Gravity Probe-B
System Reliability Plan

***Document* #P0146**

Samuel P. Pullen
N. Jeremy Kasdin
Gaylord Green
Ben Taller

Hansen Experimental Physics Labs: Gravity Probe-B
Stanford University

January 23, 1998

1.0 Introduction

The Gravity Probe-B Relativity Mission is unlike most spacecraft in that it is dependent on a number of new systems, which have never flown in space before, to carry out tests of General Relativity to the required precision. In addition, care must be taken to minimize disturbances, since values that are tolerable for most spacecraft are not tolerable for GP-B. As a result, GP-B will benefit from a modified reliability and Failure Modes, Effects, and Criticality Analysis (FMECA) procedure that uses both accepted NASA and Defense Department standards combined with newer techniques that better (or more easily) estimate performance uncertainties in orbit.

Our planned system-level reliability analysis for the GP-B mission includes both the science instrument assembly and electronics, the dewar hardware, and the spacecraft bus that supports the experiment. The spacecraft bus uses conventional technology for the most part, so its reliability will be computed using variants of standard calculations carried out by Lockheed-Martin. However, it will also be in a form that is compatible with the newer methods used to characterize the uncertainties of the experimental payload.

Reliability efforts for the payload will develop standard FMECA analyses of likely failure modes into subsystem-level models of mean reliability and reliability uncertainty using a new technique described here. Reliability and uncertainty estimates for the spacecraft bus use an improved method that converts available exponential failure rates for each component into an uncertain Weibull failure model. Although one can combine mean reliability predictions in the standard way to produce expected spacecraft reliability over time, Monte Carlo simulations of the each subsystem on the payload and spacecraft bus will give us the clearest picture of the overall performance uncertainty. These simulations will also highlight which systems are the most unreliable and/or most uncertain. This should lead to a closer focus on these areas insofar as their failure likelihoods are controllable.

2.0 Spacecraft Bus Reliability Methodology

It should be noted that the primary contractual responsibility for assuring reliability for the GP-B spacecraft bus resides with Lockheed Martin. The approach presented here is intended to *augment* their reliability analyses and allow us to combine failure uncertainty models for the spacecraft bus and payload into an overall mission reliability prediction.

2.1 Subsystem Part Counts and Uncertain Weibull Failure Models

For a given subsystem, the standard reliability analysis begins with an electronic part list and a list of possible non-electronic failure modes. Projected failure rates for each part will be obtained using MIL-HDBK-217F methods as usual. This results in a failure rate parameter λ for each component that can be used in an *Exponential distribution* to give the reliability of that component as a function of time. Using *Nonelectronic Parts Reliability Data (NPRD) - 1995* (Reliability Analysis Center, 1995), we can estimate similar failure rates for some of the components and failure modes not covered by MIL-HDBK-217F.

These exponential failure predictions have two potential areas of improvement. First, the tabulated failure rates can be inaccurate, or they may be based on parts that are not the same as the ones GP-B is using. Second, the exponential model of spacecraft failures can be improved. Typically, failures occur more often early in the mission, as hidden failures become apparent. Units that survive "burn-in" ground tests and the first year of spacecraft operations are less likely to fail randomly later in the mission. GP-B is of relatively short duration; thus exponential reliability predictions may be somewhat optimistic.

Two new measures are taken to address these concerns and better model GP-B performance uncertainties. We use the *Weibull distribution* to model failure probability, using a new approach to convert standard handbook failure rates to Weibull parameters. In addition, a model of Weibull parameter *uncertainty* has been derived for both MIL-HDBK-217 and NPRD data. Essentially, each component type has an uncertainty factor, which is also based on where the data was taken from. This uncertainty represents possible design flaws or improvements to the part in question as well as the quality of the handbook data. In a *Monte Carlo*

simulation, we can generate random numbers to resolve this uncertainty for each trial, then use the result to compute the Weibull reliability prediction for that unit as a function of time. A detailed explanation of the procedure being used here is given in Chapter 3 of Dr. Samuel Pullen's doctoral dissertation entitled *Probabilistic Engineering Design Optimization: Applications to Spacecraft and Navigation Systems* (Stanford University, SUDAAR 680, June 1996).

2.2 Subsystem Reliability Analysis Procedure

Reliability data for each of the GP-B subsystems will come from various sources. Where applicable, handbook failure rates from MIL-HDBK-217F and NPRD-95 will provide the starting point, but test data will be directly factored in as much as possible to both modify the handbook values and to reduce our uncertainty regarding the "true" failure rate. FMECA analysis of each subsystem will also provide a list of the most important system-level failure modes.

Given a set of failure distribution parameters, either the nominal ones or those resulting from a simulation trial, the subsystem-level reliability prediction is computed from its *functional block diagram*. The general principle here is that there should be no *single-point failures*, or component-level failures that cause overall mission failure by themselves. There will usually be parallel or *k*-out-of-*n* *redundancy* at the component level to avoid this. Using the standard methods for series, parallel, and *k*-out-of-*n* "binomial" function blocks (given in MIL-HDBK-756B), a reliability prediction for the subsystem is computed. Essentially no revisions to this accepted procedure are proposed by GP-B, except that in a few cases we will not make the standard *independence* assumption for failures in separate blocks. Specifically, whereas traditional reliability analysis assumes that failures of identical redundant blocks are independent of each other, the similarity between the blocs suggests that an observed failure in one of them *increases* the likelihood of a failure in the second (redundant) block (for example, if the same flawed part were included in both components). In these cases, "common-cause" failure modes may increase the probability of failure for parallel components.

At any given stage of the development process, an "up-to-date" reliability analysis for a given subsystem can be conducted based on its latest failure parameters and uncertainties. The mean reliability can be computed analytically

from the mean reliability numbers for all the failure modes, but more useful information will be obtained by running Monte Carlo simulations for each subsystem. A large number of independent sampling trials will be conducted. In each trial, a "true" success probability will be sampled for each unit and failure mode, and the multiplication of these together gives the overall subsystem reliability for that trial. Storing the results of all the trials in a histogram gives a mean reliability estimate and also shows the spread of reliability uncertainty for that system. Comparisons to similar reliability estimates for other systems will help us identify areas where more mitigating steps are required to limit this performance uncertainty to acceptable levels.

3.0 Payload Reliability Methodology

3.1 Motivation and Outline of FMECA Reliability Method

The GP-B scientific payload must be handled in a different way from the spacecraft bus because some of the payload subsystems have little or no orbital history. In a few cases, the designs themselves are new. As a result, failure modes are difficult to determine in a component-by-component sense. Doing a complete component failure rate lookup and conversion (as is being done for the spacecraft bus) is thus impractical. We have devised a new method of making reliability estimates using relevant FMECA analyses. This approach will be used to forecast reliability uncertainty for each major payload subsystem as the relevant FMECA are completed (by Lockheed) and converted. In addition, subsystems in the spacecraft bus that are substantially new and untested in space, such as the helium thrusters used for attitude control, will be handled in the same manner rather than relying on MIL-HDBK-217F failure rates.

FMECA analysis is a normal requirement of spacecraft development programs, and the procedure is generally governed by MIL-STD-1629A. Separate FMECA procedures are being used for the GP-B spacecraft bus and for the payload. The spacecraft bus FMECA simply lists the system-level redundancy for each mission failure mode. However, the payload FMECA analyses more clearly follow the pattern of MIL-STD-1629A by creating more detailed lists of failure modes and ranking them by the following three (subjective) parameters:

Pr(M) = *probability of occurrence* = an estimate of the relative probability of occurrence of a given failure mode

S_{ev} = *severity of effect* = an estimate of the worst likely consequence of a given failure mode to the overall mission

β = *conditional probability of worst postulated effect* = an estimate of the probability of the worst likely consequence *given* that the failure event has occurred

Tables 1-3 summarize the possible states of these three parameters. Normally, these values are given numerical weights and then multiplied together to give a *criticality* ranking for each failure mode. Lower criticality ratings indicate more threatening failure modes, and criticality values lower than 8 on this scale are considered to be unacceptable, requiring some form of risk mitigation to reduce their danger. Criticality rankings also help identify which failure modes carry the most risk, even when that risk is deemed acceptable.

In addition, Tables 1-3 contain uncertainty distributions of failure probabilities for each possible state. The mean failure rates for each state are based on the assumptions by which possible failure events are classified by the FMECA methodology. Since these "implied" failure probabilities are not meant to be specific, considerable uncertainty exists that is modeled by the probability distributions given for them.

Pr(M)	Meaning	Failure Prob. Dist.(μ,σ)
A	frequent	Gamma(0.2, 0.125)
B	probable	Gamma(0.1, 0.07)
C	occasional	Lognormal(2.0, 0.5)
D	remote	Lognormal(3.0, 0.75)
E	improbable	Lognormal(5.0, 1.5)

Table 1: Occurrence Probability States

Sev.	Meaning	Failure Prob. Dist.(μ,σ)
1	catastrophic	Uniform[0.5, 1.0]
2	critical	Gamma(0.1, 0.05)
3	minor	Lognormal(2.0, 0.5)
4	other	Lognormal(3.0, 0.75)

Table 2: Severity Probability States

β	Meaning	Failure Prob. Dist.(μ,σ)
1	actual loss	Uniform[0.7, 1.0]
2	probable loss	Normal(0.5, 0.15)
3	possible loss	Gamma(0.05, 0.03)
4	no effect	Lognormal(5.0, 1.5)

Table 3: Conditional Probability States

Note that the Lognormal distributions listed above are distributions of an exponent x, where the probability of the underlying event is 10^{-x}. For given sampled values of the appropriate probabilities of the events signified by Pr(M), S_{ev}, and β, the probability of mission failure due to a particular FMECA failure event is given by:

$$Pr(MF) = Pr(M = occur)\ Pr(S_{ev} \mid occur)\ Pr(\beta \mid S_{ev})$$

More simply, multiplying the three failure probabilities sampled from Tables 1-3 gives Pr(MF), the probability of mission failure.

3.2 FMECA Procedure for Electronic-Box Assemblies

Electronic boxes in the GP-B payload subsystems do not need very detailed FMECA's, since the relevant failure modes generally involve individual electronic parts. Since piece-part MIL-HDBK-217 reliability calculations are not done for payload electronics (many of which are one-of-a-kind items), FMECA's are still needed to provide reliability estimates.

Accordingly, each GP-B payload electronic box will be evaluated by a brief FMECA that focuses on the most critical failure modes -- those that would result in a non-trivial failure probability from the conversion method of Section 3.1. In some cases, critical piece-parts (and their temperature sensitivities) will need to be evaluated in detail using MIL-HDBK-217-related techniques. In general, Stanford will take the lead in developing these summary FMECA's, and Lockheed-Martin will be called on where help is needed in determining the failure rates for critical parts or when more detailed failure-mode breakdowns are required.

3.3 FMECA Procedure for Non-Electronic Assemblies

While some non-electronic assemblies have failure data tabulated in NPRD-95, the generic numbers found there are not likely to be very relevant for the special components required by GP-B. While they may be used as a guide where available, the detailed FMECA's produced by Lockheed-Martin will serve as the primary source for reliability predictions along the lines of Section 3.1. These FMECA's contain failure modes relative to ground storage, launch, and orbital stages of the mission. Only failure modes related to the latter two (i.e., during and after launch) will be included in the reliability calculations.

3.4 FMECA Reliability Conversion in Practice

Since the implied failure event probabilities given in Tables 1-3 are uncertain, Monte Carlo simulation must again be used to resolve them. For a given sample trial, "true" failure probabilities are sampled from the above distributions, and then Pr(MF) is computed for each listed failure cause. Failure causes that are similar in physical origin, such as failure of a sensor type that exists in several places on the apparatus, use the same sampled failure probabilities for each cause of that type. In this way, failure rate dependencies are modeled for events where the underlying failure likelihoods are correlated.

To compute the overall subsystem mission failure probability for a given trial, the mission failure probabilities for each event are multiplied together as in a series network. Note that at this level, probabilistic *independence* is indeed assumed. While much of the correlation between different failure modes is captured by the common failure probability sampling just described, the assumption of independence

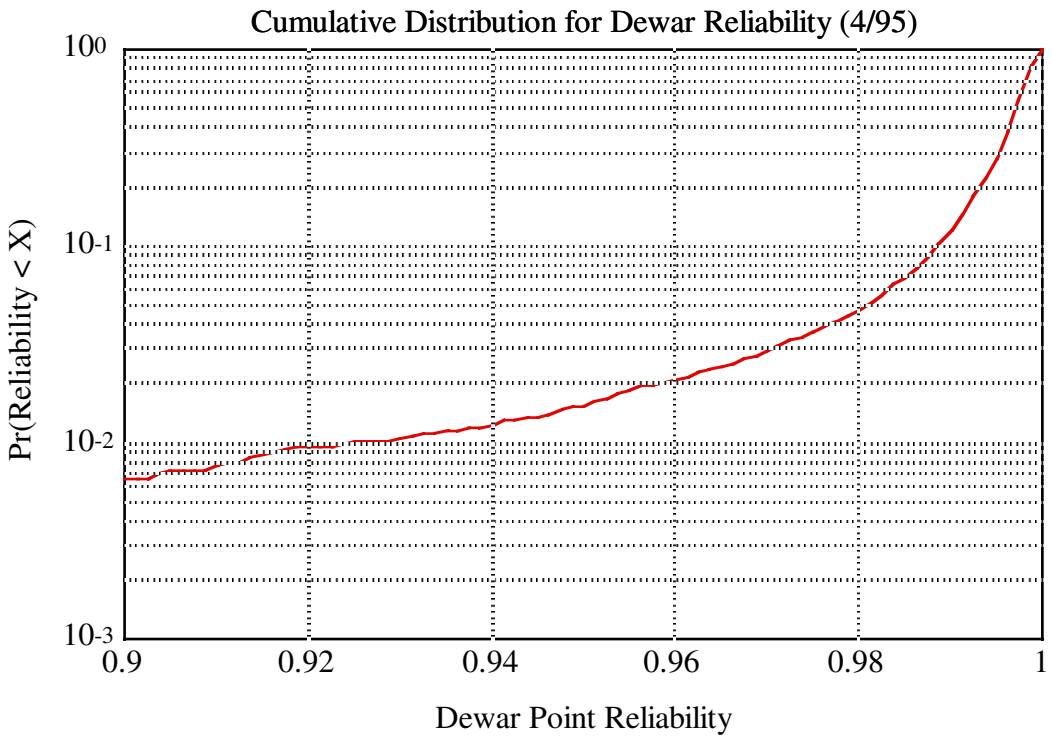

Figure 1: Cumulative Distribution of Dewar Reliability

at the top level (failure *occurrences* are independent even though failure *likelihoods* are correlated) may be questionable in a few cases. If such cases exist, they will be identified as such in the analyses and handled separately (so that independence is not assumed where it does not apply).

As in the spacecraft bus sampling procedure, top-level reliabilities for each trial are stored in histograms which are plotted and analyzed after all trials are completed. For the GP-B payload development program, draft FMECA's are presented at the PDR for each subsystem, and revised ones are completed by CDR. Thus, we will conduct reliability conversion analyses for each subsystem separately as its FMECA is completed. A subsequent Monte Carlo sampling procedure will be used as needed to combine subsystem reliability histograms into an overall payload reliability prediction.

As an example of a FMECA-derived reliability prediction, Figure 1 above shows a plot of the cumulative distribution function of reliability uncertainty for the GP-B dewar subsystem. The *x*-axis gives various reliability values, and the *y*-axis gives the probability that the true (unknown) dewar reliability is lower than that *x*-

axis value. The *median* of the reliability distribution, or the point where the *y*-axis probability of occurrence is 50%, is the most important number relative to more-common deterministic reliability predictions. In this case, the median dewar reliability is about 0.997, which is quite high. The plot also shows that the probability of the true dewar reliability being below 0.99 is just over 10%, and it is below 4% for reliabilities below 0.98. However, given what is now known about the dewar subsystem, there remains a very small probability of the true reliability being unacceptably low. In cases where this probability is unacceptable, more information is needed from the design and test process, and FMECA updates should be conducted once this information is available so that overall risk can be re-assessed. This is similar to what would be done for failure modes of unacceptably high criticality as defined by MIL-HDBK-1629A.

4.0 Overall GP-B Spacecraft Reliability Analysis

Once the reliability analyses from Sections 2.0 and 3.0 are complete, a comprehensive estimate of the overall probability of mission success for GP-B will be computed by multiplying together the independent reliabilities computed for the spacecraft bus, payload, and any relevant external categories (e.g., environment, interfaces). A mean reliability estimate for the mission can always be calculated analytically by multiplying the median reliabilities of each of these classes together, so long as the independence assumption is not violated. This overall median reliability number should give a basic level of assurance. However, our focus will be on simulation results for the overall mission.

In each Monte Carlo trial, reliability samples will be taken from the output reliability histograms from the latest simulations of each class (from Sections 2.0 and 3.0), and these samples will be used to compute the combined mission reliability for that trial. Accumulating these results into a histogram will give an excellent picture of the current reliability status of the GP-B program as a whole. Note that simulation requires that a sufficient number of samples be generated to achieve reasonable confidence that the result is a "good" estimator of the true reliability. In this case, the number of samples is on the order of 50,000 - 100,000, which gives good confidence for reliability estimates with two or three digits after the decimal. This means that the statistical uncertainty is far smaller than the

uncertainty in the reliability models and parameters that dictates the use of simulation in the first place.

Since both failure rate estimates and uncertainty factors will be changing at various levels of detail throughout the development program, periodic repetitions of the simulation process with the latest data will illustrate the trend of reliability improvement for NASA and program management. This is a great improvement over doing a conventional reliability analysis once using only handbook data. Reliability changes over time can do more than express the remaining performance uncertainty. They can also help illustrate where sufficient reliability assurance has been attained, relative to failure modes that cannot be helped, and where more effort is needed to achieve additional design or analysis improvements in subsystem areas which might otherwise drag down the overall probability of success.

5.0 Organizational Responsibility for Reliability Tasks

Responsibility for the analyses and predictions called for in this reliability plan lies in several organizations at Stanford and at Lockheed-Martin. This section details the organizations and personnel responsible for each task and its current status along with their estimated completion dates.

5.1 Stanford University Responsibilities

The systems engineering effort at Stanford University, formerly led by N. Jeremy Kasdin and now led by Gaylord Green and Bob Schultz, has primary responsibility for the following tasks:

1. completion of FMECA's for payload systems
2. payload reliability predictions based on payload FMECA's
3. adjustment of spacecraft reliability prediction based on LMMS MIL-HDBK-217F analysis
4. oversight of test and quality assurance efforts

Task 3 above has recently been updated into a near-final form. Tasks 1 and 2 have been prioritized based on the CDR schedules for each payload subsystem, although

they may be completed earlier for subsystems where reliability is a key input to design decisions. Task 4 is ongoing. Mr. Green and Mr. Schultz are supported by Dr. Sam Pullen and Ben Taller in these efforts.

Table 4: Reliability Completion Schedule

5.2 Lockheed-Martin Responsibilities

The GP-B prime spacecraft contractor, Lockheed-Martin, is responsible for completing all reliability-oriented analyses for the spacecraft as well as supporting Stanford's reliability efforts on the payload. In particular, these responsibilities include:

1. completion of spacecraft FMECA
2. completion of MIL-HDBK-217F reliability analysis
3. completion of certain payload subsystem FMECA's delegated by Stanford
4. oversight of spacecraft test and quality assurance efforts

Task 2 was completed at the time of proposal approval and was updated at the time of Spacecraft CDR-2 in August 1997. Stanford has recently updated its adjustments as mentioned above. Task 1 has been re-worked to conform to the requirements of MIL-STD-1629A and is essentially done. Tasks 3 and 4 are ongoing.

5.3 Schedule for Completion

Table 4 below lists the top-level reliability tasks for GP-B and gives our proposed schedule for their completion. These dates conform to the reporting requirements and are targeted toward specific dates of planned reviews as shown in the table.

Task	Completion Date	Review
payload FMECA's	2/26/98	SLVR/L-2
payload reliability	2/26/98	SLVR/L-2
spacecraft FMECA's	8/27/97	Spacecraft CDR-2

6.0 Conclusion

This plan outlines the reliability analysis and assurance provisions for Gravity Probe-B. The focus here is on numerical predictions of reliability and uncertainty that are realistic on an absolute as well as a relative scale. These should facilitate risk-reduction efforts throughout the spacecraft development timeline. This plan is also part of a greater effort that includes and utilizes part and assembly screening, component/subsystem testing, and mission-wide quality assurance.