 Failure Effects and Ranking

A systematic and detailed review shall be made of all possible effects resulting from the identified failure modes. Failure effects will be ranked from 1 to 100 with 100 being the worst case. Failure effect categories and rankings are as follows:

FAILURE EFFECTS CATEGORIES AND RANKING

<u>Category</u>	<u>Failure</u>	<u>Rank</u>
I	Results in catastrophic or imminent loss of power and mission.	100
II	Results in a reduction in power causing a partial mission failure.	50
III	Results in failure or out of specification condition not affecting power. Presuming KIPS is ground started and operates during launch, start failures are included in this category.	5

5.4.3 Criticality

The rankings of 5.4.1 and 5.4.2 will be multiplied to obtain a criticality ranking.

5.4.4 Failure Mode Elimination

Failure modes having high criticality ranking will be given special emphasis for elimination. Those that cannot be eliminated will be highlighted and analysis will be performed to provide justification for their retention in the design. No special tests are planned to verify an acceptably low probability of occurrence for failure modes having high ranking. A listing of particularly critical parts and processes, with critical characteristics described, will be prepared based on the results of the FMECA and the table of design criteria created in Paragraph 5.5.2.2. This list will be provided to project engineering and quality assurance in refining the design to achieve the highest practical reliability.

5.4.5 FMECA Reporting

A FMECA report will be prepared which includes hardware description and function, design specification, expected environments, assumptions, and support documentation. Detailed FMECA worksheets will be provided and include the information required from Sections 5.4.1, 5.4.2, and 5.4.3 and 5.4.4. The format for the FMECA tabulation will be similar to the format of Figure 3. Summary sheets will be used to highlight failure modes having a high relative criticality ranking.

5.5 System Logic Synthesis

A System Logic Synthesis will be prepared to indicate the logical combination of failure modes leading to a critical system failure, provide a basis for allocating the failure probabilities of the system to the failure modes, and to assess system reliability from the assessed failure mode probabilities. The system logic synthesis is defined in the following subparagraphs.

5.5.1 Logic Diagrams

System logic block diagrams will be developed to accurately depict the logical association between various modes of failure that individually or in combination can cause a critical system failure. The system logic block diagram will generally follow the functional logic of the system and will be capable of describing synergistic and dependent modes of failure as well as multiple modes of failure from the same component or components. Logical symbols such as AND, OR, NOR gates, etc., will be used as required.

5.5.2 Probability Equations

System failure (or success) equations will be developed to describe the association between the failure modes and their impact on the system.

5.5.2.1 Allocations

The logic diagram and probability equation shall be used as a guide to perform an allocation study to allocate failure probabilities to components based on the requirements of Paragraph 5.1.

5.5.2.2 Assessment

The logic diagram and probability equation shall be used to assess system reliability. The results of the assessment will be compared with the reliability goals. In general, failure rate sources for the reliability prediction will be as follows:

5.5.2.2 Assessment (Continued)

- Sundstrand failure rate data
- AVCO Corp. Reliability Engineering Data Series
- MIL-HDBK-217B, Reliability Prediction for
Electronic Equipment
- Supplier Failure rate data
- Current literature
- Engineering judgement

In addition, to support the assessment, a table of design criteria (e.g., environment, stress levels, safety factors) will be prepared for critical components.

5.5.2.3 Sensitivity Analysis

The reliability equation will be used where necessary to determine the sensitivity of the system assessment to possible ranges of failure mode assessments.

6.0 TEST PROGRAM

6.1 Purpose

The purpose of the test program is to evaluate and verify the KIPS flight system design.

6.2 Requirements

The test program will be conducted according to the approved KIPS test plans prepared in Tasks 8.0 and 9.0. Data from the tests will be used, to substantiate the FMECA and give additional confidence to the reliability assessment.

6.3 Data Sources

Test data, along with any other DOE contract data, will be used, to the extent possible, to substantiate failure modes and to assess their criticality.

6.4 Failures and Corrective Action

6.4.1 Failure Definition

An item which does not meet the performance requirements of its specification is defined as failed.

6.4.2 Failure Reporting

Failures which occur during the reliability and qualification tests of the KIPS test plan will be recorded and analyzed. Failure analysis and corrective action will be recorded on the Sundstrand Malfunction and Trouble Report form.

6.4.2.1 Description and Analysis

Each reliability and qualification test failure will include a description of the failure, test conditions, cause of failure, and corrective actions.

6.4.3 Failure Review Board

Failures and/or malfunctions occurring during qualification testing will require review by the failure review board. Membership of the failure review board shall consist of the following personnel or their designees:

6.4.3 Failure Review Board (Continued)

- a) KIPS Program Office
- b) KIPS Project Engineering
- c) KIPS QA Engineer
- d) KIPS Reliability Engineer
- e) KIPS Design Engineer
- f) DOE Representative-observer capacity only

When a failure or malfunction is experienced, the responsible personnel shall take the following actions:

- 1) Test Personnel shall take whatever actions are necessary for the protection of test personnel and test hardware.
- 2) Test Engineering shall place a hold on the test.
- 3) KIPS Project Engineer/Q.A. Engineer shall convene the FRB.
- 4) FRB determines the root cause of the failure or malfunction. If not possible within a reasonable length of time, the FRB shall collect all available evidence for determining the root cause of failure or malfunction at a later time.

6.4.3 Failure Review Board (Continued)

- 5) Failure Review Board determines disposition.
- 6) Failure Review Board determines corrective action or defer a decision until a later time if not practical prior to resuming test.
- 7) Failure Review Board shall obtain safety concurrence.
- 8) Failure Review Board only may release the hold on the test.

7.0 MAINTAINABILITY

7.1 Maintenance Free Design

The system will be designed to be maintenance free or as near maintenance free as is practicable.

7.2 Tolerance Control

As a design goal, tolerances will be controlled to allow interchangeability of replaceable components.

7.3 Maintenance and Operation Analysis

Maintenance and operation will be considered during the design stage. Areas requiring maintenance or related efforts will be analyzed to ensure that capabilities and procedures exist to adequately perform the functions.

8.0 HUMAN FACTORS ANALYSIS

8.1 Human Problems and Failures

Human problems and failures will be considered during the design stage.

8.2 Reports

Human factors considerations will be included, where appropriate, in other reliability program reports.

Figure 1 KIPS Program Organization

Revised

Form 6418

FIGURE 2 - TASK AND MILESTONE SCHEDULE

• SUNDSTRAND MACHINE TOOL

(815) 226-6000 • TWX 910-631 4255 • TELEX 267-440

FAILURE MODE AND EFFECTS ANALYSIS

③ CRITICALITY RANK, $1 \times 2 = 3$
② FE RANK
① FM LIKELIHOOD

DESIGN/SAFETY CONSIDERATIONS

① ② ③

FIGURE 3 - FMECA FORM.

8.2 DIFFERENCES BETWEEN PHASE I AND PHASE II RELIABILITY PLANS

The preliminary Phase II reliability program plan presented in subsection 8.1 is substantially unchanged from the Phase I plan. Significant changes in the plan are as follows: (Note the Phase I plan paragraph numbers.)

- 4.2.1 EXPECTED ENVIRONMENTS - Revised to include requirement for preparation of a Manufacturer to Use Sequence (MUS).
- 4.3 SYSTEM VARIABLES ANALYSES - Requires update of Phase I analyses.
- 5.1 RELIABILITY GOAL - Revised to current goal, 0.93 for 7 years.
- 5.2 DEMONSTRATED RELIABILITY - Minimum acceptable level to be established by DOE.
- 5.4 FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA) - Requires continuation of Phase I analysis.
 - 5.4.2 FAILURE EFFECTS AND RANKING - Revises failure effects ranking table for flight system.
- 6.4.2 FAILURE REPORTING - Adds requirement that reliability and qualification test failures be recorded on the Sundstrand Malfunction and Trouble Report form.
- 6.4.3 FAILURE REVIEW BOARD - Adds requirement for failure review board.

8.3 RELIABILITY ESTIMATION

This section presents the results of the reliability prediction estimation. The seven year reliability goal for KIPS is 0.93. The estimated seven year reliability is 0.938.

Table 8-A presents a summary of the allocated and estimated reliabilities for the KIPS components. Table 8-B contains the supporting rationale for the reliability estimate.

Table 8-A KIPS Flight System Reliability Allocation/Estimate

<u>COMPONENT</u>	<u>Reliability (7 years)</u>	
	<u>ALLOCATED</u>	<u>ESTIMATED</u>
System Accumulator & Filter Assembly	0.999	0.9993
Flow Control Valve	0.999	0.9937
Regenerator	0.994	0.9986
Combined Rotating Unit (CRU)	0.986	0.986
Jet Condenser	0.994	0.9944
Radiator Bypass Valve & Filter Assembly	0.999	0.9993
Radiator	0.986	0.986
Heat Source Assembly (HSA)	0.994	0.9985
Electronic Controls	0.986	0.982
Loop Containment Integrity	0.992	0.9983
SYSTEM	0.93	0.938

COMPONENT	FAILURES PER 10^9 HOURS		REMARKS
	ALLOCATED	ESTIMATED	
System Accumulator and Filter Assembly	16.3	11.6	<p>One flight system lifetime is estimated to consist of 20 start cycles and 2555 thermal excursion partial cycles (1 cycle per day for 7 years). The Metal Bellows Company design for each accumulator bellows is for: 10^6 full cycles, 10^7 partial cycles. Metal Bellows Company has extensive background in designing and manufacturing bellows accumulators and reservoirs for aerospace applications.</p> <p>Dual <u>redundant bellows</u> are used in the accumulator, such that failure of either will not affect system performance. Metal Bellows Company reliability calculation, based on their historical data, shows a failure probability for the redundant bellows assembly to be less than 1×10^{-9}.</p> <p>A more conservative failure rate estimate was also obtained using failure rate handbook data. The estimated failure rate for the accumulator was calculated by modeling the bellows in parallel and using a bellows failure rate of 0.1×10^{-6} (Avco Reliability Engineering Data Series - Failure Rates). The accumulator reliability (7 years) was found to be .99996 ($\lambda = .64 \times 10^{-9}$). The estimated <u>filter</u> failure rate is 11×10^{-9} (Avco Reliability Engineering Series - Failure Rates). The 7 year reliability for the filter is .9993. The total estimated failure rate for the accumulator and filter assembly is 11.6×10^{-9}. (NOTE: External leakage rates are included in the loop containment integrity category of this analysis.)</p>

COMPONENT	FAILURES PER 10^9 HOURS		REMARKS
	ALLOCATED	ESTIMATED	
Flow Control Valve	16.3	103	<p>Moving parts in the flow valve are: 2 redundant thermal sensors 2 redundant bellows seals 2 nozzle flappers</p> <p>Each <u>thermal sensor</u> provides dual bellows containment so that, in the event of the primary bellows failure, Nak is not released into the system.</p> <p>KIPS power capability is not degraded due to leakage failure of one thermal sensor. However, one thermal sensor failure in the extended mode due to a plugged capillary tube will result in eventual system loss. The reliability of the redundant thermal sensor pair is calculated using the following series-parallel model:</p> <pre> graph LR S1R["Sensor No. 1 fails in retract mode λ = 0.05 x 10⁻⁶"] S2R["Sensor No. 2 fails in retract mode λ = 0.05 x 10⁻⁶"] S1E["Sensor No. 1 fails in extend mode λ = 0.05 x 10⁻⁶"] S2E["Sensor No. 2 fails in extend mode λ = 0.05 x 10⁻⁶"] S1R --- P1(()) S2R --- P1 P1 --- S1E S1E --- S2E </pre> <p>The estimated failure rate for each thermal sensor is 0.1×10^{-6} (Avco Reliability Engineering Data Series-Failure Rates). For this analysis, the failure rate is split equally between the failed extended and failed retracted modes. On this basis, the reliability of the pair of thermal sensors is calculated to be .99388 for 7 years. This is equivalent to a failure rate of 100.1×10^{-7}.</p>

Table 8-B KIPS Flight System Operating Reliability Estimation (cont'd)

3 of 4

COMPONENT	FAILURES PER 10 ⁹ HOURS		REMARKS
	ALLOCATED	ESTIMATED	
Flow Control Valve (Continued)			<p>Reliability testing to identify the predominant thermal sensor failure mode is proposed for Phase II. If the capillary plugging mode is predominant, the redundancy reduces rather increases reliability. Available data indicates that, at the KIPS operating temperature, plugging shall not be a problem when high purity Nak is used.</p> <p>The estimated failure rate for dual redundant bellows seals was calculated by modeling the bellows in parallel. The estimated failure rate for each bellows is 0.1×10^{-6} (Avco Reliability Engineering Data Series Failure Rates). The estimated failure rate for the redundant bellows configuration was calculated to be 0.64×10^{-9}.</p> <p>The <u>nozzle flappers</u> are designed for a failure probability of 1×10^{-9}.</p> $\lambda_{\text{Total}} = (100.1 + 0.64 + 1 + 1) \times 10^{-9}$ $\lambda_{\text{Total}} = 102.7 \times 10^{-9}$ <p>As part of the valve module is the <u>Non-Condensable Gas Seperator(NCGS)</u>. The NCGS is a static device, essentially a variable conductance heat pipe. The predominant NCGS failure mode is expected to be external leakage which failure rate is covered in the loop containment integrity category.</p>

Table 8-B KIPS Flight System Operating Reliability Estimation (cont'd)

of

COMPONENT	FAILURES PER 10^9 HOURS		REMARKS
	ALLOCATED	ESTIMATED	
Check Valves (2)	---	---	<p>There are 2 check valves in the flight design. One is located at the accumulator outlet; one is located at the system pump outlet. The check valves are required to function only during system start-up.</p> <p>Check valve failure rate is derived from Sundstrand constant speed drive valve historical failure rate data. The valve failure rate has been factored for the space environment. The estimated failure rate for each check valve is 3×10^{-9}. Presuming ground startup for KIPS, the check valve failure rate is not included in the operating reliability calculation.</p>
Regenerator	98.1	23	<p>The KIPS <u>regenerator</u> consists of seamless finned tubing welded end to end to form a vapor-liquid heat exchanger. The tubing is sized for a failure probability of 1×10^{-9}.</p> <p>RADC Data Collection for Nonelectronic Reliability contains failure rates for heat exchangers, in the ground-air environment of 154×10^{-9} (15 million part hours) and 230×10^{-9} (10 million part hours) for a combined failure rate of 184×10^{-9} (25 million part hours). Improvement should be expected in this failure rate in a space environment. Avco Reliability Data Series-Failure Rates shows an 8:1 failure rate improvement from ground environment to space environment. Considering an 8:1 improvement, the estimated regenerator failure rate becomes 23×10^{-9} failure per hour. The 7 year reliability is then .9986.</p>

Table 8-B KIPS Flight System Operating Reliability Estimation (cont'd)

COMPONENT	FAILURES PER 10^9 HOURS		REMARKS
	ALLOCATED	ESTIMATED	
Combined Rotating Unit (CRU)	229	229	<p>The CRU consists of the turbine, alternator and system pump. The CRU rotor is supported by tilting pad thrust and radial bearings.</p> <p>The <u>turbine wheel</u>, <u>alternator rotor</u>, and <u>system pump</u> are each designed for a failure probability of 1×10^{-9}.</p> <p>The estimated failure rate for the <u>alternator windings</u> was calculated using MIL-HDBK-217B failure rate data and the MIL-HDBK-217A estimation procedure for rotary electrical devices. The alternator insulation system is rated at 230°C for the field windings. Using MIL-HDBK-217B, Section 2.7 (Inductive Devices, MIL-T-27), the alternator windings failure rates were calculated for the space flight environment.</p> <div style="margin-left: 40px;"> Stator windings - 0.014×10^{-6} Field windings - 0.012×10^{-6} TOTAL - 0.026×10^{-6} </div> <p>Sundstrand has considerable experience with <u>tilting pad bearings</u>, having built a 6KW ORC using Dowtherm A and a 1.0 KW system using toluene as the working fluid. The 6 KW machine ran 3000 hours with no detectable tilting pad bearing damage. The 1.0 KW system accumulated 16,500 hours with no primary failures (one bearing set has accumulated 8800 hours). Sundstrand Sundyne compressor gearboxes have accumulated more than 7.5 million hours using tilting pad bearings.</p> <p>It is expected that KIPS tilting pad bearing failure rate will allow the apportioned reliability goal for the CRU to be achieved.</p>

Table 8-B KIPS Flight System Operating Reliability Estimation (cont'd)

of

COMPONENT	FAILURES PER 10^9 HOURS		REMARKS
	ALLOCATED	ESTIMATED	
Jet Condenser	98.1	92	<p>From a component failure rate standpoint, the principal parts of the jet condenser are the <u>liquid injector</u>, 90 <u>nozzles</u> on the liquid injector, and the <u>vapor funnel</u>.</p> <p>The estimated failure rate for the 90 <u>nozzles</u> is $.090 \times 10^{-6}$. (The Avco Reliability Engineering Data Series-Failure Rates lists orifice failure rate as 0.01×10^{-6}. Since KIPS is a closed loop system with adequate filtration provided to prevent orifice plugging, an order of magnitude improvement is estimated.</p> <p>The <u>liquid injector</u> and vapor funnel are each designed for a failure probability of 1×10^{-9}.</p> $\lambda_{\text{Total}} = (90.0 + 1 + 1)$ $\lambda_{\text{Total}} = 92$
Radiator Bypass Valve and Filter Assembly	16.3	11	<p>Two welded stainless steel <u>bellows</u> are the only dynamic parts of the radiator bypass valve. Failure of either bellows (leakage) will cause the valve to fail in the no bypass position and result in system <u>degraded</u> operation. Using a bellows failure rate of 0.1×10^{-6} (Avco Reliability Engineering Data Series Failure Rate), the failure rate for the valve (2 bellows) becomes 0.2×10^{-6}. Since the valve failure will result in only slightly degraded system operation (loss of 35 - 40 watts in the worst case), the valve failure rate is not included in the system failure rate.</p> <p>The estimated <u>filter</u> failure rate is 11×10^{-9} (Avco Reliability Engineering Data Series-Failure Rate). The seven year reliability is .9993.</p>

Table 8-B KIPS Flight System Operating Reliability Estimation (cont'd)

of

COMPONENT	FAILURES PER 10^9 HOURS		REMARKS
	ALLOCATED	ESTIMATED	
Radiator	229	229	<p>The KIPS space radiator is an aluminum welded assembly in the shape of a right circular cylinder. It attaches directly to the Power Conversion System (PCS). The fluid passes through vertical tube extrusions which are connected, at each end, to a common header. Each extrusion serves three purposes, as a passageway for the organic fluid, as the frontside and backside meteoroid armor protection and as vertical stiffening for the radiator shell.</p> <p>The fluid passages are protected against meteoroid penetration. Sizing of components for meteoroid puncture probability will be such that, when combined with the PCS puncture probability the reliability will be .99 for 5 years (which is equivalent to a failure rate of 229×10^{-9}).</p>
Heat Source Assembly (HSA)	98.1	25	<p>The HSA consists of: Isotope heat source (IHS); Emergency Heat dump System (EHDS); Boiler tube loop (≈ 8 feet/HSA); Cooling tube loop (≈ 10 feet/HSA).</p> <p>The <u>boiler and cooler tubes</u> are single seamless finned tube heat exchangers. The tubing is sized for a failure probability of less than 1×10^{-9}. The length of boiler and cooler tubing is less than the length of the regenerator tubing (≈ 18 feet per HSA v.s. ≈ 180 feet) and is expected to have a lower failure rate. The boiler and cooler tubing failure rate for 3 HSA's is expected to be less than one-half the regenerator failure rate. The boiler and cooler tubing failure rate is estimated to be less than 12×10^{-9}.</p>

COMPONENT	FAILURES PER 10^9 HOURS		REMARKS
	ALLOCATED	ESTIMATED	
Heat Source Assembly (HSA) (Continued)			<p>The EHDS provides a protective function. From a reliability standpoint, failure of the EHDS is the premature meltdown of the EHDS (below the predetermined temperature level) resulting in degradation or loss of KIPS output capability. The probability of premature EHDS meltdown is expected to be very low.</p> <p>The reliability of the basic isotope heat source is considered unity for this analysis.</p> <p>On this basis, the HSA failure rate is estimated to be 25×10^{-9}. The estimated seven year reliability is .998.</p>
Electronic Controls	229	301	<p>The controls for KIPS consist of: KIPS alternator controller; Parasitic load bank radiator.</p> <p>The KIPS electronic controls were designed with a reliability goal of .986 for 7 years (.99 for 5 years). This controls reliability goal is felt to be consistent the overall 7 year reliability goal of .93 for KIPS. The highest reliability parts available have been selected. Redundancy has been incorporated in the controls to reduce the number of single point failures and approach the allocated controls reliability.</p> <p>Three parasitic load resistor (PLR) elements are used, each driven by a separate power switch. Any two of the three are capable of handling full system load (if a power switch or PLR fails open there is no effect on KIPS output).</p>

Table 8-B KIPS Flight System Operating Reliability Estimation (cont'd)

COMPONENT	FAILURES PER 10 ⁹ HOURS		REMARKS
	ALLOCATED	ESTIMATED	
Electronic Controls (Continued)			<p>The controls failure rate has been calculated using MIL-HDBK-217B. The model for the controls failure rate calculation allowed one of three load switch/PLR paths to fail. An estimated failure rate of 1×10^{-6} was used for each PLR element for this analysis.</p> <p>The calculated 7 year controls reliability is .9817. This is equivalent to a failure rate of 3.01×10^{-9}. The following is a reliability block diagram which summarizes the reliability calculations for the controller.</p> <div style="text-align: center;"> <pre> graph LR R1[Rectifier R1] --> R2[95% CKT R2] R2 --> R3[100% CKT R3] R3 --> R4[PWM CKT R4] R4 --> R5[Voltage Regulator R5] R5 --> P1(()) P1 --> R6a[PLR Driver and PLR R6] P1 --> R6b[PLR Driver and PLR R6] R6a --> End(()) R6b --> End </pre> <p> $\lambda_1 = .0491967$ $\lambda_2 = .0109658$ $\lambda_3 = .0152158$ $\lambda_4 = .0403732$ $\lambda_5 = .016037$ $\lambda_6 = 1.0048562$ </p> <p> $\sum_{i=1}^5 \lambda_i = .1317885$ $R_{1-5} = .9919513$ $R_{\text{controller}} = R_{1-5} \times R_6$ $R_{\text{controller}} = .98174789$ </p> <p> $R = e^{-\lambda T}$ $= .9402422$ 2 of 3 required $R_6 = .9897138$ </p> </div>

Table 8-B KIPS Flight System Operating Reliability Estimation (cont'd)

of

COMPONENT	FAILURES PER 10 ⁹ HOURS		REMARKS																		
	ALLOCATED	ESTIMATED																			
Loop Containment Integrity (External Joints)	131	27	<p>KIPS contains 185 external joints. External leakage will result in eventual system loss. There are no seals which failure would result in external leakage of working fluid. 100% NDT inspection of joints will verify joint integrity. The KIPS components and assembled system will be leak checked.</p> <p>The total loop (joint) failure rate for the flight system has been calculated using the approach described in General Electric Space Division Report (to JPL) "Mini-Brayton Outer Planets Class of Mission Study Loss of Coolant Assessment". The GE report provides failure rates of welded joints based on weld type, temperature and weld length. The failure rates were obtained from "Reactor Power System Design Document, Vol. II", Contract NASA 25140, page 106, and are as follows:</p> <table><thead><tr><th><u>Weld Type</u></th><th><u>Temperature</u></th><th><u>Failures λ-Weld-Hr</u></th></tr></thead><tbody><tr><td rowspan="2">Butt</td><td>>600°F</td><td>1 x 10⁻⁹</td></tr><tr><td><600°F</td><td>1 x 10⁻¹⁰</td></tr><tr><td rowspan="2">Seam</td><td>>600°F</td><td>2 x 10⁻⁹</td></tr><tr><td><600°F</td><td>2 x 10⁻¹⁰</td></tr><tr><td rowspan="2">Double Containment</td><td>>600°F</td><td>2 x 10⁻¹¹</td></tr><tr><td><600°F</td><td>2 x 10⁻¹²</td></tr></tbody></table> <p>The above failure rates are based on aerospace weld experience and quality control procedures.</p>	<u>Weld Type</u>	<u>Temperature</u>	<u>Failures λ-Weld-Hr</u>	Butt	>600°F	1 x 10 ⁻⁹	<600°F	1 x 10 ⁻¹⁰	Seam	>600°F	2 x 10 ⁻⁹	<600°F	2 x 10 ⁻¹⁰	Double Containment	>600°F	2 x 10 ⁻¹¹	<600°F	2 x 10 ⁻¹²
<u>Weld Type</u>	<u>Temperature</u>	<u>Failures λ-Weld-Hr</u>																			
Butt	>600°F	1 x 10 ⁻⁹																			
	<600°F	1 x 10 ⁻¹⁰																			
Seam	>600°F	2 x 10 ⁻⁹																			
	<600°F	2 x 10 ⁻¹⁰																			
Double Containment	>600°F	2 x 10 ⁻¹¹																			
	<600°F	2 x 10 ⁻¹²																			

Table 8-B KIPS Flight System Operating Reliability Estimation (cont'd)

1 of 1

COMPONENT	FAILURES PER 10 ⁹ HOURS		REMARKS																														
	ALLOCATED	ESTIMATED																															
Loop Containment Integrity (Continued)			<p>For the KIPS joints failure rate calculation, socket brazed joints were estimated to have the same failure rates as welded seam joints. For the radiator, the butt weld joint rate was used for the fillet weld joints and socket weld joints.</p> <p>The KIPS joints and estimated failure rates are summarized as follows:</p> <table><thead><tr><th></th><th><u>Temp °F</u></th><th><u>n</u></th><th><u>λ each</u></th><th><u>λ Total (x 10⁻⁹)</u></th></tr></thead><tbody><tr><td>PCS Butt Welded Joints</td><td>< 600</td><td>90</td><td>1 x 10⁻¹⁰</td><td>9.0</td></tr><tr><td>PCS Butt Welded Joints</td><td>> 600</td><td>9</td><td>1 x 10⁻⁹</td><td>9.0</td></tr><tr><td>PCS Socket Brazed Joints</td><td>< 600</td><td>4</td><td>2 x 10⁻¹⁰</td><td>0.8</td></tr><tr><td>Radiator Welded Joints</td><td>> 600</td><td>82</td><td>1 x 10⁻¹⁰</td><td><u>8.2</u></td></tr><tr><td colspan="4">TOTAL</td><td>27.0</td></tr></tbody></table> <p>The seven year reliability is .9983.</p>		<u>Temp °F</u>	<u>n</u>	<u>λ each</u>	<u>λ Total (x 10⁻⁹)</u>	PCS Butt Welded Joints	< 600	90	1 x 10 ⁻¹⁰	9.0	PCS Butt Welded Joints	> 600	9	1 x 10 ⁻⁹	9.0	PCS Socket Brazed Joints	< 600	4	2 x 10 ⁻¹⁰	0.8	Radiator Welded Joints	> 600	82	1 x 10 ⁻¹⁰	<u>8.2</u>	TOTAL				27.0
	<u>Temp °F</u>	<u>n</u>	<u>λ each</u>	<u>λ Total (x 10⁻⁹)</u>																													
PCS Butt Welded Joints	< 600	90	1 x 10 ⁻¹⁰	9.0																													
PCS Butt Welded Joints	> 600	9	1 x 10 ⁻⁹	9.0																													
PCS Socket Brazed Joints	< 600	4	2 x 10 ⁻¹⁰	0.8																													
Radiator Welded Joints	> 600	82	1 x 10 ⁻¹⁰	<u>8.2</u>																													
TOTAL				27.0																													

8.4 FAILURE MODES, EFFECTS AND CRITICALITY ANALYSIS (FMECA)

The results of the failure modes, effects and criticality analysis (FMECA) for the KIPS flight system is presented on the tabular FMECA work sheets contained in this subsection of the report. The FMECA is a systematic examination of all components of the system to identify their function and how they can fail and to determine the effects of each component failure on the system.

Credible failure modes are listed on the FMECA work sheets together with the possible failure effects resulting from the identified failure modes. Failure modes are ranked on a relative scale of likelihood from 1 to 100 according to the guidelines of Table 8-C. These ranks have been assigned according to engineering judgment and experience. This approach tends to eliminate confusion with failure rates, per se, whose credibility may be somewhat debatable. Failure effects are also ranked on a scale from 1 to 100 as defined in Table 8-D. Note that failure modes which result in failure of the system to start are assigned a failure effect ranking of 5. The rationale for the low start failure effect ranking is that, for the baseline KIPS approach, the system will be started on the ground and left operating for launch; a start failure can then be corrected before launch.

Since there is only limited use of redundancy in the system, most of the component failures have the same ultimate effect on the system, loss of electrical power output.

System failures which result in loss of working fluid flow would allow the heat source to overheat if backup provisions were not incorporated. In space, the HSA emergency heat dump system (EHDS) will melt so that the heat source temperature will remain at a safe level. On the ground and in the space shuttle bay, the heater temperature control support equipment will provide emergency cooling flow to control the HSA temperature in event of loss of system flow.

8.4.1 CATASTROPHIC FAILURE MODES

Failure modes/effects are ranked in the FMECA according to the severity of the failure effect. Catastrophic (single point) failure modes are classified as Category I and are given a failure effect (FE) rank of 100 on the FMECA form.

External leakage results in loss of working fluid (in vacuum environment) and HSA overtemperature shutdown (multifail melts), a catastrophic failure mode. External leakage can result from a defective welded joint, tubing rupture or housing (e.g., turbine housing) crack or micrometeorite puncture. The KIPS contains a number of external welds which must be kept leak tight. Welded joints are designed with large margins of safety. High quality welding techniques and 100 percent NDT and inspection will contribute to high reliability. Double containment joints will be used for any joints for which inspection may be difficult. The baseline system design generally uses single containment joints. However, schemes are available for incorporating double containment joints throughout the system. External leakage due to rupture/cracking of tubing, turbine housing, jet condenser funnel, accumulator housing, cooler, centrifugal separation, etc., is considered to be extremely unlikely because of the conservative approach used in the design analysis of these components. Reliability stress margins have been established which must be met or exceeded in the design of each component. These reliability stress margins consider the statistical variation of material strength to arrive at a minimum margin of safety which is acceptable from a reliability viewpoint for each material/design. For KIPS, reliability stress margins are used which yield a 1×10^{-9} failure probability.

External leakage of the radiator is largely a function of the probability of surviving the

Table 8-C Failure Mode Likelihood Rank

<u>RANK</u>	<u>RATIONALE FOR RANKING</u>	<u>GUIDELINE FOR RANKING</u>
100	Most likely failure mode	Failure mode occurrences should be expected during the KIPS flight program.
75	Very likely failure mode	
50	Likely failure mode	It is reasonable to expect that failure mode could occur during the KIPS flight program.
25	Minor failure mode	
10	Unlikely failure mode	It is reasonable to expect that failure mode would not occur during the KIPS flight program.
5	Highly unlikely failure mode	
1	Improbable failure mode	No possibility of failure mode occurrence.

Table 8-D Failure Effects Categories and Ranking

<u>CATEGORY</u>	<u>FAILURE</u>	<u>RANK</u>
I	Results in catastrophic or imminent loss of power performance and mission.	100
II	Results in a reduction in power resulting in a partial mission failure.	50
III	Results in failure or out of specification condition not affecting power during mission. Presuming KIPS is ground started and operates during launch, start failures are included in this category.	5

micrometeorite environment. The system is designed for a non-puncture probability of 0.99 for seven years. This is consistent with a reliability goal for KIPS of 0.93 for seven years.

Failure of the combined rotating unit (CRU) is a catastrophic failure. The turbine wheel, alternator rotor and pump are each designed for a failure probability of less than 1×10^{-9} using the approach described above. The rotor assembly (turbine wheel, alternator rotor and pump) will be proof-spun to verify its structural integrity. Tilting pad thrust and radial bearings support the CRU. Unlike ball bearings, which have some probability of failure for their lifetime, tilting pad bearings designed for full film lubrication and, hence, no metal-to-metal contact, have theoretically "infinite life". Sundstrand has considerable experience with tilting bearings, having built a 6 KW ORC using Dowtherm A and a 1.0 KW system using toluene as the working fluid. The 6 KW machine ran 3000 hours with no detectable tilting pad bearing damage. The 1.0 KW systems accumulated 16,500 hours with no primary tilting pad bearing failures, with one bearing set accumulating 8800 hours. Sundstrand Sundyne compressor gearboxes, which use tilting pad bearings, have accumulated more than 7.5 million hours of operating time. The KPS tilting pad bearing pads are silver plated to prevent/minimize damage should a high speed rub occur. The Sundyne gearbox, 6 KW ORC and 1.0 KW ORC tilting pad bearings are also silver plated.

Alternator stator power windings and field windings are single failure points. Considering that the shorted failure mode due to insulation breakdown is the most likely failure mode, redundancy did not offer substantial advantages. However, based on MIL-HDBK-217B prediction techniques, the alternator windings are very low failure rate items (windings failure rate calculated to be 0.026×10^{-6} failures per hour). The insulation system is rated at 230°C, while the maximum continuous windings temperature is 121°C for the stator windings and 114°C for the field windings.

Catastrophic system failure will result from flooding of the jet condenser. Jet condenser flooding can result from excessive concentration of non-condensable gases, injector/throat misalignment, or a plugged condenser throat. A non-condensable gas separator has been incorporated in the system to prevent non-condensable gas buildup. The non-condensable gas separator is a static device utilizing proven heat pipe technology.

Plugged jet condenser nozzles would result in a degradation of power output. As nozzles become plugged, jet condenser pressure recovery decreases with a resultant increase in turbine back pressure and decrease in system efficiency. Complete system loss results only if an excessive number of jets should become plugged. Filtration is provided at the radiator outlet, directly upstream of the jet condenser injector, to protect the condensing jets.

The flow control valve contains redundant NaK filled capillary thermal sensors. In the event of a bellows leakage failure; the system will continue operation under control of the other thermal sensor. However, if the capillary should become plugged in the extended position, then the redundancy reduces rather than increases reliability. The consideration then is whether leakage or capillary plugging is the predominant failure mode. Reliability testing to identify the predominant thermal sensor failure mode has been proposed for Phase II. Available data indicates that when high purity NaK is used at the KIPS operating temperature, plugging should not be a problem. General Electric Appliance Division, during their testing using commercial grade NaK, experienced capillary plugging only when temperature exceeded 1000°F. Other sources have reported similar or better results. The KIPS thermal sensors use high purity NaK; KIPS bulb temperature is 650°F. Procedures controlling thermal sensor cleaning and filling are being imposed. Samples of NaK used for filling will be subjected to chemical analysis as a check of purity level.

The electronic controls are designed to provide a 7 year reliability of 0.986. In the baseline design, redundancy has been incorporated where necessary in order to reduce the number of single point failures and attain the 0.986 reliability goal.

Single failure points exist in the baseline controller; however, these failure points are associated with extremely low failure rate electronic devices. These single failure point failure modes are voltage regulator open circuit, rectifier short, speed controller circuit short, and overload protection circuit failed short. The highest reliability parts available are used in the flight design so that the probability of single failure point failure mode occurrence will be very small.

8.4.2 SYSTEM DEGRADATION FAILURE MODES

Failure modes/effects are ranked in the FMECA according to the severity of the failure effect. Degradation failure modes are classified as Category II and are given a failure effect (FE) rank of 50 on the FMECA form.

The degraded boiler and regenerator heat exchange failure mode is a time related process which would result in a gradual reduction of system efficiency. Since degradation could possibly occur to the extent that a HSA overtemperature would result, the failure mode is shown as catastrophic (loss of power, therefore, FE rank = 100) on the FMECA sheet. However, as a practical matter, system degradation more aptly describes the failure mode, with overtemperature shutdown occurring well into the life of the system.

A reduction of system efficiency, and resultant reduction in power output capability, can be caused by a plugged turbine nozzle. The centrifugal separator, located directly upstream of the turbine, traps contaminant particles to minimize the possibility of nozzle plugging.

The radiator bypass valve is a "fail-operational" valve since system operation will continue with a small power loss in the event that the bypass valve does fail. The radiator bypass valve is designed to fail in the no bypass position in the event of bellows leakage. Failure in the no bypass position results in a maximum loss of 35-40 watts of power capability at the worst case. If the valve had been designed to fail in the non-zero bypass position, the maximum power loss would have been more than 56 watts at the end of mission and at 422°F sink temperature.

Failure of the electronic controls is considered unlikely due to the extremely low failure rate parts which have been selected for the KIPS flight controller. Failure of a tuning capacitor in the tuning capacitor load bank will result in a slight decrease in system (alternator) efficiency. A voltage regulator short circuit would allow maximum field current to the alternator such that, at design load, output voltage would be approximately 39 volts. A rectifier open failure would result in low quality power ripple in DC output.

FAILURE MODE AND EFFECTS ANALYSIS

1 of 13

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	DESIGN/SAFETY CONSIDERATIONS	<div> <div>③ CRITICALITY RANK, ①×②=③</div> <div>② FE RANK</div> <div>① FM LIKELIHOOD</div> </div>		
						①	②	③
1.	POWER CONVERSION SYSTEM (PCS)							
1.1	<u>Fluid Containment Components</u> Tubing, housing, manifolds provide for fluid passage and containment. Interconnecting Tubing Electronics Cooling Turbine Housing Regenerator Housing Transition Section Jet Condenser Housing Accumulator Housing Valve Pack/Filter Housing Non-Condensable Gas Separator Housing Centrifugal Separator Bearing Tee Radiator	External leakage	Tube rupture, housing cracked or welded joint failure caused by fatigue, thermal stress, material defect, defective weld, manufacturing defect, meteorite puncture.	<p>During operation in space, external leakage results in loss of working fluid and electrical power loss.</p> <p>While on ground, may result in external leakage of system fluid or air-in leakage (depending on system pressure). Air-in leakage results in jet condenser flooding and no start or electrical power loss.</p> <p>potential fire hazard on ground if ignition source is present.</p>	Seamless tubing Tubing, housings, manifolds sized for 1×10^{-9} failure probability.	10	100	1000
1.2	<u>Boiler</u> Finned tube heat exchanger vaporizes and superheats working fluid with heat received via radiation from heat source.	<p>Rupture in tube or weld failure.</p> <p>Contaminates working fluid.</p> <p>Degraded heat exchange capability.</p>	<p>Fatigue, overheating, thermal expansion, material defect, defective weld.</p> <p>Corrosion of tube inner surface, or tube insert due to material incompatibility, overtemperature.</p> <p>Deteriorated tube inner surface due to corrosion, tube inner surface coated with decomposition products. Excessive deterioration of tube or fin surface due to vaporization, thermal effects. Fin separates from tube due to thermal effects, vibration, manufacturing defect, radiation effects.</p>	<p>Leakage inside boiler box contacts heat source. Potential fire hazard during ground operation in air. Heater temp. control support equipment controls heat source temp. on ground and in shuttle bay.</p> <p>Contaminant particle may obstruct a turbine nozzle with resultant reduced turbine efficiency and reduced system electrical power output capability.</p> <p>Reduced system efficiency. Reduced electrical power output capability. HSA temperature tends to increase. Ultimately, possible HSA overtemp. shutdown (EHDS).</p>	<p>Dowtherm has narrow flammability limits. HSA inerted during ground operation.</p> <p>Centrifugal separator traps contaminant particles.</p> <p>Material selection through compatibility testing.</p> <p>Material selection through compatibility testing.</p>	5	100	500
						10	50	500
						10	100	1000

FAILURE MODE AND EFFECTS ANALYSIS

2 of 13

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	DESIGN/SAFETY CONSIDERATIONS	<div> <div>③ CRITICALITY RANK, ① × ② = ③</div> <div>② FE RANK</div> <div>① FM LIKELIHOOD</div> </div>		
						①	②	③
1.3	<u>Regenerator</u> Circular finned tube heat exchanger with turbine exhaust vapor on hot side and boiler feed fluid on cold side. Regenerator increases temperature of working fluid prior to entering boiler by transferring super heat from the turbine exhaust vapor.	Tube rupture, weld failure, fitting failure.	Material defect, fatigue from vibration, defective weld, fretting at tube support points.	Liquid leaks to vapor side. Flow limiter increases flow to boiler to maintain turbine inlet temperature. Small leakage results in reduced system efficiency and reduced electric power output capability. Gross leakage results in reduced flow to boiler, reduction or loss of system electrical power capability. HSA overtemp. shutdown (EHDS).	Seamless finned tubing. Tubing sized for 1×10^{-9} failure probability.	5	100	500
		Degraded heat exchange capability.	Buildup on fins due to working fluid deterioration. Fin separates from tube due to thermal effects, vibration, manufacturing defect.	Reduced system efficiency. Reduced electrical power output.	Centrifugal separator removes any fluid degradation products.	10	50	500
		Contaminates vapor.	Fin erosion	Contaminant particles may foul jet condenser. Jet condenser floods out. HSA overtemp. shutdown (EHDS).	Vapor velocity is relatively low through heat exchanger. Material selection through compatibility testing.	5	100	500
1.4	<u>Regenerator Electric Preheater</u> Heats regenerator prior to start-up.	Does not heat regenerator.	Open circuit to heater coil.	System may not start.		5	5	25
1.5	<u>Combined Rotating Unit (CRU)</u> CRU is turbine-alternator-pump. Single stage turbine spins alternator and pump. Double-ended homopolar inductor alternator provides electrical power output to rectifier. Centrifugal pump provides working fluid to fluid loops. CRU rotor is supported by fluid lubricated tilting pad bearing.	Turbine failure.	Turbine wheel rupture due to material defect, manufacturing defect.	Loss of electrical power output. HSA overtemp shutdown (EHDS). Turbine pieces propelled through CRU housing. Hazard for ground personnel, damage to shuttle and equipment.	Turbine wheel is designed for 1×10^{-9} failure probability.	5	100	500

FAILURE MODE AND EFFECTS ANALYSIS

3 of 13

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	DESIGN/SAFETY CONSIDERATIONS	③ CRITICALITY RANK, ①x②=③ ② FE RANK ① FM LIKELIHOOD		
						①	②	③
1.5	<u>Combined Rotating Unit (CRU)</u> (Continued)	Turbine failure. (Continued)	Turbine wheel rubs due to high temperature creep.	Turbine rubs down. Loss of system flow, loss of electrical power output. HSA overtemp. shutdown (EHDS).	Adequate tip clearance is provided. Operates well below material creep range.	5	100	500
			Turbine nozzle obstructed by contaminant particle.	Reduced turbine efficiency. Reduced electrical power output capability.	Six turbine nozzles. Centrifugal separator traps contaminant particles upstream of turbine nozzle.	10	50	500
		Alternator failure.	Open, shorted or grounded windings.	Reduction or loss of electrical power output. In event of loss of electrical output, system continues to run at no load speed (58,200 RPM)	Insulation system is rated at 230°C for 60,000 hours. Max. continuous windings temperatures are: field winding 237°F (114°C) stator winding 249°F (121°C)	10	100	1000
			Structural failure of rotor pole.	CRU failure. Loss of system flow, loss of electrical power output. HSA overtemp. shutdown (EHDS).	Rotor is designed for 1×10^{-9} failure probability. Rotor contains no windings, slip rings, magnets, etc. Stator is conduction cooled.	5	100	500
		Pump failure.	Cavitation erosion of impeller.	Decreased system fluid flow. Possible bearings damage with reduced or loss of system output capability. Contamination.	Due to high inlet pressure from jet condenser, cavitation should not be a problem. Material selection.	5	100	500
			Impeller shears from rotor.	Loss of system flow, loss of electrical power output. HSA overtemp. shutdown (EHDS).	Designed for 1×10^{-9} failure probability.	5	100	500
			Pump inlet seal failure results in degraded pump performance.	Reduced electrical power output capability.		10	50	500

FAILURE MODE AND EFFECTS ANALYSIS

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	DESIGN/SAFETY CONSIDERATIONS	4 of 13		
						③ CRITICALITY RANK, ① × ② × ③	② FE RANK	① FM LIKELIHOOD
1.5	<u>Combined rotating Unit (CRU)</u> (Continued)	Bearing failure.	Contamination, corrosion, loss of fluid film (plugged restrictor), pivot wear or brinelling causes CRU misalignment, mechanical interference.	Generates wear particles. Vibration, CRU damage. Reduction or loss of electrical power output.	Bearings are designed for low stress levels in the pivots. 3000 hours test time on Sundstrand 6 KW machine (using Dowtherm A working fluid) with no detectable tilting pad bearing damage. 16,500 hours test time on Sundstrand 1.0 KW REMCOM systems with 8,800 hours on one bearing set. Bearing pads are silver plated to prevent/minimize damage should a high speed rub occur. Sundyne, 6 KW & 1 KW tilting pad bearings use silver plate with no flaking problem.	25	100	2500
1.6	<u>Jet Condenser</u> Condenses turbine exhaust vapor by directing the vapor into a vapor funnel coaxially with liquid jets of subcooled liquid working fluid.	Condenser floods.	Liquid injector cracked due to material defect, manufacturing defect, fatigue due to vibration. Misdirected jets from liquid nozzles partially blocked with contaminant particles. Diffuser misaligned due to thermal effects. Excessive concentration of noncondensable gases. Jet condenser throat obstructed by contaminant particle.	Flow stops, loss of electrical power output. HSA overtemp shutdown (EHDS).	Liquid injector has 90 nozzles. Extensive development testing of jet condenser performed. Orifice diameter is 0.010 in. Filtration is provided upstream of jet condenser by filter at radiator outlet. Injector ring joints will be penetrant inspected.	25	100	2500

FAILURE MODE AND EFFECTS ANALYSIS

5 of 13

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	DESIGN/SAFETY CONSIDERATIONS	<div> <div>③ CRITICALITY RANK, ① x ② = ③</div> <div>② FE RANK</div> <div>① FM LIKELIHOOD</div> </div>		
						①	②	③
1.7	<u>System Accumulator and Filter</u>							
1.7.1	<u>System Accumulator</u>							
	Contains working fluid and pressured gas which are separated by a dual redundant metal bellows seal. Accumulator receives fluid leaving jet condenser and provides pressurized working fluid to CRU pump.	Bellows leaks.	Fracture at material defect, manufacturing defect, defective weld, fatigue.	No effect on system operation (redundant bellows)	Dual redundant bellows seal. Potentially, burn-in cycling may be conducted.	10	5	50
		Leakage between fluid and pressurization gas sides of accumulator.	Fracture at material defect, manufacturing defect, defective weld.	Fluid loss to gas side, pressurization gas in fluid loop. Gas in fluid loop floods out jet condenser. Loss of electrical power output. HSA overtemp. shutdown (EHDS).	Designed for 1×10^{-9} failure probability.	5	100	500
1.7.2	<u>Filter</u>							
	Filters contaminants from working fluid.	Filter clogged.	Upstream incipient failure generates particles; fluid deterioration products.	Reduced system flow, jet condenser floods out. Loss of system flow, loss of electrical power output. HAS overtemp. shutdown (EHDS).	Secondary failure.	10	100	1000
1.8	<u>Check Valve (System Accumulator Outlet)</u>							
	Prevents working fluid flow into system accumulator during start-up.	Fails to open.	Valve jammed closed due to mechanical failure.	PCS fluid loop blockage. Jet condenser floods out. System will not start.	Valve has large flow passages. Design is such that flow is thru clearance so that flow will tend to pass contamination thru valve.	10	5	50
		Failed open at start-up.	Valve stuck or jammed open due to contamination or mechanical failure.	Allows reverse fluid flow, during start-up, back to system accumulator. System may not start.	Valve is required to function during start-up only.	10	5	50

FAILURE MODE AND EFFECTS ANALYSIS

6 of 13

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	<div> <div> <div>③ CRITICALITY RANK, ① × ② = ③</div> <div>② FE RANK</div> <div>① FM LIKELIHOOD</div> </div> <div>DESIGN/SAFETY CONSIDERATIONS</div> </div>	①	②	③
1.9	<u>Check Valve</u> (System Pump Outlet) Prevents reverse working fluid flow at start-up.	Failure to open. Failed open at start-up.	Valve jammed closed due to mechanical failure. Valve stuck or jammed open due to contamination or mechanical failure.	System shuts down when start module is disconnected after start-up. Heater temperature control support equipment controls HSA temperature. System may not start.	Valve is required to function during start-up only.	10	5	50
1.10	<u>Radiator By-Pass Valve & Filter Assembly</u>							
1.10.1	<u>Radiator By-Pass Valve</u> Diverts flow around radiator to maintain jet condenser liquid in temperature above approx. 160°F.	Fails closed (loss of radiator by-pass capability).	Thermal Sensor failure due to bellows leakage.	Allows no radiator by-pass flow. Some reduction in system electrical power capability under certain conditions; loss of 35-40 watts in the worst case.	Thermal sensor is filled with Dowtherm A (system fluid). Valve design precludes fail open mode. Such a failure mode would result in max. power loss of more than 56 watts in the worst case. Bellows burn-in cycling may be conducted for flight system.	10	50	500
1.10.2	<u>Radiator Outlet Filter</u> Filters any spallation particles generated by meteoroid impacts on radiator tubes.	Filter clogged.	Upstream incipient failure generates particles; fluid deterioration products.	Reduced flow to jet condenser, jet condenser floods. Loss of system flow, loss of electric power output. HSA overtemp. shutdown (EHDS).	Secondary Failure.	10	100	1000
1.11	<u>Start Valve</u> Normally open solenoid valve is closed to allow pressure build-up in fluid cooling loop during initial stage of start-up sequence. Valve opens to allow fluid flow to jet condenser shower head for jet condenser operation.	Fails to close for system start-up. Fails to reopen during start-up.	Valve stuck open, electrical failure. Valve stuck closed.	System may not start. No start.		25	5	125
						10	5	50

FAILURE MODE AND EFFECTS ANALYSIS

7 of 13

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	DESIGN/SAFETY CONSIDERATIONS	③ CRITICALITY RANK, ① × ② = ③ ② FE RANK ① FM LIKELIHOOD		
						①	②	③
1.12	<u>Auxiliary Cooler</u> Provides for working fluid cooling during system enclosed operation.	System fluid side tubing rupture.	Material defect, manufacturing defect.	System working fluid leaks into coolant or coolant into system fluid loop. Eventual loss of electrical power output, contaminates coolant loop. Heater temperature control support equipment controls HSA temperature.	No joints internal to heat exchanger. Cooler designed for 1×10^{-5} failure probability.	5	100	500
1.13	<u>Flow Control Valve</u> Mechanical device which controls flow in turbine loop to maintain turbine inlet temperature (TIT). Flow limiter is two stage mechanical valve which controls flow to boiler in response to changes in supply pressure and changes in boiler output temperature. Maintains fluid flow in turbine loop at nominal value as supply pressure changes. Increases fluid flow in turbine loop as TIT increases. Decreases fluid flow in turbine loop as TIT decreases.							
1.13.1	<u>Thermal Sensor</u> Two redundant NaK filled bellows/bulbs position temperature bias nozzle flapper in response to TIT. Dual containment bellows on each thermal sensor.	Inner bellows leaks NaK into cavity between inner and outer bellows.	Bellows leakage due to fatigue, material defect, manufacturing defect, weld defect.	Other thermal sensor provides for continued system operation. Small step change in turbine inlet temperature. No effect on electrical power output capability.	Bellows burn-in may be conducted.	10	5	50

FAILURE MODE AND EFFECTS ANALYSIS

8 of 13

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	DESIGN/SAFETY CONSIDERATIONS	<div> <div> <div>③ CRITICALITY RANK, ① x ② = ③</div> <div>② FE RANK</div> <div>① FM LIKELIHOOD</div> </div> </div>		
						①	②	③
1.13.1	<u>Thermal Sensor</u> (Continued)	Outer bellows leaks.	Bellows leakage due to fatigue, material defect, manufacturing defect, weld defect.	No effect on thermal sensor operation. No effect on system operation. No effect on electrical power output capability.		10	5	50
		Bulb (tube) leakage or capillary tube leakage.	Tube leakage due to fatigue, material defect, manufacturing defect, weld defect.	Other thermal sensor provides for continual system operation. Small step change in turbine inlet temperature. External NaK leakage. No effect on electrical output capability.		5	5	25
		Capillary tube plugs.	NaK-carried impurities.	Thermal sensor failed extended -- System eventually runs cold; turbine inlet temp. too low for continued operation. Turbine speed decreases, jet condenser floods, flow stops. HSA overtemp. shutdown (EHDS).		5	100	500
				Thermal sensor failed retracted -- No effect. System continues operation under control of other thermal sensor. Small step change in turbine inlet temp. No effect on electrical power output capability.		5	5	25
1.13.2	<u>Pressure Motor</u> Dual containment actuator positions flow limiter nozzle flapper in response to delta P across temperature bias nozzle.	Bellows leaks excessively.	Bellows leakage due to fatigue, material defect, weld defect.	Secondary containment bellows unaffected. No effect on system operation. No effect on electrical power output capability.	Pressure motor has dual redundant bellows seal. Bellows burn-in cycling may be conducted.	10	5	50

FAILURE MODE AND EFFECTS ANALYSIS

9 of 13

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	DESIGN/SAFETY CONSIDERATIONS	<div> <div>③ CRITICALITY RANK, ① × ② = ③</div> <div>② FE RANK</div> <div>① FM LIKELIHOOD</div> </div>		
						①	②	③
1.13.3	<u>Nozzle Flappers</u> Flow limiter nozzle flapper meters flow through flow limiter nozzle. Temperature bias nozzle flapper meters flow through temperature bias nozzle.	Either nozzle flapper fractures at flex point	Fatigue, material defect, manufacturing defect.	System runs cold. Turbine inlet temperature too low for continued operation. Turbine speed decreases jet condenser floods, flow stops. HSA overtemp. shutdown (EHDS).	Designed for 1×10^{-9} failure probability. Reliability test for nozzle flapper	5	100	500
1.14	<u>Non-Condensable Gas Separator</u> Heat pipe device separates non-condensable gases from working fluid vapor and vents non-condensable gases thru capillary tube to space.	Loss of function.	Plugged capillary tube or fouled heat pipe wick caused by system contamination, fluid degradation products.	Potentially system life limiting due to build-up of non-condensable gases in system. Eventual loss of system.	Sensitivity of system to non-condensable gas build-up evaluated during GDS testing.	10	100	1000
1.15	<u>Disconnect</u> Quick-disconnect coupling provides for attachment and detachment of start module to PCS.	Poppet at PCS leaks prior to start-up.	Broken spring, damaged or deteriorated seal, contamination corrosion.	Allows air leakage into system prior to start-up. Possible inability to start system due to non-condensable gases in jet condenser.	Minor fluid leakage, which may occur when coupling is detached after start-up, will be blocked when hermetic seal is fixed into place.	10	5	50
		Poppet at PCS fails to close when start module is disconnected.	Same as above.	Loss of working fluid, loss of system flow. Loss of electric power capability. Heater temperature control controls heat source temperature.	A very small amount of fluid (at 217°F) may normally spill (.003 cu. in. max.) when start module is disconnected. Failure of the PCS poppet to close when the start module is disconnected after start-up will cause rapid loss of hot fluid (217°F), a hazard for test personnel.	5	5	25

FAILURE MODE AND EFFECTS ANALYSIS

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	DESIGN/SAFETY CONSIDERATIONS	10 of 13		
						③ CRITICALITY RANK. ①x②-③	② FE RANK	① FM LIKELIHOOD
2	<u>Radiator</u> Provides for waste heat rejection to space from circulated fluids.							
2.1	<u>Structural Parts</u> Skin, splice plates, fittings, channel frames, angle frames, and meteoroid shield, rivets, welds.	Structural failure	Handling damage, launch or transport dynamic forces	Twisted/distorted radiator resulting in a coolant system leak,	All basic structural type static components having no moving or operating parts. Experience data and Q.C. controllable.	5	100	500
2.2	<u>Emissive Coating</u> Improve heat rejection characteristics (high emissivity and low solar absorptivity)	Loss of coating	Dynamic Environments - shock, vibration Vacuum vaporization	Significant reduction in radiation heat rejection	Dynamic and vacuum tests	5	50	250
		Chipping	Thermal cycling Bending and torsion loading during handling Improper coating application Environments - humidity, salt air ultra violet light	Partial reduction in radiator heat rejection	Surface may be cleaned and refinished	10	50	500
		Cracking	Same as chipping	Minor effect on heat rejection		5	50	250
		Degradation	Solar absorptivity	Significant reduction in radiation heat rejection		25	50	1250
2.3	<u>Cooling Tubes, Coolant Manifolds and Connecting Tubes</u>	Rupture in tube wall or weld leak failure	Fatigue, material defect, defective weld Meteoroid Penetration	Leakage resulting in loss of cooling fluid, System overheats and over temperature shutdown (EHDS opens)	Long tube lengths (110 in.) seamless tubing Q.C. inspection of welds plus leak tests to detect possible leak points. Dowtherm A has narrow flameability limits - low explosion probability	50	100	5000
		Clogged or partially clogged line	Inner surface Meteoroid dent		Filters down-stream	50	50	2500

FAILURE MODE AND EFFECTS ANALYSIS

11 of 13

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	DESIGN/SAFETY CONSIDERATIONS	<div> ③ CRITICALITY RANK, ①x②-③ ② FE RANK ① FM LIKELIHOOD </div>		
						①	②	③
3.	<u>ELECTRONIC CONTROLS</u>							
3.1	<u>Tuning Capacitor Bank</u> Serves to decrease losses in alternator thereby increasing alternator efficiency.	Capacitor fails open.	Defective termination.	Power factor changes; decrease in alternator efficiency. Reduced system electrical power output capability.		10	50	500
		Capacitor fails short.	Ruptured/cracked dielectric.	Current surge results in open capacitor. Effect is same as above.		10	50	500
3.2	<u>Voltage Regulator</u> Provides field coil excitation to alternator.	Open circuit (as seen by alternator).	Circuit component failure due to thermal stress, vibration, shock.	No field current to alternator. Loss of electrical power output from alternator. System continues to run at no load speed (58,200 RPM).	High reliability parts JANTX and JANTXV diodes and transistors. Largest operating to rated stress ratio for a part is 0.29.	10	100	1000
		Short circuit (as seen by alternator).	Circuit component failure due to thermal stress, vibration, shock.	Maximum field current to alternator. Alternator output voltage varies with load. Load is maintained at design load by speed controller. At design load, output voltage is 39 volts (approx.).		10	50	500
		Drift of voltage regulator set point.	Circuit component parameter change due to thermal stress.	Output voltage outside of specified limits.		25	50	1250
3.3	<u>Rectifier</u> Converts alternator AC output to KIPS DC output.	One diode fails open.	Shock, vibration, thermal stress.	Ripple in DC power output. Low quality power.	JANTX qualified diodes. Operating to rated stress ratio for each diode is 0.22.	10	50	500
		One diode fails short.	Shock, vibration, thermal stress.	Alternator windings failure will result in loss of electrical power output from system.		10	100	1000

FAILURE MODE AND EFFECTS ANALYSIS

12 of 13

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	DESIGN/SAFETY CONSIDERATIONS	<div> <div> <div>③ CRITICALITY RANK. ①x②-③</div> <div>② FE RANK</div> <div>① FM LIKELIHOOD</div> </div> <div> <div>①</div> <div>②</div> <div>③</div> </div> </div>		
						①	②	③
3.4	<u>Speed Controller</u> On-off speed controller. Controls speed of CRU (and, thereby, output frequency of alternator) by switching parasitic loads to maintain an average alternator output load constant at load level required to maintain desired alternator frequency. 3 PLR's are used, each driven by a separate power switch. Any two of three PLR's are capable of handling full system output.	Circuit failed open.	Circuit component failure due to shock, vibration, thermal stress.	Continued system operation in frequency wild mode. As load decreases, CRU speed will increase (58,200 RPM at no load). No effect on DC output. No degradation in electrical quality.	High reliability parts. JANTX and JANTXV diodes and transistors. Largest operating to rated stress ratio for a part is 0.28. Stress ratio for most parts is less than 0.10.	10	5	500
		Circuit failed short.	Circuit component failure due to shock, vibration, thermal stress.	Continuous parasitic load (1950 Watt approx.) on alternator. CRU speed decreases and overload protection circuit removes field excitation. Loss of electrical power output. Heater temperature control module maintains HSA temperature. No effect on DC output. No degradation in electrical quality.		10	100	1000
		One of three parallel legs of power switch or PLR fails open.	Circuit component failure due to shock, vibration, thermal stress.	Continued system operation in frequency wild mode. As load decreases, CRU speed will increase (58,200 RPM at no load). No effect on DC output. No degradation in electrical quality.		10	5	50
		One of three parallel legs of power switch fails shorted.	Circuit component failure due to shock, vibration, thermal stress.	Continuous parasitic load (650 watts approx.) on alternator. Reduction in system useful power output to 650 watts. No degradation in electrical quality.		10	50	500

FAILURE MODE AND EFFECTS ANALYSIS

13 of 13

NO.	COMPONENT & FUNCTION	FAILURE MODES (FM)	POSSIBLE FAILURE CAUSES	FAILURE EFFECT (FE)	DESIGN/SAFETY CONSIDERATIONS	<div> <div> <div>③ CRITICALITY RANK, ① × ② × ③</div> <div>② FE RANK</div> <div>① FM LIKELIHOOD</div> </div> </div>		
						①	②	③
3.5	<u>Overload Protection Circuit</u> Removes alternator field excitation when alternator frequency drops below 95 percent of nominal.	Circuit failed open.	Circuit component failure due to shock, vibration, thermal stress.	Loss of system overload protection. In the event of an overload, system speed will decrease and system will not self sustain if overload is not removed. Loss of electrical power output.	High reliability parts. JANTXV diodes and transistors. Stress ratio for most parts is less than 0.10.	10	*	
		Circuit failed short.	Circuit component failure due to shock, vibration, thermal stress.	Loss of generator field excitation. Loss of electrical power output.		10	100	1000
3.6	<u>Parasitic Load Resistor (PLR)</u> High temperature radiator dissipates unused electrical power. Any two of three PLR's are capable of handling full system output.	One of the three load resistors fails open.	Shock, vibration, thermal stress, meteorite damage.	No effect on dc output due to redundancy. No degradation in electrical quality.	*Circuit provides protective function.	50	5	25

8.5 SINGLE POINT FAILURES

Based on the results of the Failure Modes, Effects and Criticality Analysis, single point failure sites have been identified and listed. Single point failures are component failures which would normally lead to a major power loss in the system.

Table 8-E lists the single point failure sites in the KIPS. The table is organized to separate component functional failures from failures which result in external leakage. Component functional failure sites are further grouped for mechanical components and electrical components. Finally, single point failure components are broken down to identify the single point failure parts.

Some of the single point failure sites result from system contamination due to an upstream failure. These sites are noted in the listing as secondary failures: filter plugged, bearing restrictor plugged, jet condenser throat plugged. Internal leakage failure sites are considered to be in the minor leakage category with no major system loss and are not included in the single point failure list. However, internal leakage between the accumulator pressurization gas and system fluid are included since system loss will eventually result. Component failures which result in system start failure are not included since they can be corrected prior to launch.

Table 8-E Single Point Failure Sites

SINGLE POINT FAILURE SITE	REMARKS
I. EXTERNAL LEAKAGE	Seamless tubing used throughout system.
A. Joints (External):	
Power Conversion System Joints (14) Jet Condenser/Accumulator Joints (8) Valve Pack Joints (7) Non-condensable Gas Separator Joints (16) Centrifugal Separator Joints (1) Radiator Joints (134) Interconnecting Tubing Joints (57)	Single containment joints are used; however, methods are available for incorporating double containment joints, if deemed desirable. Housings and tubing are sized for 1×10^{-9} failure probability.
B. Housings (External):	100% NDT of housings and joints. X-ray or ultrasonic inspection of housings and joints. Penetrant inspection may be performed in areas which will not see contact with working fluid. Helium leak checks of components and system.
Turbine Housing Regenerator Housing Jet Condenser Housing Accumulator Housing Valve Pack/Filter Housing Non-condensable Gas Separator (NCGS) Housing Centrifugal Separator Radiator Manifold Bearing Tee	
C. Tubing (External):	
Interconnecting Tubing Radiator Tubing HSA Boiler Tubing Electronics Cooling Tubing	
II. FUNCTIONAL COMPONENTS	
A. Mechanical Components:	
1. Combined Rotating Unit:	
1.a. Rotor Balance Assembly — Turbine Wheel — Alternator Rotor — System Pump	Rotor Assembly designed for 1×10^{-9} failure probability.
1.b. Radial Bearings (2): — Pads (4) — Pivots (4)	Rotor Assembly will be subjected to proof spin test.
1.c. Thrust Bearing: — Pads (6) — Pivots (6) — Load Levelers (12)	Bearings are designed for low stress levels in the pivots. Bearing pads are silver plated to prevent/minimize damage from rubs or particulate ingestion.
1.d. Bearing Flow Restrictors (2)	Sundstrand has used tilting pad bearings on the 6KW ORC, 1KW REMCOM ORC, and Sundyne petro chemical compressors. One bearing set accumulated 8800 hours without failure in the 6KW REMCOM ORC.
2. Valve Module:	Bearing restrictor plugging is a secondary failure resulting from system contamination. Filtration is provided upstream of restrictors.
2.a Thermal Sensor (2) (failed extended mode only)	High purity NaK used. Process controls imposed for cleaning and filling. NaK filled samples subjected to chemical analysis.
2.b. Flappers	NDT method to verify absence of gas bubbles should be developed.
2.c. Filter	Flappers are sized for 1×10^{-9} failure probability. Flapper reliability test completed during Phase I.
	Filter plugging is a secondary failure due to system contamination. Filter has adequate capacity.

Table 8-E Single Point Failure Sites (cont'd)

SINGLE POINT FAILURE SITE	REMARKS
3. Non-condensable Gas Separator	Single point failure modes are a fouled heat pipe wick or plugged capillary vent tube. These are secondary failures resulting from system contamination or fluid degradation products. Centrifugal separator traps fluid degradation products (tarry residue).
4. Jet Condenser:	Extensive development testing of this jet condenser performed during Phase I. Filtration is provided upstream of the jet condenser injector to prevent nozzle plugging. It is estimated that as many as 30 percent of the nozzles may be plugged without system shutdown, but with some drop in system efficiency. With 30 percent of the nozzles plugged, a system efficiency drop of 1.5 points would result. Jet condenser throat plugging is a secondary failure which would result from ingestion of a large contaminant particle.
4.a. Injector	
4.b. Throat	
5. Accumulator	Filter plugging is a secondary failure due to system contamination. Filter has adequate capacity.
5.a. Filter	
5.b. Pressurization Gas Containment	Internal leakage between the pressurization gas and the system fluid would result from leakage of the accumulator inner housing, diaphragm or welded joints. 100% X-ray or ultrasonic inspection of the housing, diaphragm and joints. Helium leak checks of the accumulator as a component will be conducted.
B. Electrical/Electronic Components:	
1. Alternator Stator	Alternator windings temperatures are well below rated temperature. Maximum continuous winding temperature is 121°C vs. insulation system rating of 230°C for 60,000 hours. Dielectric strength test will be performed.
2. Connectors	The highest reliability connectors will be used.
3. Controller (23):	The baseline controller is essentially single channel. As such, it contains numerous single point failures. However, if deemed desirable, redundancy can be incorporated in the controller to eliminate all single point failures. The electronic device failure rates should be extremely low. The highest reliability parts available will be used. The largest operating to rated stress ratio for a part is 0.29. Stress ratios for most parts is less than 0.10. The highest calculated failure rate for a single point failure part is 0.0056×10^{-6} failure per hour for filter L3.
Diodes (7):	
Transistors (10):	
Resistors (5):	
Filter (1)	
C. Other Components:	
1. HSA Multifoil Insulation (premature meltdown)	EHSA foil system meltdown test conducted during Phase I.