Requirements for

RELIABILITY AND MAINTENANCE ANALYSIS AND ASSESSMENT OF SPACE SHUTTLE AND OTHER SPACECRAFT ELEMENTS

Safety, Reliability, and Quality Assurance Office
Johnson Space Center
October 6. 2000

Prepared By

Richard P. Heydorn
Code NX / Technology Division

Approved By

Malcolm J. Himel Jr.
Code NX / Chief, Technology Division

John H. Casper
Code NA / Director, Safety, Reliability, and Quality Assurance Office

FOREWORD

This document defines the structure and content of an approach for conducting a reliability and maintenance (R&M) analysis and assessment. It's primary purpose is to serve as an instrument for establishing an R&M analysis and assessment agreement between a contractor and the Safety, Reliability, and Quality Assurance (SR&QA) Office of the Johnson Space Center (JSC). It is also a document that presents basic principles of an R&M analysis and assessment that are endorsed by the SR&QA office of JSC. Accordingly then, this document should be considered by anyone performing an R&M analysis and assessment for the SR&QA office at JSC.

It is recognized that one document cannot cover the best analyses and assessments that should be done over a broad spectrum of problems. This document should not be a substitute for good technical leadership. Conversely, however, good technical arguments should be presented for not following the principles of this document. Reliability and maintenance is not a static science and therefore this document is expected to evolve as it becomes apparent that other aspects of R&M analysis and assessment should be covered. Partially in this spirit of evolving into a more authoritative document, several appendices are included. These appendices have evolved from analyses that have been done prior to the writing of this document. While they represent, possibly an incomplete, theory of how to handle certain circumstances of reliability estimation, they do contain concepts that should be further developed and demonstrated through analysis of real systems.

Emphasis has been placed on reliability and maintenance as a process. In particular, R&M in a space program is difference from R&M that is often related to the manufacturing of a large number of items. There it makes sense to cast reliability in terms related to placing items on test and deducing their propensity to fail. In a typical space program, only a few items are produced, and therefore, to deduce the reliability of an item often requires a process of monitoring, estimation, and assessment that takes place during the operation of the item. During this time the item may be repaired or renewed and placed back in operation and so concepts related to repairable or renewable processes should be considered. And, consequently this is the emphasis that is intended in this document.

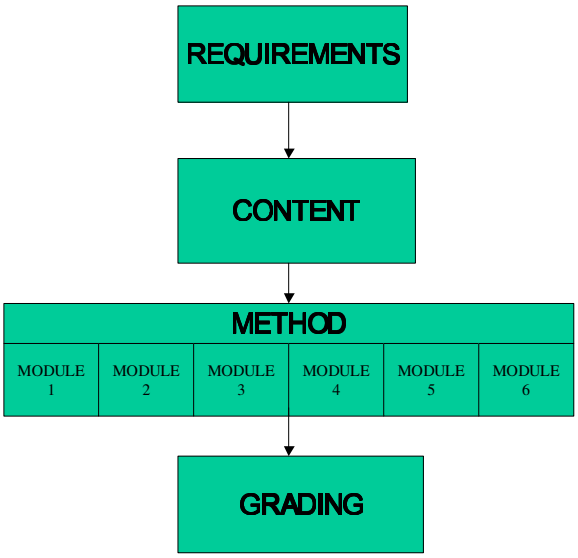
Finally, it should be noted that reliability is covered in much more detail than is the subjects of maintenance, cost, and schedule. This reflects the emphasis that has been placed on these subjects in past analyses done by the JSC SR&QA office with the possible exception of certain maintenance analyses and assessments that have been done. Once again this may change as this document evolves.

TABLE OF CONTENTS

SECTION	PAGE
DOCUMENT OVERVIEW	5
I. RELIABILITY AND MAINTENANCE (R&M) REQUIREMENTS	6
II. CONTENT OF THE R&M ANALYSIS AND ASSESSMENT	7
III. R&M METHOD MODULES	10
MODULE 1: RELIABILITY AND MAINTENANCE ANALYSIS AND ASSESSMENT PROCESS REQUIREMENTS	11
MODULE 2: RELIABILITY AND MAINTENANCE STATISTICAL METHODS REQUIREMENTS	13
Appendix I: Estimating the Reliability of HAINS Gyros – A Case Study in the Analysis of Repairable Systems in the Presence of Time Censoring	19
Appendix II: Estimating Reliability When No Past Failures Have Been Observed	22
Appendix III: Estimating Parameters in a Weibull Process: An Explanation of the AMSAA Model	27
MODULE 3: DATA REQUIREMENTS	30
MODULE 4: CORRECTIVE AND PREVENTIVE ACTION REQUIREMENTS	31
MODULE 5: ROOT CAUSE ANALYSIS REQUIREMENTS	32
MODULE 6 REPORT CONTENT REQUIREMENTS	34
IV. GRADING CRITERIA	39
References	40

DOCUMENT OVERVIEW

This document is divided into four major parts. These are Requirements, Content, Method, and Grading. When performing an R&M analysis and assessment, the activity should flow as shown below beginning with Requirements and ending with Grading.



Requirements

The requirements are the objectives of the analysis and assessment. In this document, a basic set of requirements are listed. These are the requirements that should be followed if a customer requests a typical R&M analysis and assessment without specifying specific requirements.

Content

The content is a list of specific topics that are to be part of an analysis and assessment should the effort be directed by the basic set of requirements. This content is laid out in the form of a matrix which can be used as a summary of agreement between the contract manager and the contractor.

Method

This part of the document deals with some of the specific statistical models that are endorsed by JSC SR&QA for doing a basic analysis and assessment. In this part separate modules discuss the methods that are to be employed. By modularizing this part of the report it was felt that changes could be easily incorporated in later versions without disrupting other parts of the document. The intent, of course, is to allow for an evolution of this document as new and improved methods of analysis become apparent.

Grading

A grading section has been included to provide a means for evaluating the performance of the contractor and to standardize the evaluation procedure for the contract technical monitor.

RELIABILITY AND MAINTENANCE (R&M) REQUIREMENTS

Customer Requirements for a Basic R&M Analysis and Assessment

General Requirements

1. Assess Shuttle hardware elements in terms of safety risk, operational cost risk, and operational schedule risk.
2. Provide supportive data and data assessments to project management required for making decisions related to appropriate corrective action to reduce safety risk as well as operational cost and operational schedule risks.
3. Estimate the reliability of a given hardware element and provide suitable confidence bounds. Compare to stated reliability goals and vendor expectations.
4. Estimate expected repair time and confidence intervals of a given hardware element.

Safety Risk Requirements

1. For a given hardware element, assess the contribution to the safety risk of each Shuttle system function that the element supports.
2. Compare the hardware element safety risk contribution to stated goals and vendor expectations.
3. Forecast the contribution of the hardware element to the safety risk related to given mission scenarios.
4. Provide data and data assessments that will aid in the determination of the root cause of a failure. Where possible relate failures to pertinent FMEA/CIL and hazard reports.
5. Provide data and data assessments that will support forecasts of safety impacts of proposed corrective actions.

Operational Cost Risk Requirements

1. Provide data and assessments to support estimation of the Shuttle operational cost risk due to the hardware element failures.
2. Develop maintenance strategies for reducing the operational cost risk attributable to the hardware element failures.

Operational Schedule Risk Requirements

1. Estimate the contribution of hardware element failures to the critical path time distribution of the Shuttle operations schedule.
2. Develop maintenance strategies for reducing shuttle operations schedule impacts due to failures of hardware elements.

CONTENT OF THE R&M ANALYSIS AND ASSESSMENT

This section is designed to be a concise agreement between the contractor and the government on what is to be done. This agreement is laid out in the form of a matrix in Table II.1. The first column of the matrix is a listing of the 8 categories that are expected to be part of a basic R&M analysis and assessment. The second column is a listing of the topics that can be a part of each category. In some cases items in the second column provide more detail on what is expected to be covered in the related category. Under the category 1.0 Specifications, for example, there are five major items that are expected to be covered. In other cases this column gives certain options that can be chosen. For example, under the subcategory 4.1 Mission Reliability, there are two options. One specifies that the analysis and assessment consider how a failure of a unit affect the function that the unit supports. The other specifies that a safety analysis and assessment will be done. That is, if this second option is selected and, for example, the units being analyzed are part of the guidance navigation and control system (GN&C), then it is expected that the analysis and assessment will address how failures of these units affect the loss of vehicle and crew and comment on the safety implications of these failures. The government and the contractor are expected to agree upon the items in column 2 that will be part of the final analysis and assessment. The third column will show what has been agreed upon. The fourth column is to be filled out by the contractor upon completion of the analysis and assessment. The contractor is required to indicate where the corresponding topic agreed upon in the "plan" column appears in the final report. This can be done by citing the appropriate page and paragraph number. The last column is to be used by the government to show how each category was evaluated.

Upon selection of the subcategories for analysis and assessment the contractor may choose to submit a proposal to the government that specifies the detail that will be covered in the selected subcategories. This proposal may also identify the specific types of data that will be used and the resources and schedule required to complete the analysis. Interim negotiations of the requirements as agreed upon in this proposal may be necessary to cover unforeseen events that may occur during the course of the analysis and assessment.

Table II.1

R&M CONTENT FOR ELEMENT _____

Note: An element is at one of the following levels: functional, system, or LRU.

Analysis and Assessment Category	**To Be Included in the Analysis and Assessment Category ***	**Plan ****	**Actual *****	**Grade ********
1.0 Specifications	1.1 Manufacturer 1.2 Name of major elements , part numbers, serial numbers 1.3 Vendor specification of reliability 1.4 Life limit 1.5 Repair and servicing details.			
2.0 Data Module Reference [3]	2.1 Data fields as given in Module [3] 2.2 Revised fields			
3.0 Scenarios	3.1 Mission scenarios (e.g. flights to support space station) 3.2 Flight rules (e.g. minimum number of elements that must operate before early termination of the mission) 3.3 Special scenarios			

Analysis and Assessment Category	To Be Included in the Analysis and Assessment Category *	Plan **	Actual ***	Grade ****
4.0 Quantitative Analysis and Assessment				
4.1 Mission Reliability Module Reference [1]	4.1.1 Contribution of the element to the failure of the host function 4.1.2 Reliability of the element as it relates to the loss of vehicle or crew			
4.2 Hardware Reliability Module References [1],[2]	4.2.1 Reliability growth 4.2.2 Wearout 4.2.3 Random failure			
4.3 Maintenance Module References [1],[2]	4.3.1 Corrective maintenance 4.3.2 Preventive maintenance			
4.4 Cost Risk Module Reference [1]	4.4.1 Incorporate element cost risk into a vehicle life cycle cost model 4.4.2 Cost risk of the element 4.4.3 Cost benefit			
4.5 Schedule Risk Module Reference [1],[2]	4.5.1 Incorporate schedule risk into a vehicle operational network schedule model 4.5.2 Compute statistics on the time to repair or renew			
5.0 Quantitative Findings Module Reference [2]	5.1 Point estimates and confidence intervals 5.2 Point estimates 5.3 Some combination to be explained			
6.0 Root Cause Analysis and Assessment Module Reference [5]	6.1 Root cause analysis and assessment using existing data 6.2 Defer to a separate study that requires additional data			
7.0 Summary, Conclusions, and Recommendations	7.1 Discussion of findings related to each major analysis and assessment objective 7.2 Corrective and preventive actions recommendations. 7.3 Impacts and benefits of corrective and preventative action			
8.0 Report Format Module Reference [6]	8.1 Executive summary presented in a “dashboard format”. 8.2 Objectives of the analysis and assessment 8.3 Background 8.4 Analysis and assessment methodology 8.5 Analysis and assessment findings 8.6 Root cause of failures 8.7 Corrective and preventive action and the benefits 8.8 Conclusions and recommendations 8.9 References 8.10 Data Appendix			

* Subject to the concurrence of the responsible division, the contractor has the option to select subject topics in this column to be covered in the analysis and assessment.
** Contractor should select items from column 2 that are to be part of the analysis and assessment.
*** Contractor should specify where the selected item in the Plan Column appears in the final report. Specify page and paragraph.
**** A grade will be assigned by the responsible division upon completion of the study in accordance with criteria stated in this grading criteria section.

CONCURRENCE:

Responsible Division Manager

Contractor Manager

R&M REQUIREMENT MODULES

The R&M requirement modules provide an explanation of the categories listed in Section II. In the matrix in Table II.1 of Section II these modules are referenced by the bracketed numbers. These modules should give the contractor a basic understanding of what material is expected to be included in a basic analysis and assessment if it can be supported by data and resources. They are not, however, to be considered to be a complete tutorial on a subject. Some subject matter is covered more briefly than others, so the contractor should rely on the government technical monitor of a given analysis and assessment to provide any missing detail.

There are 6 modules. An annotated listing is as follows:

[1] Reliability and Maintenance Analysis and Assessment Process Requirements

This module divides the analysis and assessment into five parts called Mission Reliability, Hardware Reliability, Maintenance, Cost Risk, and Schedule Risk. The requirements for these parts specify the topics that are to be considered in the analysis and assessment, but do not define the specific estimators to be used.

[2] Reliability and Maintenance Statistical Methods Requirements

Statistical estimators and confidence bounds that are to be part of a basic analysis and assessment are defined in this module.

[3] Data Requirements

Types of data and the data fields are defined in this module.

[4] Corrective and Preventive Action Requirements

This module defines the types of analyses that are to be considered to forecast the effects of any corrective or preventive action that is recommended in the analysis and assessment.

[5] Root Cause Analysis Requirements

This module discusses the process for determining the root cause of a failure.

[6] Report Content Requirements

This module discusses the content of the sections that should be part of the final report. It also states a basic set of objectives of an analysis and assessment of the Shuttle hardware. The report should be a complete record of the analysis and assessment. In particular, there should be enough data and analysis steps documented so that it would be possible to reproduce the analysis results given just the report.

MODULE 1

RELIABILITY AND MAINTENANCE ANALYSIS AND ASSESSMENT PROCESS REQUIREMENTS

This module discusses categories of a basic analyses that should be considered when addressing the reliability and maintenance aspects of a system. The statistical methods that should be applied are discussed in Module 2. Five categories which should be considered for a basic analysis and assessment are mission reliability, hardware reliability, repair or replacement time, operational cost risk, and operational schedule risk.

Mission Reliability

Mission reliability deals with the failure of a function, or the reduction of its reliability, that would jeopardize the completion of the mission. For example, the failure of a gyro unit might require the termination of a mission due to fact that the reliability of the guidance and navigation function has decreased to a point where it no longer meets stated flight rules. When assessing mission reliability it is therefore important that the probability of failure of a piece of hardware be related to the probability that the mission will succeed. In addition if there are safety concerns over the failure of a piece of hardware, then they should be assessed or referred to a separate study which may require the analysis of the systems or functions being affected.

The method used to estimate the failure probability of a piece of hardware may be the same as the method used to estimate the failure probability (or reliability) in the Hardware Reliability section but the definition of a failure may not be the same for mission reliability. In particular it should depend on the failure modes related to mission reliability.

Hardware Reliability

In general hardware reliability applies to LRU (Line Replacement Unit) reliability; but, it can also apply to a system of LRU's. Failure of an LRU should be treated, whenever possible, as a failure process. That process can be a repair or a renewal process and can involve censored data. Where applicable, wearout failure and reliability growth models should be considered. System reliability estimates should be primarily based on the reliability estimates for the LRU elements, but for comparative purposes, the system can also be treated as one piece of hardware and reliability estimates made accordingly. All probability estimates should be given with confidence intervals.

Table M1-I shows types of analyses that should be considered when estimating hardware reliability.

Table M1- I
Hardware Reliability Analysis and assessment

Type of Analysis and assessment	When it Should be Considered
Reliability growth	A piece of hardware has gone through a sequence of design changes.
Wearout Failure	Any hardware that contains mechanical parts or materials that are subject to wearout.
Random Failure	When there is no evidence of wearout or when time-to-failure is not given, random failure analysis and assessment can be considered.
Repairable systems	Failure times that are related to a sequence of failure events in which the hardware is repaired (not renewed) following each failure.
Renewable systems	When a hardware element is replaced with a new element upon failure.

Maintenance

There are two basic types of maintenance. One is *corrective maintenance* and the other is *preventive maintenance*. Corrective maintenance is concerned with the amount of time spent in repairing or renewing a piece of hardware over a given period of time. Preventive maintenance is concerned with the amount of time that is devoted to repairing any damage to a piece of hardware prior to the occurrence of a failure mode or to the amount of time spent in inspecting and other activities (such as applying lubricants) that are of a preventive nature.

Module 2 discusses some statistical methods that can be applied to estimate the expected amount of time that would be spent on maintenance.

Operational Schedule Risk Requirements

For failures that do not cause the loss of the Shuttle, the operations schedule is determined by the critical path in the network of activities that make up the length of time it takes to turn around the Shuttle. This implies that any delay that could result from a failure needs to be determined relative to an operational schedule of the Shuttle. Short of determining the expected delay (schedule risk) in the operational schedule, one can estimate the expected time and the maximal time it would take to restore a failed unit. These estimates can provide needed data for the Shuttle schedule.

MODULE 2

RELIABILITY AND MAINTENANCE STATISTICAL METHODS REQUIREMENTS

The purpose of this module is to define a set of statistical methods that are representative of a basic set of requirements for an R&M analysis and assessment. This module supplements Module 1. Module 1 primarily defines the analysis and assessment process that is to be used in a basic R&M analysis and assessment.

Since the hardware reliability methods portion contains a large number of equations and specific related information, it is encapsulated in a table. This table also refers to three appendices which are meant to document methods that have been used in previous analyses and which have a possible wide application (Appendix I and II) or they document methods which have application and are not easily found in the literature (Appendix III). They are not complete. For example, in Appendix I and III discuss point estimation methods but do not elaborate on methods for estimating confidence intervals.

The sections on maintenance, cost risk, and schedule risk are brief and merely represent a very basic set of methods that can be done.

Hardware Reliability Methods

TableM2- I shows the preferred methods for estimating hardware reliability and confidence. This table complements Table II in Module 1.

TableM2- I
Hardware Reliability Analysis and Assessment Methods

Type of Analysis and Assessment	Estimator	Confidence Interval	Reference	Comment
Random Failure - time dependent	Reliability is: $R(t) = e^{-\lambda t}$ Estimator of λ is: $\hat{\lambda} = \frac{n}{T}$ where n is the number of failures and T is the total time (sum of times to failure plus sum of censored times). Estimator of the reliability is obtained by inserting the estimator of λ for λ.	1- α confidence interval on λ is: $\frac{\hat{\lambda}\chi^2_{2n,1-\frac{\alpha}{2}}}{2n} < \lambda < \frac{\hat{\lambda}\chi^2_{2n,\frac{\alpha}{2}}}{2n}$ The confidence interval on the reliability, over time period t, is obtained by first multiplying this inequality by -t and then exponentiating it.	[1] pages 37-38	This confidence interval is an approximation for type I and for variable censoring cases. Most of the time variable censoring will prevail.
Type of	**Estimator**	**Confidence Interval**	**Reference**	**Comment**

Analysis and Assessment				
Random failure - single event	Reliability is 1-p where p is the probability of failure. Estimator of p is x/n where x is the number of failures and n is the number of attempts.	Exact confidence intervals can be found in tables for the binomial. For large n and a small number of failures use Poisson tables.	Exact confidence interval tables can be found in [2] pages 219- 237. Confidence intervals using the Poisson can be found in [3].	This case assumes that there has been at least one failure. If there are no failures then the next formula should be used.
Single event with no failures recorded	Estimator of p is x/(x+1) where x is the number of tests with no failures. For more information see Appendix II	Lower C% confidence bound is $(1-C)^{\frac{1}{x}}$		Details given in Appendix II.
Failures that involve a changing hazard function (wearout or reliability growth). Nonrepairable case.	Use the reliability estimation methods of the computer program SUPERSMITH WEIBULL	Use the confidence interval methods found in SUPERSMITH WEIBULL.		This applies to single failures and to a renewable process.

Type of Analysis and Assessment	Estimator	Confidence Interval	Reference	Comment
Failures that involve a changing hazard function (wearout or reliability growth). Repairable case and time truncated data.	Treat the repairable case as a Weibull process. Reliability is: $R(t) = e^{-\left(\frac{t}{\theta}\right)^{\beta}}$ The estimator for β is: $\hat{\beta} = \frac{n}{\sum_{i=1}^{n-1} \ln(t_n / t_i)}$ The estimator for θ is: $\hat{\theta} = \frac{t_n}{n^{1/\hat{\beta}}}$	Confidence interval for β : $\frac{\hat{\beta}\chi^2_{1-\alpha}}{2n} < \beta < \frac{\hat{\beta}\chi^2_{\alpha}}{2n}$ where n is the sample size. Confidence interval for θ : $\theta_L < \theta < \theta_U$ where $\theta_L = \hat{\theta}\left(n[(n+1)t_\gamma(n+1)]^{-n/(n+1)}\right)^{1/\hat{\beta}}$ $\theta_U = \hat{\theta}\left(n[(n+1)t_{1-\gamma}(n+1)]^{-n/(n+1)}\right)^{1/\hat{\beta}}$ where $t_\gamma(n) = \exp\left(\frac{\ln(n)}{\sqrt{n}}\, q_\gamma(n)\right)$	See [4] and [5].	Formulas in this section apply to a single unit that experiences multiple failures and repairs. For a repairable process in which data on several identical units is given, the formulas in Appendices I and III apply.
		where $q_\gamma(n)$ is found in Table I page 419 of reference [4]. Confidence interval for the reliability [5]: $R_L(t_o) < R(t_o) < R_U(t_o)$ where $R_L(t_o) = \exp(-t_o \nu_U)$ $R_U(t_o) = \exp(-t_o \nu_L)$ $\nu_L = [(n+.25 + z^2_{1-\alpha}/4) - (z_{1-\alpha}/2)(2n+.5 + z^2_{1-\alpha}/4)^{1/2}]^2 / ty$ $\nu_U = [(n+.25 + z^2_{1-\alpha}/4) + (z_{1-\alpha}/2)(2n+.5 + z^2_{1-\alpha}/4)^{1/2}]^2 / ty$ where t is the truncation time and where $y = n/\hat{\beta}$		

Hardware Maintenance Methods

Corrective Maintenance

For a single unit that is repaired N(t) times in a period of length t, the total repair time is

$$T = T_1 + T_2 + \ldots + T_{N(t)}$$

and so the expected time to repair that unit over t is, provided the time to repair and the number of failures are independent,

$$E(T) = MTTR\ E(N(t))$$

where E(N(t)) is the expected number of failures in time t and MTTR is the mean time to repair. When there are M units that can fail, this equation becomes, again letting T be the total time of repair,

$$E(T) = \sum_{i=1}^{M} MTTR_i E(N_i(t))$$

If the number of failures follows a Poisson process, then $E(N(t)) = \lambda t$ where λ is the failure rate. If the units are repairable and they are not renewed after each failure, then a possible model for the process {N(t), t>0} is a nonhomogeneous Poisson process. The expected number of failures is

$$E(N(t)) = \left(\frac{t}{\theta}\right)^{\beta}$$

where θ is the characteristic life and β is the shape factor. If units are renewed each time they fail, then the expected number of failures is obtained by solving the renewal equation. Letting M(t) = E(N(t)), the renewal equation is

$$M(t) = F(t) + \int_0^t F(t-s)dM(s)$$

where F(t) is the cumulative distribution of the time-to-failure. When the number of failures follow a Poisson process, the solution of this equation gives $M(t) = \lambda t$. When the hazard function changes with time, then the renewal equation is our way of finding the expected number of failures. For this basic analysis and assessment, however, we will assume that if renewal occurs, then the number of failures will be treated as a Poisson process. If a more sophisticated analysis and assessment is planned, then the renewal equation should be used. Good basic references are [6], [7], and [8].

The estimator of E(T) involves two basic parameters. One is MTTR and other is E(N(t)). If $T_1, T_2, \ldots, T_n$ are n random repair times, then the estimator for MTTR is

$$\hat{\mu} = \frac{1}{n}\sum_{i=1}^{n} T_i \quad \ldots (1)$$

The estimators for E(N(t) can be found in TableM2- 1. If the number of failures follow a Poisson process, then use the estimator $\hat{\lambda}$ for λ. If we are dealing with failures of a repairable unit, then use the Poisson process estimators for θ and β. The estimator for the expected number of failures is then

$$\hat{M}(t) = \left(\frac{t}{\hat{\theta}}\right)^{\hat{\beta}}$$

For the basic analysis and assessment we will not deal with confidence intervals on E(T). For a more sophisticated analysis and assessment we recommend using a bootstrap method to compute confidence intervals, c.f. reference [9].

Preventive Maintenance

The time for preventive maintenance can be expressed as

$$T = T_1 + T_2 + \ldots + T_n$$

This equation is the same as equation (1) except that the number of interventions (i.e., the number of preventive maintenance operations) is not random. It is simply a given number, n. The expected preventive maintenance time is therefore

$$E(T) = (MTBPM)(n)$$

where MTBPM is the mean time between preventive maintenance actions. MTBPM can be estimated by simply averaging sample times to repair.

Operational Cost Risk

Each time a unit fails and has to be repaired or replaced, a cost is incurred to the program. If $E(N(t))_i$ is the expected number of failures of the i^{th} unit and $E(C_i)$ is the expected cost for each repair or replacement for the i^{th} unit, then $E(C_i)\,E(N(t))_i$ is the total expected cost (or cost risk) for the i^{th} unit over the time period t. If there are M units that can fail, the cost for all the M units is then just the sum of the individual expected costs.

The costs, C_i, i= 1,2, ... , M can be a function of a number of other variables such as labor cost for repair, hardware cost for new parts, cost of delay while the unit is being repaired, etc.. Also, if a unit causes other units to fail, additional costs are incurred. Since each time a cost is incurred, the amount may be different, cost is treated as a random variable and we compute the expected cost. Often cost cannot be directly determined, but must be estimated from other variables. In design situations, weight and unit complexity are common variables that are used. In those cases regression expressions, often called cost estimating relationships, are used.

In a more complex cost model there may be costs that are triggered by failures of any one of a number of units. As an example if an APU fails structurally it can cause the loss of the Shuttle. For these types of analyses, however, it not expected that such complex models will be developed specifically as part of this analysis. If such a model is being used, consideration should be given to using that model or at least to provide supporting data for others that are using the model.

Schedule Risk Methods

If T is the random time it takes to restore a failed unit and if T is assumed to have a lognormal distribution, then the expected time that it takes to restore can be estimated using the estimator given by equation (1). For scheduling purposes however it is useful to know the maximum time it would take to completely restore the failed unit. We can estimate the time beyond which there is only a 5% chance that the time-to-restore would take longer than that time. Since log (T) has a normal distribution, this can be computed as follows. If

$$\Pr(T > \delta) = .05$$

then

$$\begin{aligned} .05 &= \Pr(\log(T) > \log(\delta)) \\ &= \Pr\left(\frac{\log(T) - \xi}{\sigma} > \frac{\log(\delta) - \xi}{\sigma}\right) \end{aligned}$$

where ξ = E(log(T)) and σ = Var (log(T)). Since log(T) is normally distributed, it must be that

$$\delta = \exp(\xi + 1.645\sigma)$$

To estimate δ use the usual normal estimators for ξ and σ.

Appendix I

Estimating the Reliability of HAINS Gyros – A Case Study in the Analysis of Repairable Systems in the Presence of Time Censoring

A repairable system is one that is repaired, but not renewed, and then placed back in operation. This means that only the part of the system that actually failed is repaired or replaced and any wear that has accumulated in the parts of the system that were not repaired will be there when the system is placed back in operation. The hazard function for a repairable system can be increasing or decreasing. It will be increasing if subsequent times-to-failure are dominated by the components that are wearing out and are not repaired. If on the other hand, the repaired parts turn out to be the major sources of wear, then the hazard may decrease. This latter condition is known as reliability growth.

A common situation occurs when several systems are operated with some failing and others not failing. When one system fails it is repaired and placed back in operation. As a case study in which this situation was analyzed, consider the analysis of the HAINS gyros discussed in reference [10]. There are 34 HAINS gyros. Of those 34 gyros, there have been only 5 failures in 107167 unit hours of operation. This implies that the data is highly censored. . One way to estimate model parameters in the presence of this censoring problem is to model the failure process as a nonhomogeneous Poisson counting process. This is the approach we will now consider.

For a nonhomogeneous Poisson counting process the probability of getting n failures in the time interval (t, t+δ) is:

$$\Pr(N(t+\delta) - N(t) = n) = \frac{\left(H(t+\delta) - H(t)\right)^n}{n!} \exp(-\left(H(t+\delta) - H(t)\right))$$

and the expected number of failures in that interval is $H(t+\delta) - H(t)$. In this formula H is the cumulative hazard function. For our purposes $H(t) = \left(\frac{t}{\eta}\right)^{\beta}$, where β is the shape factor and η is the characteristic life.

If all the 34 gyros run for the same amount of time, we could set up the following regression equation to model this counting process at m sample points in time. Thus for i = 1,2, ... , m,

$$N(t_i) = 34\left(\frac{t_i}{\eta}\right)^{\beta} + \varepsilon_i$$

where ε_i is the random error and $N(t_i)$ is the actual number of failures observed in the interval (0, t_i). Here t_m is the total operating time for all 34 gyros.

In fact the 34 gyros run for different amounts of time and so we have to adjust the above equation to account for this fact. To do this we proceed as follows. Let $t_0, t_1, \ldots, t_m$, be a partition of (0, t) and

$$N(t_m) = (N(t_m) - N(t_{m-1})) + (N(t_{m-1}) - N(t_{m-2})) + \ldots + (N(t_1) - N(t_0))$$

If the number of gyros operating at time t is G(t), and G is a monotone decreasing function, then the

expected number of failures in (0, t_m) is bounded as follows:

$$G(t_m)(H(t_m) - H(t_{m-1})) + G(t_{m-1})(H(t_{m-1}) - H(t_{m-2})) + \ldots + G(t_1)(H(t_1) - H(t_0)) > E(H(t_m) > G(t_{m-1})(H(t_m) - H(t_{m-1})) + G(t_{m-2})(H(t_{m-1}) - H(t_{m-2})) + \ldots + G(t_0)(H(t_1) - H(t_0))$$

This can be written as

$$G(t_m)H(t_m) + (G(t_{m-1}) - G(t_m))H(t_{m-1}) + \ldots + (G(t_0) - G(t_1))H(t_0) > E(N(t_m) > G(t_{m-1})H(t_m) + (G(t_{m-2}) - G(t_{m-1}))H(t_{m-1}) + \ldots + (G(t_0) - G(t_1))H(t_1)$$

Assuming that G is a continuous function and letting the partition of (0, t) become increasingly finer, it is easy to see that

$$E(N(t)) = G(t)H(t) - \int_0^t H(x)dG(x) \quad \ldots (1)$$

In our case the number of gyros operating at any given time is approximately as shown in Figure 1.

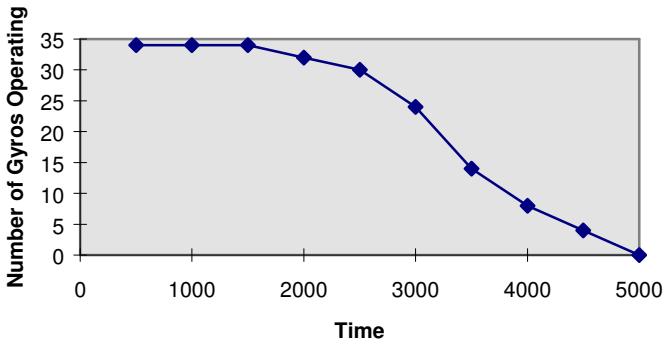
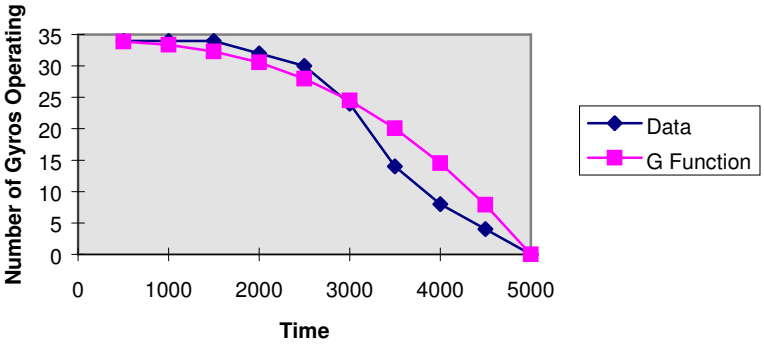


Figure 1: Straight Line Approximation of the Number of Gyros Operating at Any Given Time

The G function we will use to represent the number of gyros operating is shown in Figure 2.



and the equation is

$$G(t) = 34\left[1 - \left(\frac{t}{5000}\right)^{2.5}\right]$$

Substituting this form of G into equation (1), our nonlinear regression equation for estimating β and η becomes, for i = 1,2, ... ,m

$$N(t_i) = \frac{t_i^{\beta}}{\eta^{\beta}}\left[34 + \left(\frac{t_i}{5000}\right)^{2.5}\left(\frac{85}{\beta + 2.5} - 34\right)\right] + \varepsilon_i$$

Appendix II

ESTIMATING RELIABILITY WHEN NO PAST FAILURES HAVE BEEN OBSERVED

In this appendix methods for estimating the reliability when the only data available are records of successful tests on a unit where no failures occurred. The basic ideas are based on the use of a geometric distribution in a Bayesian setting.

Two methods are discussed. The first is a Bayesian estimation and confidence method which a-priori places no preference on the value of the reliability. This method tends to be conservative in the sense that it gives point estimates and confidence values that are lower when rationally compared to certain other estimators. The second method makes use of the Fisher [1] concept of a fiducial probability. Here a special prior probability is chosen so that a Bayesian method is made to coincide with a fiducial confidence bound. This fiducial confidence bound is attractive in the no failure setting since it is the one that is often quoted in that situation. By keeping with the Bayesian estimation method in this case, advantages related to the computation of a confidence interval for a system reliability is preserved.

Bayes Estimates

Suppose a number of tests are run in a manner such that each test is independent of the rest of the tests and the probability of success for each test is a constant value, p. The probability of having x straight success without a failure is p^x. Assume that prior to any testing, which represents the case where x = 0, the unit being tested starts in an operating state. For this case p^x can be taken as the survival function of the unit for x = 0,1,2, … . The cumulative distribution function is then $1 - p^x$. The distribution, or density function, that will give this cumulative distribution function is then the geometric distribution $f(x|p) = p^{x-1}(1-p)$ for x>0 and 0 for x=0. Indeed

$$1 - p^x = \sum_{y=1}^{x} p^{y-1}(1-p)$$

As stated above, p is the probability of success on a single trial and therefore will be taken as the reliability of the unit that is being tested. In the Bayesian setting, p as well as x are treated as random variables. These random variables will be denoted by P and X respectively and the Bayes estimate for p is E(P|X=x). In this case, then, the Bayes estimate for p is the expected value of P given that one has observed x straight successes without a failure. To compute the Bayes estimate, however, one must produce a probability distribution for P known as the prior distribution. Normally the prior distribution (density), g(p), represents the statisticians estimate of P before any data pertaining directly to P is observed. For this prior density and the likelihood, f(x|p), a probability density of p given x, called the posterior density, h(p|x), is

$$h(p \mid x) = \frac{f(x \mid p)g(p)}{\int_0^1 f(x \mid p)g(p)dp} \quad \ldots (1)$$

The Bayes estimate of P is the mean of the posterior distribution.

When data exits on units that are similar to the one for which the reliability is being estimated, then such data may provided the basis for developing a prior. If no such data exist,

and there is complete ignorance about likely values of P, then a uniform prior is often used. This option will be explored below.

There is, however, another way to look at the role of the prior. As stated above, the mean of the posterior distribution is the Bayes estimate of P, and in addition, the posterior distribution determines an uncertainty region for P. This suggests that a reasonable strategy would simply be to use the prior to shape a posterior distribution that produces estimates of P that have certain desirable properties. As mentioned in the beginning of this note, this leads to a fiducial lower confidence bound. Before this approach is discussed, however, first consider the case where a uniform prior is assumed.

The Bayes Estimate of P for a Uniform Prior

First assume that no particular preference is warranted and so the prior to be chosen distributes the probability uniformly between 0 and 1. That is g(p) = 1 for $0 \le p \le 1$ and 0 otherwise. Using equation (1), with this prior the posterior distribution of P given x, for x>0, is

$$h(p \mid x) = x(x+1)p^{x-1}(1-p) \quad \ldots (2)$$

The Bayes estimate, which is $E(P|X=x) = \int_0^1 ph(p \mid x)dp$, becomes in this case

$$E(P|X=x) = \frac{x}{x+2} \quad \ldots (3)$$

The reliability of a unit that has had x straight successful tests is therefore estimated to be (x)/(x+2).

The confidence in this estimated reliability, from the Bayesian perspective, can be computed in the following way.

$$Pr(P>y \mid X=x) = \int_y^1 h(p \mid x)dp$$

and for the posterior distribution given by equation (2) this probability is

$$Pr(P>y \mid X=x) = 1 + xy^{x+1} - (x+1)y^x$$

If this is to be equal to 1 - α, then one needs to solve the following equation for y

$$0 = \alpha + xy^{x+1} - (x+1)y^x$$

Here 1 - α is the probability that P will be larger than y, or stating this in a different way, there is only an α% chance that the reliability would be y or smaller. As an example if 1 - α is .95, then the probability is .95 that the true reliability has the value greater than y, or there is only a 5% chance that the reliability would be y or smaller. These statements are statements of confidence that are meant to convey the uncertainty in the Bayes estimate of the reliability.

Alternate estimates of the reliability of a unit can be based on the mode of the posterior probability given in equation (2). The mode of this distribution is $\frac{x-1}{x}$, where again x the number of tests where no failures have been observed. For x>2 this estimate will give a larger value for the reliability than will the estimate compute using formula (3). Similarly one could use the median of the distribution of equation (2) as an estimate of the reliability.

Bayes Estimate of P by Shaping the Posterior

Next consider the second option where the prior is selected so that the posterior distribution has certain desirable properties.

If x-1 successes occur with one failure, then a reasonable estimate of the probability of failure is $\frac{1}{x}$. Notice that the estimate of the probability of failure given the estimate of the probability of success in equation (3) is $\frac{2}{x+2}$. The estimate for 1-P, the probability of failure, when there has been one failure in x attempts should not be smaller than is the estimate of 1-P when there have been x attempts and no failures; but, when one compares $\frac{1}{x}$ with $\frac{2}{x+2}$ this is indeed the case for x > 2.

Consider a prior probability density that is a beta density of the form, for 0 < p < 1, $\alpha > 0$, and $\beta > 0$,

$$g(p) = \frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1}$$

For $\alpha = 1$, this density becomes

$$g(p) = \beta(1-p)^{\beta-1} \quad \ldots (4)$$

and as β approaches 0, this density becomes highly peaked near p =1.

The posterior probability for the prior given in equation (4) and for the likelihood probability density $f(x|p) = p^{x-1}(1-p)$ for x>0 and 0 for x=0 is

$$h(p \mid x) = \frac{\Gamma(x+\beta+1)}{\Gamma(x)\Gamma(\beta+1)} p^{x-1}(1-p)^{\beta}$$

and this leads to the following posterior probability density in the limit as β goes to 0,

$$h(p|x) = xp^{x-1} \ldots (5)$$

The average of this posterior probability, which is the Bayes estimate of P, is

$$E(p|x) = \frac{x}{x+1} \ldots (6)$$

and therefore, the estimate of 1-P is $\frac{1}{x+1}$. For all values of x, this estimates is slightly smaller than is the estimate $\frac{1}{x}$, which, recall, was the estimate when there was 1 failure among the x attempts. Thus replacing the 1 failure with a success decreases the estimate of the probability of a failure, which is reasonable.

Next consider the uncertainty related to the estimate of P. The cumulative distribution for the density of equation (5) is

$$F(p|x) = 1-p^x \ldots (7)$$

and for F(p|x) = c, (where c is similar to the standard confidence value) the solution for p is $p_0 = (1-c)^{\frac{1}{x}}$. This is a fiducial confidence bound and is the one that is often computed for the case where x successes have been observed with no failures. Wang [2] offer a nice introduction to this type of a confidence bound.

Examples

To get some feel for the two above methods for computing point estimates and uncertainties, the following example is offered.

Table 1. Example Point Estimates and Lower Uncertainty Bounds

Number of Tests With No Failures, x	5	50	100
Point Estimate of Reliability, $\frac{x}{x+2}$	.7143	.9615	.9804
Lower 95% Uncertainty Bound, p_α (Solve for p_α in $0 = .05 + x p_\alpha^{x+1} - (x+1) p_\alpha^{x}$)	.4100	.9100	.9500
Point Estimate of Reliability, $\frac{x}{x+1}$	.8333	.9804	.9901
Lower 95% Uncertainty Bound, p_α ($p_\alpha = .05^{\frac{1}{x}}$)	.5493	.9418	.9705

Concluding Remarks

Point estimates of reliability for cases where no failures have been observed in test or operational records of a unit has often been dealt with by assuming some fraction of a failure has occurred. These leads to, for example, the one third rule. Bayesian methods, on the other hand,

often handle the no failure cases with ease. Several examples exist when the reliability of the unit is a function of time. In this note the case where time is not a factor is discussed. These cases apply to situations where the operation of a unit occurs over a very short period of time so that for all practical purposes time is not a factor. Rocket launches are an example of such a case. The motivation for these methods were the flight termination events that are related to the X-38.

The general Bayes point estimate is based on the mean of the posterior distribution. This posterior distribution also provides a means for computing uncertainty bounds that can be placed on this estimate. When dealing with the reliability of a system of units, this means that the point estimate of the system can be computed from the point estimates of the individual units and the uncertainty bounds for the system can be gotten by Monte Carlo methods using the posterior distributions for these units.

The posterior distribution can also be used to compute alternative point estimates to the Bayes estimate. Two such point estimates are the median and the mode of the posterior distribution. In this note an expression for the mode was given for the uniform prior case.

The first point estimate that is given deals with the case where the prior distribution is uniformly distributed between 0 and 1. This represents the case where no a-priori emphasis is placed on any particular values of p. And, this produces a very conservative estimate of the reliability. If, however, a prior is selected that places a large emphasis on the value p = 1, then an estimate is produced which has properties that seem more reasonable when compared to non-Bayesian and fiducial methods.

References

1. Fisher, R. A., “Inverse Probability,” Proceedings of the Cambridge Philosophical Society, 1930, 26, 528 – 535

2. Yang Y. H., “Fiducial Intervals : What are They ?” , American Statistician, May 2000, 54, No. 2. 105 - 111

Appendix III

ESTIMATING PARAMETERS IN A WEIBULL PROCESS: AN EXPLANATION OF THE AMSAA MODEL

This appendix came from a note originally written by Bruce C. Reistle and Timothy D. Schick of SAIC and modified by Richard P. Heydorn.

Consider a Weibull point process {N(t), t>0} where

$$\Pr(N(t+s) - N(t) = n) = \frac{(\lambda(t+s)^{\beta} - \lambda t^{\beta})^{n}}{n!} e^{-(\lambda(t+s)^{\beta} - \lambda t^{\beta})}$$

and where N(t) is the number of events (failures of a unit) in the time interval (0,t). Estimates of the characteristic life, λ, and the shape parameter, β, will be derived using a maximum likelihood method in the presence of censoring. It is assumed that this process describes the failure times of a unit that is repaired instantaneously after each failure. The purpose of this note is to derive the estimators for these parameters for the case where we observe the responses from K identical Weibull processes. These estimators are discussed in Crow [1,2], but in those references the derivations are not given.

We begin by first considering the case for K = 1. Let $t_0 < X_1 < X_2 < \ldots < X_{N(t_1)} < t_1$ be a sequence of random failure times that occur up to a censoring time t_1. Here t_0 is the time that we start observing the process. We will assume that t_0 is the time when the unit is first placed in operation. $N(t_1)$ is a random variable and is the number of failures that have been observed prior to the censoring time t_1. Assume that we have observed n failures just prior to t_1, and, conditional on $N(t_1) = n$, let x_i be an observation on X_i for i = 1,2, … , n.

Let $z_i = \lambda x_i^{\beta}$ for i = 1,2, … ,n and let $z_i = \lambda t_i^{\beta}$ for i = 0 and n+1. Then we have the ordered observations $z_0 < z_1 < z_2 , \ldots . < z_n < z_{n+1}$. Here z_{n+1} is a censoring time. These z-variables are observations of failure times from a Poisson process with z_0 as a start time and z_{n+1} as a censoring time where the failure rate is 1. Next consider the sequence $z_1 - z_0 , z_2 - z_1 , \ldots , z_{n+1} - z_n$. Since we are dealing with a Poisson process, these differences are independent and identically distributed interarrival times. Now let $w_i = z_i - z_{i-1}$, for i = 1,2, … , n+1. Notice that w_{n+1} is a censoring point for the $n+1^{st}$ interarrival time. In matrix form **w** = **Az** where **A** is a lower triangular matrix with 1's on the diagonal. If we leave off the last row and column of **A**, the resulting submatrix applies to the transformation of the n transformed failure times with the last censored time removed. This means that the Jacobian related to the transformation of the failure times is 1. And since each w has an exponential density with rate 1, we have,

$$f_w(w_1, w_2, \ldots, w_n) = e^{-w_1} e^{-w_2} \ldots e^{-w_n}$$
$$= e^{-\sum_{i=1}^{n} w_i}$$

Since w_{n+1} is a censoring point, the likelihood function, L, for the entire set of data , w_1, w_2, … , w_{n+1}, is f_w multiplied by the reliability $e^{-w_{n+1}}$. Thus

$$L = e^{-\sum_{i=1}^{n} w_i} e^{-w_{n+1}}$$
$$= e^{-\sum_{i=1}^{n+1} w_i}$$

In terms of the z-variables, this becomes $e^{-(z_{n+1}-z_0)}$ (note that the Jacobian going back to the z-variables is also 1). The final step here is to transform back to the original failure times, x_i for i = 1,2, … ,n. The Jacobian that gets us back to these x-variables is $\lambda^n \beta^n \prod x_i^{\beta-1}$. The likelihood function is therefore of the form

$$L(\lambda, \beta) = \left(\lambda^n \beta^n \prod_{i=1}^{n} x_i^{\beta-1} \right) e^{-\lambda(t_1^{\beta} - t_0^{\beta})}$$

Taking the derivative of $\ln L(\lambda, \beta)$ first with respect to λ and then with respect to β, and equating to 0, gives the respective equations

$$0 = \frac{n}{\lambda} - (t_1^{\beta} - t_0^{\beta})$$

$$0 = \frac{n}{\beta} + \sum_{i=1}^{n} \ln x_i - \lambda(t_1^{\beta} \ln t_1 - t_0^{\beta} \ln t_0)$$

and these give the following estimators for λ and β,

$$\hat{\lambda} = \frac{n}{(t_1^{\beta} - t_0^{\beta})}$$

$$\hat{\beta} = \frac{n}{\hat{\lambda}(t_1^{\beta} \ln t_1 - t_0^{\beta} \ln t_0) - \sum_{i=1}^{n} \ln x_i}$$

When $t_0 = 0$ then these equations become

$$\hat{\lambda} = \frac{n}{t_1^{\beta}}$$

$$\hat{\beta} = \frac{n}{\sum_{i=1}^{n} \ln \frac{t_1}{x_i}}$$

Next consider the more general case when K > 1. For the k^{th} unit let $t_{0k} < X_{1k} < X_{2k} < \ldots < X_{N(t_{1k})} < t_{1k}$ be the sequence of random failure times that begin at t_{0k} and are censored at t_{1k}. Following a similar approach used for K = 1, the likelihood function for K like units (i.e., each unit has the same characteristic life and shape factor) given that $N(t_{1k}) = n_k$ is

$$L(\lambda, \beta) = \prod_{k=1}^{K} \left(\lambda^{n_k} \beta^{n_k} \prod_{i=1}^{n_k} x_{ik}^{\beta-1} \right) e^{-\lambda(t_{1k}^{\beta} - t_{0k}^{\beta})}$$

Equating the partial derivatives of $\ln(L(\lambda, \beta))$ with respect to λ and β to 0 and solving for λ and β respectively gives the following equations for the estimators of λ and β.

$$\hat{\lambda} = \frac{\sum_{k=1}^{K} n_k}{\sum_{k=1}^{K} (t_{1k}^{\hat{\beta}} - t_{0k}^{\hat{\beta}})}$$

$$\hat{\beta} = \frac{\sum_{k=1}^{K} n_k}{\hat{\lambda} \sum_{k=1}^{K} (t_{1k}^{\hat{\beta}} - t_{0k}^{\hat{\beta}}) - \sum_{k=1}^{K} \sum_{i=1}^{n_k} \ln(x_{ik})}$$

It is seen that if the expression for $\hat{\lambda}$ is first substituted into the next equation, the equation for $\hat{\beta}$ just involves $\hat{\beta}$, and using an iterative algorithm, such as Newton-Raphson, it can be solved for $\hat{\beta}$. Once this is done, the resulting answer can be substituted into the first equation to solve for $\hat{\lambda}$.

References

1. Crow, Larry H., “Reliability Analysis for Complex, Repairable Systems”, AMSAA report no. 158

2. Crow, Larry H., “Evaluating the Reliability of Repairable Systems”, RAMS, 1990, pp. 275 - 279

MODULE 3

DATA REQUIREMENTS

Table I describes the data to be collected on each hardware unit that is part of the basic R&M analysis.

Table I
R&M Data Fields

Data Category	Explanation
1. Time-to-failure	This is the time the unit has been operated (either in flight or on test) until it fails
2. Censor time	This is the time the unit has been in operation since the last failure, if any. The period of time recorded as censor time does not involve any failure event.
3. Failure description	The failure mode or modes should be described. If possible, the probable cause of the failure should be described.
4. Failure effect	The effect of the failure on the host system and dependent systems should be described.
5. Time-to-repair	The time to repair or renew the failed unit should be recorded. The time should not include in situ time, but any queue related time.
6. Repair description	If the unit has to be removed or if it is repaired in place should be recorded. Also if the unit is removed, then a record of where it was repaired should be included.
7. Description of preventive maintenance	A record of the type of preventive maintenance and the schedule at which it was done on a unit should be recorded.
8. Time spent in preventive maintenance	The time from the start to the end of preventive maintenance should be recorded.
9. Cost of a unit	This is the cost of obtaining a new unit from the vendor
10. Cost of the labor hours and materials to repair or renew a unit	This includes the cost of maintenance at KSC and at the vendor.

MODULE 4

CORRECTIVE AND PREVENTIVE ACTION REQUIREMENTS

Once the hardware reliability and maintenance impacts are determined, further study is needed to develop a corrective or preventive (CP) action plan. This plan should address what corrective or preventive action should be taken and it should predict the effects of this action. These predictions should consider the effects on safety, reliability, maintenance, cost risk, and schedule risk.

If the CP action involves the elimination or the modification of a failure mode, then the explanation of the change should include suggested modifications to the FMEA/CIL and the Hazard Analysis that apply prior to the change. Similar suggestions may be needed if a CP process action is proposed (e.g. changing the frequency of inspections, changing lubrication schedules, or flushing contaminates from a hydraulic system).

The benefits related to a given CP action should be assessed by comparing the state of the element (in terms of safety, reliability, maintenance, cost risk, and schedule risk) before and after the proposed change.

MODULE 5

ROOT CAUSE ANALYSIS REQUIREMENTS

Root cause analysis is a process of investigation in which the initiator of a sequence of events which lead to the observed failure mode is identified. One should be able to start with the failure mode that occurred and develop a list of possible causes which are consistent with all the related observed data. By having an understanding of the material properties of the unit that failed, manufacturing, assembly, or test process variables associated with the unit, the stress environment at the time of the failure, the possible contributors to the failure, and any history of this failure or related failures, one should be able to reduce this list to the event that initiated the failure. Typical environment categories that can induce stress on a unit are:

1. Vibration
2. Acoustics (Noise and Vibration)
3. Overload (Structural or Electrical)
4. Chemical Reaction
5. Pressure Differential
6. Thermal Shock
7. Ionizing Radiation
8. Micrometeoroid /Orbital debris
9. Acceleration
10. Electromagnetic Fields
11. Mechanical Shock
12. Temperature Gradients
13. Toxic Substances
14. Contaminates (e.g. particles in the hydraulic system)

Typical manufacturing process variables that can induce stress on a unit are:

1. Material substitution
2. Dimensional tolerance variance
3. Position (fit) variance
4. Test set up
5. Out-of-spec conditions (e.g. leakage, torque, resistance)

A good root cause analysis relies on a convergence of evidence that is not only consistent with the physics related to the failure, but also the history of what was done to the unit, and by whom, prior to the failure. An effort should therefore be made to collect all relevant information regarding the failure. At times this may involve talking to experts in technical areas related to failure. Questions that may have a bearing on the failure include:

1. What was the age of the unit when it failed? What information is available from the vendor on the life limit of the unit. Was there any evidence of wear prior to the failure?
2. What acceptance tests had been done on the unit? What type of failure occur prior to acceptance testing? If failures did occur, were design or operating procedure modifications made to eliminate the failure?
3. Was the unit operated within the vendor's design requirements?
4. Were there any anomalies that occurred during the operation that could have manifested into this type of a failure?
5. Were there any opportunities for the failure to be human induced? For example did the operators follow operating instructions? Could the unit have been damaged during any repair or inspection process?
6. Is there any evidence of damage to surrounding units that would have a bearing on the failure.

If the cause of a failure is difficult to determine, then the root cause analysis may become a lengthy process. It may, for example, involve additional testing or it may involve forensic analysis in a laboratory. The ultimate test to determine that the root cause of a failure was correctly determined, is to place the repaired or redesigned unit back in operation under the same environmental conditions and demonstrate that the failure will no longer occur. Unless some form of accelerated testing can be used, however, this approach may be too lengthy to be feasible. If a lengthy process is required to complete a root cause analysis , then the analysis should be deferred and not be part of the R&M analysis for which these requirements are written. For these requirements it is intended that the investigation process to determine the root cause of the failure be done with the data that exists at the time of the failure.

MODULE 6

REPORT CONTENT REQUIREMENTS

Executive Summary

The executive summary should be a concise account of the major results of the analysis. Often it is possible to convey information more clearly to the reader using a small amount of space if proper use is made of graphs and tables. Data that involves a time history of events and which, for example, displays a trend or pattern should be displayed using some type of a graph. Data that represents a number of isolated facts can often be presented most efficiently in tabular form.

Since the executive summary is intended to be read mostly by high level managers who may wish to combine the information from this analysis with other information to aid in their decision-making, there should be 1) a clear connection between the objectives of the analysis and the conclusions, 2) a standard format developed by the contractor so that other analyses which adhere to the same format can be easily compared.

Above all, the executive summary should convey the major message of the analysis and assessment in a poignant way that will allow management to easily grasp the intended message. In this respect graphics can play a major role. A good reference here is [11].

Objectives of the Analysis and Assessment

The report should state each customer requirement that is to be addressed in the analysis. These requirements should then form the objectives of the report.

The following list of requirements (as given in Section I) are considered to be the base set of customer requirements. These may not apply to each analysis, but they should be considered when developing the contents of the analysis.

General Requirements

1. Assess Shuttle hardware elements in terms of safety risk, operational cost risk, and operational schedule risk.
2. Provide supportive data and data assessments to project management required for making decisions related to appropriate corrective action to reduce safety, operational cost, and operational schedule risks.
3. Estimate the reliability of a given hardware element and provide suitable confidence bounds.
4. Compare to stated reliability goals and vendor expectations. Estimate expected repair time and confidence intervals of a given hardware element.

Safety Risk Requirements

1. For a given hardware element, assess the contribution to the safety risk of each Shuttle system function that the element supports.
2. Compare the hardware element safety risk contribution to stated goals and vendor expectations.
3. Forecast the contribution of the hardware element to the safety risk related to given mission scenarios.
4. Provide data and data assessments that will aid in the determination of the root cause of a failure. Where possible relate failures to pertinent FMEA/CIL and hazard reports.
5. Provide data and data assessments that will support forecasts of safety impacts of proposed corrective actions.

Operational Cost Risk Requirements

1. Provide data and assessments to support estimation of the Shuttle operational cost risk due to the hardware element failures.
2. Develop maintenance strategies for reducing the operational cost risk attributable to the hardware element failures.

Operational Schedule Risk Requirements

1. Estimate the contribution of hardware element failures to the critical path time distribution of the Shuttle operations schedule.
2. Develop maintenance strategies for reducing shuttle operations schedule impacts due to failures of hardware elements.

Background

This section should be devoted to the data and information that will determine the major properties of the units under study and how they function within their parent system. Flight rules (or KSC OMRSD or SPI rules if these apply) that govern how the units are to be operated should be discussed. The history of design changes that can effect the current hazard rate of the units should also be discussed. How the units are maintained which includes any special considerations that may provided added information related to the time-to-repair should be a part of this discussion.

Specific items that should be included in this section of the report include are:

1. a high level discussion of the functional purpose and operation of the unit
2. LRU part #
3. quantity of units and location of all LRUs by serial number in the fleet
4. an informal reliability diagram
5. list of the SRUs and part number
6. the cert/spec life
7. flight rules regarding the minimum number of LRUs that must operate before the flight must be terminated early
8. can the unit be repaired on the vehicle or must it be removed
9. time at which parts will become obsolete
10. and a discussion on whether or not parts are readily available.

Analysis and Assessment Methodology

This section should discuss the approach that was used to analyze the data. If the methods of modules 1 and 2 are used, these can be referenced or included as an appendix to the report. This section will depend on the topics that are addressed in the study. In general, however, the following discussion topics may be addressed.

Safety

The units under study should be related to the system or systems that they affect. If possible, the safety analysis should address the contribution of the failure of the units under study to the probability of crew or vehicle survival. This may be done through the use of a combination of constructs such as fault trees, event trees, and reliability block diagrams (c.f. Module 1). These constructs should be included in the report and may be best included in an appendix with some explanation in this section.

Hardware Reliability

It is expected that the basic methods discussed in Modules 1 and 2 will be part of the study if appropriate. There may, however, be other study topics that need to be considered. The following should be considered:

1. Trends of failures or anomalies that might indicated an increasing or decreasing problem with the units should be identified. Regression analysis, Laplace trend scoring, or other appropriate methods should be used to quantify the trend.
2. Failure predictions based on causal variables may provide a better understanding of the reliability of a unit than just a time-to-failure type of analysis. Regression, logistic regression, or proportional hazards models may apply.
3. The probability of successfully performing some scenario that is related to some mission success should be addressed if required. A typical scenario would involve the probability of successfully completing the build-flights for the International Space Station.

Maintenance

It is expected that the basic methods discussed in Modules 1 and 2 will be part of the study if appropriate. There may, however, be other study topics that need to be considered. The following should be considered:

1. In modules 1 and 2 methods are discussed for estimating failure rates. No mention is made of the definition of a failure. These methods will apply under various definitions of failure. This may include events which simply require that a unit be removed. This would lead to a estimator of the mean time between removals, for example. If anomalies are having an effect on maintenance, then the mean time between anomalies might be an appropriate quantity to estimate.
2. In module 2 the expected repair time is discussed in terms of the mean time-to-repair and the expected number of failures. The mean time-to-repair may involve a number of event times that collectively may not fit a lognormal distribution. Such events might include cannibalization of units, waiting for spares, etc.. Thus a more sophisticated model that involves other variables besides time may be required to estimate mean time-to-repair.
3. As discussed above, estimation of trends that apply to the mean repair time should be considered here as well.

Cost Risk

Cost risk is discussed in Module 1. There just the basic expression for the expected cost is discussed. As pointed out, the individual unit cost may be a function of several variables that could be modeled using a regression model (cost estimating relationship). While cost is an important variable in making management decisions, it is not expected that these studies will require the development of an elaborate cost model unless it is requested. A basic consideration to cost is, will in general, however, be a part of the study.

Schedule Risk

Modules 1 and 2 discuss schedule risk. To properly estimate this type of a risk, one should fit the effects of unit failures into the network model that is to be used for scheduling events on the Shuttle. What is discussed in Module 2 is an analysis that should provide data for such a network model. If possible, however, one should attempt to interface with such model and provide the data that is exactly required by that model.

Results

The results section should contain all the findings from the study as well as the supportive data that was used to determine these findings. The report should be reasonably well self contained so that a reader should be able to reproduce the findings from the data in the report. References to other material are acceptable if they are readily available to the reader. Consideration should be given to the following.

1. The major findings should address the objectives of the report which in turn contain the customer requirements. Other findings that become apparent during the course of the study and which have a bearing on related issues should also be discussed.
2. The findings should be prioritized according to their importance to any major decisions that should be made regarding the operation of the Shuttle. Any special alerts should be clearly discussed.
3. Where possible information should be presented in a way that best summarizes the major points to be made. Effective use of graphs, charts, and table should be stressed. When such material would make good briefing charts, a separate appendix should be provided for this material if requested.
4. In Module 2 expressions are given for the computation of confidence intervals that should accompany point estimates. This should be considered to be a minimal list. If sufficient data are available, other confidence interval computation should be considered. In some cases it may be appropriate to make uncertainty statements that do not involve confidence intervals.

Root Cause of Failures

If a root cause analysis is done as part of this R&M analysis and assessment, then this section should be a narrative of what process was followed and the findings. In this case the requirements stated in Module 5 should be used to develop the analysis approach. If, on the other hand, it is intended that a separate study should be done to complete the root cause analysis, then some indication of the process that will be followed in that analysis should be given here.

Corrective Action and its Benefits

In this section possible corrective actions and the implications of these corrective actions should be discussed. In principle any proposed corrective action should include a discussion of:

1. The benefits related to safety, hardware reliability, maintenance, cost risk, and schedule risk that would be realized if the corrective action were implemented. If there are no data available to quantify these benefits (as, for example, discussed in modules 1 and 2) then an attempt should be made to estimate these benefits from expert opinions. At the very least, there should be a discussion of the failure mode that will be eliminated or modified by the corrective action.
2. The cost of the corrective action should be estimated if the appropriate data are available. This cost should be compared with the cost risk of not doing the corrective action.
3. The schedule benefits should be estimated if the appropriate data is available.
4. A plan to test or verify that the corrective action will implement the benefits cited above should be considered if the benefits of corrective action are not clear.

Summary, Conclusions, and Recommendations

For the summary it is suggested that material (a few paragraphs) that embraces the following thoughts start off this section:

> "The first unit was flown on STS xx. There are x number of serial numbers in the fleet. Each unit consists of x LRUs and has a reliability block diagram arrangement as shown in chart x. The mission reliability, at least as computed from the binomial model, is x. The major problems with this system are x and the solutions, at least from the subsystem engineers (SSEs) vantage point, is x. If we lost this system during a mission then the impact is x and the flight rules say x. On the ground the repairability of this unit is x due to x. If I was the Upgrades Manager I would or would not do x in regards to this system because of reasons x."

The conclusions section should provide a discussion of the major findings along with a discussion of their implications. Any conclusions and recommendations should be based on facts. Opinions of the authors of the study that can not be directly substantiated should be avoided unless there is a definite need to bring a potentially dangerous situation to the forefront for possible further study.

The reader should be able to trace the major findings of the study to the customer requirements cited in the beginning of the study.

References

The reference section should cite any references that a reader would need, in additions to the contents of the report, to understand the methodology and replicate the finding of the analysis.

Supportive Data

This section should include the following.

1. The data that was used to compute and interpret the various statistics used in the report should be in tabular in a data appendix. The data fields that should be included are discussed in the Data Requirements Module.
2. The system fault trees, event sequence diagrams, reliability diagrams, and any other system descriptions or process flows should be included in an appendix if they do not conveniently fit in the main body of the report.
3. Any material that is of an explanatory nature but may be too lengthy to included in the main body of the report (e.g. long derivations) should be placed in an appendix.
4. Graphs, tables, and other material that may be used as briefing material for the analysis should be included in a separate appendix. This material may also be included in the main body of the report if its inclusion at that point makes the report more readable.

SECTION 4

GRADING CRITERIA

A grade will be assigned to each completed analysis by the responsible division. The criteria that are to be used are based on a strength and weakness type of subjective assessment of the analysis. Once the contractor specifies items that are to be covered in the analysis (c.f. the column labeled Plan in the R&M Requirements for Element matrix), each of these items will be addressed in the evaluation process. Analysis Category 1, 2, and 3 will be treated as one grading unit and Analysis Category 4 through 8 will each be treated as a grading unit. In all, there are therefore 6 grading units. The following table will be used in assigning a numerical grade.

Definition of Strength and Weakness	Designated Code*
Major Strength The contractor did more than the basic analysis and assessment and showed an innovative approach to problems.	MS
Minor Strength The contractor did the basic analysis and assessment and did what was planned.	ms
Minor Weakness The contractor addressed each planned item but sections of the analysis and assessment required rework.	mw
Major Weakness The contractor did not do what was planned and the analysis and assessment required major rework	MW

* Designated codes are to be placed in column 5 of the CONTENT OF THE R&M ANALYSIS AND ASSESSMENT matrix.

The contractor will be given the opportunity to correct minor weakness by performing the rework that is planned and a new grade will be assigned in accordance with the revised analysis. Modification for grades given to major weakness will be left up to the discretion of the responsible division. In any case the contractor will be required to complete the planned analysis unless unforeseeable circumstances occurred in the course of the analysis that would prevent the contractor from completing the required work.

Strengths and weaknesses will be accompanied by a narrative that specifically defines the nature of the strength or weakness.

No attempt will be made to arrive at a total numerical grade. Other evaluations of the contractor (such as conducted in the Technical Management Review) can make use of the strength and weakness descriptions assessed in a given analysis and assessment.

A Technical Monitor (TM) will be assigned to each R&M analysis and assessment. It will be the responsibility of the TM to develop the strength and weakness as defined in this section.

REFERENCES

1. Cox, D.R. and Oakes, D., “Analysis of Survival Data”, Chapman & Hall, 1984

2. Beyer, William H., “Handbook of Tables for Probability and Statistics”, second edition, CRC Press, 1988

3. Ricker, William E., “The concept of Confidence or Fiducial Limits Applied to the Poisson Frequency Distribution”, JASA, Volume 32, pp. 349-356

4. Bain, Lee J., Englehardt, Max, “ Statistical Analysis of Reliability and Life-Testing Models”, second edition, Marcel Dekker, Inc., New York, 1991

5. Bain, Lee J., Englehardt, Max, “Inferences on the Parameters and Current System Reliability for a Time Truncated Weibull Process”, Technometrics, vol. 22, No. 3, August 1980, pp 421-426

6. Barlow, R.E., Proschan, F., “Statistical Theory of Reliability and Life Testing: Probability Models”, Holt, Rinehart and Winston, New York, 1975

7. Zacks, S., “Introduction to Reliability Analysis: Probability Models and Statistical Methods”, Springer-Verlag, 1992

8. Leemis, L.M., “Reliability: Probabilistic Models and Statistical Methods”, Prentice-Hall, 1995

9. Meeker, W.Q., Escobar, L.A., “Statistical Methods for Reliability Data”, John Wiley & Sons, 1998

10. High Accuracy Inertial Navigation System (HAINS) Reliability & Maintenance Analysis and Assessment, NASA Johnson Space Center Space Shuttle Development Office (MA), SSMA-98-009, April 9, 1999

11. Tufte, Edward R., “Visual Explanations Images and Quantities, Evidence and Narrative”, Graphics Press, May 1997