

P176819

No. 001

Part 1
R DOCV

Square
/ Gray



AGARD-LS-47-71

AGARD-LS-47-71

AGARD

ADVISORY GROUP FOR AEROSPACE RESEARCH & DEVELOPMENT

7 RUE ANCELLE 92 NEUILLY-SUR-SEINE FRANCE

LECTURE SERIES No. 47

on

Reliability of Avionics Systems

NORTH ATLANTIC TREATY ORGANIZATION



DISTRIBUTION AND AVAILABILITY
ON BACK COVER

~~046020~~
046027 DP

UNLIMITED

4

AGARD Lecture Series No. 47/71

2

NORTH ATLANTIC TREATY ORGANIZATION
ADVISORY GROUP FOR AEROSPACE RESEARCH AND DEVELOPMENT
(ORGANISATION DU TRAITE DE L'ATLANTIQUE NORD)

RELIABILITY OF AVIONICS SYSTEMS

7

This material has been assembled to support a Lecture Series under the sponsorship of the Avionics Panel and the Consultant and Exchange Programme of AGARD, presented in Rome 16–17 September 1971, and London 20–21 September 1971.

THE MISSION OF AGARD

The mission of AGARD is to bring together the leading personalities of the NATO nations in the fields of science and technology relating to aerospace for the following purposes:

- Recommending effective ways for the member nations to use their research and development capabilities for the common benefit of the NATO community;
- Providing scientific and technical advice and assistance to the North Atlantic Military Committee in the field of aerospace research and development;
- Continuously stimulating advances in the aerospace sciences relevant to strengthening the common defence posture;
- Improving the co-operation among member nations in aerospace research and development;
- Exchanging of scientific and technical information;
- Providing assistance to member nations for the purpose of increasing their scientific and technical potential;
- Rendering scientific and technical assistance, as requested, to other NATO bodies and to member nations in connection with research and development problems in the aerospace field.

The highest authority within AGARD is the National Delegates Board consisting of officially appointed senior representatives from each Member Nation. The mission of AGARD is carried out through the Panels which are composed of experts appointed by the National Delegates, the Consultant and Exchange Program and the Aerospace Applications Studies Program. The results of AGARD work are reported to the Member Nations and the NATO Authorities through the AGARD series of publications of which this is one.

Participation in AGARD activities is by invitation only and is normally limited to citizens of the NATO nations.

The material in this publication has been reproduced directly from copy supplied by AGARD or the author.

Published July 1971

658.562:629.7:621.38



*Printed by Technical Editing and Reproduction Ltd
Harford House, 7-9 Charlotte St, London. W1P 1HD*

FOREWORD

This Lecture Series is sponsored by the Avionics Panel and the Consultant and Exchange Programme.

Most modern systems are now dependent on proper performance of a rather complex complement of Avionics equipment. Without the proper sequencing of a series of successes, these systems will not survive.

World technology has demonstrated time and again in these systems, as nature has proven with the human machine, that survivability related to reliability can also be predicted, estimated, monitored, tested and controlled.

This Seminar examines many historically proven techniques for assuring adequate levels of product reliability. We will examine the concepts, and theorems and their practical application and results in an attempt to pass on the lessons learned, fostering technology growth through information exchange and a better understanding of the effects on survivability of man-made machines in their natural environment.

A round table discussion with the participation of all the speakers will conclude the Lecture Series.

SPEAKERS

Mr E.Keonjian
Lecture Series Director
Section Chief
Grumman Aerospace Corporation
Bethpage, New York 11714
USA

Mr B.E.Baker, M.A.
Command Chief Research Officer
HQ Strike Command
RAF High Wycombe, Bucks.
England

M.l'Ingénieur en Chef Blanquart
Chef du Département Q.F.C.
C.N.E.T.
Route de Trégastel
22 – Lannion
France

Mr J.J.Bussolini, Jr
Director of Engineering Operations
Grumman Aerospace Corporation
Bethpage, New York 11714
USA

Mr W.T.Sumerlin
Manager, Engineering Reliability
McDonnell Aircraft Corporation
Dept 150, Bldg.33
St. Louis, Missouri 63166
USA

Mr M.M.Tall
Manager, Product Assurance/RCA
RCA, Building 108-102,
Moorestown, New Jersey 08057
USA

Dipl.-Ing. G.Vollhardt
Siemens A.G.
N. ZL Lab. 557
8 München
Hofmannstrasse 51
Germany

CONTENTS :-

~~FOREWORD~~

Page

iii

~~SPEAKERS~~

iv

~~INTRODUCTORY PAPER~~

by E.Keonjian

vii

Reference

SESSION I - FACTORS AFFECTING RELIABILITY OF AVIONICS SYSTEMS

also TECHNIQUES OF SYSTEM RELIABILITY ESTIMATION, INCLUDING
 FAILURE EFFECT ANALYSIS (FAILURE CONSEQUENCE)

by W.T.Sumerlin

1

CORRELATION BETWEEN ESTIMATION TESTS AND SYSTEM OPERATING DATA

by M.M.Tall

2

EFFECTIVENESS OF RELIABILITY PROGRAM ELEMENTS

by W.T.Sumerlin

3

SESSION II - CRITERIA FOR DESIGN OF HIGH RELIABILITY AVIONICS SYSTEMS

COST EFFECTIVENESS OF BUILT-IN TEST PROVISIONS

by M.M.Tall

4

HIGH RELIABILITY DESIGN TECHNIQUES APPLIED TO THE LUNAR MODULE

by J.Bussolini

5

TESTING THE RELIABILITY OF AVIONICS EQUIPMENT FOR SPACECRAFT
 APPLICATION

by G.Vollhardt

6

METHODS OF SPECIFYING AND CONTROLLING DESIGN RELIABILITY

by J.Bussolini

7

SESSION III - APPLIED RELIABILITY TESTING AND COSTS

RELATIONSHIPS BETWEEN PROGRAM TEST AND USER SUPPORT COSTS

by M.M.Tall

8

SYSTEM OPERATIONAL CONSIDERATIONS AND THEIR RELATIONSHIP TO THE
 TEST PROCESS

by W.T.Sumerlin

9

LA TECHNIQUE DES ESSAIS ACCELERES

par P.Blanquart

10

THE BENEFITS OF A TOTALLY INTEGRATED RELIABILITY TEST PROGRAM

by J.Bussolini

11

SESSION IV - USER RELIABILITY CONSIDERATIONS

and OPERATIONAL CONSIDERATIONS AND SYSTEMS RELIABILITY

by B.E.Baker

12

RELIABILITY AND SURVIVABILITY

by

Edward Keonjian
Grumman Aerospace Corporation
Bethpage, New York, U.S.A.
Director of the Lecture Series

INTRODUCTORY COMMENTS

The flight of Apollo XIII never reached the Lunar surface precluding the planned scientific experimentation to be completed as scheduled. To many, this fact classified the mission as a failure. The tensions around the world that accompanied the return trip to earth in a crippled spaceship had a tendency to overshadow many of real successes of the mission. In retrospect, we can look back on the Apollo XIII journey and realize that it highlighted some previously untested theories that there is a one-to-one correlation between Reliability, Survivability and the Human Machine. Every dollar invested in reliability in this vehicle had paid dividends in terms of human survivability and perhaps the results shed a new light on the importance of total reliability in the design process.

The persistence of modern technology was demonstrated by the Apollo XIV flight. After scientists and engineers painstakingly evaluated flight data from the ill-fated Apollo XIII flight, necessary changes were incorporated and the Lunar exploration program proceeded as planned. That flight, as so many situations before it, proved the value of a carefully integrated man-machine system.

The need for man as an integral element in aerospace systems seems likely for the next decade. His role and the proper integration of man and machine for maximum system effectiveness will, however, require periodic re-examination of his survivability in the environment which is not his natural habitat.

Man's total ability to survive is dependent upon a long series of successful events, many in series, many in parallel, some man-made, some natural. The body itself is perhaps the most complex natural machine known to modern technology and its ability to function can be predicted, estimated, monitored, tested, fixed and to a large extent controlled in its natural environment.

In the rather short history of aerospace technology, which perhaps began with the first flight of the Kitty Hawk in 1903, world scientists have taken gigantic strides forward in the development of design innovations that have extended man's ability not only to survive in known environments but to explore and further his knowledge of the unknowns of the universe. Even today as we watch the growth of space technology leading to the development of orbiting laboratories and transportation systems to carry men and supplies to these space stations, we have unmanned probes searching the mysteries of Mars and other planets.

Satellite systems have been in operation for several years, providing world-wide links that have improved international communications, broadened man's knowledge of the science of astronomy, and are even today providing valuable data for weather forecasting and ecological studies that will aid in the survivability of man on earth.

Our ability to develop systems that can shield man from hostile environments is still further demonstrated by vehicles that permit extended exploration deep beneath the ocean's surface, aircraft that can comfortably transport passengers at supersonic speeds, and surface transportation systems that provide significant improvement in passenger safety.

Although reliability as a specific engineering technology has seen a rather sudden surge to prominence over the last 20 years, its popularity was certainly forced by the desire to improve what existed and the knowledge that the complex systems of the future world advance the state-of-the-art at an unpredictable pace.

Most of today's modern systems are dependent on proper performance of a rather complex complement of electronics equipment. Without the proper sequencing of a series of successes, these systems will not survive. World technology has demonstrated time and again in these systems, as nature has proven with the human machine, that survivability related to reliability can also be predicted, estimated, monitored, tested, and controlled.

We should look at today as the first day of the future. Although much of the hardware that will become operational over the next 50 years is perhaps beyond our ability to thoroughly comprehend now, we can be sure that it will be the result of all that we have learned in the past. The effectiveness of future systems will illustrate how well we applied our lessons learned to the continued growth of design integrity.

This Seminar examines many historically proven techniques for assuring adequate levels of product reliability. We will examine the concepts, and theorems and their practical application and results in an attempt to pass on the lessons learned, fostering technology growth through information exchange and a better understanding of the effects on survivability of man-made machines in their natural and unnatural environments.

TECHNIQUES OF SYSTEM RELIABILITY ESTIMATION, INCLUDING FAILURE EFFECT ANALYSIS (FAILURE CONSEQUENCE)

W. T. SUMERLIN
 Manager, Engineering Reliability
 McDonnell Aircraft Company
 P.O. Box 516
 St. Louis, Missouri 63166, U.S.A.

SUMMARY

The "system reliability estimation" process begins with complete establishment and understanding of the system reliability requirement and the importance of its attainment. Probability of attainment is then studied by selective reliability allocation among subsystems, followed by feasibility estimates based on experience, complexity, failure rate summations and/or other effective techniques. Constraints including allowable degradation, alternative mode operation, environment, operator effectiveness, and excellence of maintenance will permit improved estimates. Failure mode and effect analyses can serve to guide conceptual design decisions so as to eliminate single point failures and identify areas for judicious application of redundancy, requirements for high reliability parts, special environmental control, and beneficial choice of operating profile. This then leads to recognition of any need for special design decisions, worst case design analysis, circuit standardization, preferential environmental control, close manufacturing control and/or exploration testing. Careful failure observation and study once hardware comes into existence can become an early precursor of the reliability to be attained. Then measurement of local environments, operating levels and other stresses, will permit greatly improved estimates. Once reasonably representative hardware exists, burn-in procedures and operational shakedown permit verification of the validity of parts failure rates and considerable insight to reliability growth and ultimate reliability.

INTRODUCTION

There is a not-insignificant number in the engineering profession whose encounters with reliability have left a bad flavor for statistical practices. Perhaps to them any attempt to forecast the probability of system success or failure is a numbers game not to be trusted. All such experiences and opinions notwithstanding, numerical estimation of avionic system reliability is one of the basic tools of a reliability program. It provides useful quantitative expectation of the reliability of the avionic system and its individual subelements. These numerical quantities are largely based on a process of mathematical synthesis of failure probabilities from the system subelements, usually starting from the part level and continuing up to the system level. Assumptions are heavily utilized in adapting generic failure-rate data to a specific avionic system with a particular mission. As a result, such a process in the hands of an experienced engineer usually can provide a useful estimate of the reliability of system elements, albeit broad.

The reliability estimation process can be as simple as making a wager which is entirely based on experience, judgment, and intuition. Conversely, it can be an exceedingly complicated engineering process comprising extensive effort readily justified because of the dependence of safety and financial risk on the outcome. Obviously its value depends on the experience and capability of its practitioner. To place a review of present day estimation techniques in suitable perspective, it will be beneficial to examine the circumstances which lead to a need for avionic reliability estimation, and also to review the expected consequences which may follow and relate to the success or failure of the estimate. Importantly it must be noted that most estimating processes are reiterative, going through many updating cycles from the time of earliest program concept until a final design is frozen and proven. The first step in our assignment, therefore, is the gaining of a quite thorough understanding of the avionic system reliability requirement.

UNDERSTANDING THE RELIABILITY REQUIREMENT

Frequently the reliability requirement for an avionic system comes into being as an outgrowth of the overall reliability requirement for the aerospace vehicle which will carry the avionic system. With this heredity, it shares the overall unreliability with all the other elements that make up the overall vehicle system. Study of the other system elements may give some indication of flexibility, means for adjustment, in the avionic requirement. It is possible that undue optimism surrounds the unreliability apportioned to the non-avionic elements, and as development proceeds, it will become necessary to strive for higher avionic reliability than the initial requirement if the ultimate overall system is to have a satisfactory market. On the other hand, it may be found that far more than justified conservatism has been associated with the non-avionics, putting an unfair burden on avionic development. The best approach for judging the fairness or appropriateness of the avionic requirement is to compare the expected avionic reliability with known and achieved state-of-the-art. To do this requires some sort of reliability estimation, and because a quick judgment may be essential before an avionic requirement becomes too permanent, there is need for a family of estimating techniques such that the best possible estimate can be obtained within the time available, even if the time available is extremely short.

Even if an avionic reliability requirement is judged within the state-of-the-art, it is usually desirable to do a trade study which compares the expected total reliability program cost with the benefits to be gained from having higher than essential reliability. As reliability requirements approach the state-of-the-art, the cost in labor, delay in schedule, and other factors are apt to increase nonlinearly. Frequently a reliability requirement well within the state-of-the-art turns out to be unexpectedly very difficult to meet, and by the time this becomes known, it is no longer possible to reapportion part of the burden to non-avionic system elements.

When apportioning reliability requirements among avionic subsystem elements or equipments such that the overall avionic reliability meets an overall requirement, it is sometimes desirable to classify the performance of each of the several avionic units with respect to their effect on overall performance. Some avionic failures will be catastrophic, some only critical, some of marginal importance. Some failures cause a safety abort wherein the preservation of life and limb is jeopardized. Other failures while not affecting

safety will cause a mission abort. Ideally, failures would only slowly precipitate graceful degradation, wherein performance would slowly diminish with successive failures, but many failures would take place before all performance is lost. A review of these failure factors very early in the program while it is still possible to readjust reliability apportionments between or among subsystems and equipments will yield much more than later when re-apportionment becomes much more difficult. The final result of this effort must yield a specific reliability requirement for each separately qualified subsystem element or equipment, for each separately procured avionic item if quantitative reliability is to be a procurement requirement. Experience of the past decade in the U.S.A. has rather adequately demonstrated that a desired quantitative reliability will not be regularly achieved in avionic procurement unless there is a quantitative reliability requirement imposed by specification together with sound means for verification, or, in the case of consumer goods, unless there is close competition and the purchasing public comparison shops for reliability.

Since some adequate verifying means are essential to procure desired quantitative reliability, the specification of the reliability requirement should identify the means for verification and then match the reliability requirement to the verifying means. To clarify this point, if a mission reliability is desired, and the means for verification will be to fly a sufficient number of missions with failures logged to establish with adequate confidence that the mission reliability has been adequately demonstrated, then the quantitative reliability requirement should be spelled out as a probability of mission success with a closely defined mission. On the other hand, if a reliability demonstration test is to be run in an environmental chamber with simulated (or cycled) environment, and the observed number of failures are to be the criterion of test success, then the reliability requirement should be specified as a mean-time-between-failures and the quantitative value should be chosen taking into account the relative severity between the test environment and the ultimate use condition. Many standardized reliability demonstration tests have been run in the last few years where, for the sake of test standardization (which permits comparisons with other test findings), the test environment is chosen to be equal to or even slightly greater than the most severe use conditions. When this happens, the demonstrable reliability during test is somewhat lower than the reliability demonstrated in actual field use.

The foregoing discussion should lead to an intelligent choice or a least a thorough and intelligent understanding of the quantitative reliability number imposed on an avionic item as a requirement. But this is not quite all of the consideration. Not only must the complete environment and its severity under which the required reliability must be obtainable be carefully defined, but the avionic item under consideration must be thoroughly defined. It must be possible to mathematically model the avionics so completely that the reliability or failure rate of the lowest level item of interest in the avionics can be related systemwise to the overall avionics. Design drawings to the extent they have been developed will suffice, but as the total design evolves, it may be necessary to re-review reliability requirements and apportionments. Furthermore, desired avionic operation must be carefully defined, because it is from lack of performance that decisions on failure occurrence are possible. One more item. Since the way in which the avionics will be operated may have a large effect on how many failures occur, it is necessary to define or describe such things as operating cycle; continuous or intermittent, or stand-by operation; relationship between operating time in flight and operating time on the ground. Then because the presence of redundancy at any level within the avionics will affect the way failures relate to performance degradation, a decision must be made as to whether all failures will be identified and counted during reliability demonstration, or only those failures which produce an avionic loss of performance. The former approach greatly simplifies testing and the administration of reliability demonstration, and is more frequently used, but its anticipated use should be known from the beginning of the requirement.

A last consideration relating to reliability requirements is an assessment of the challenge. Requirement relationship to state-of-the-art for avionic development has already been mentioned. Austerity of reliability funding can make an excursion beyond the present state-of-the-art a little more horrifying. When this is all coupled with schedule compression, and/or concurrent production before development is complete, the picture becomes worse yet. Such a combination of adverse situations will put great emphasis on reliability monitoring and many efforts to accelerate reliability growth.

PROBABILITY OF RELIABILITY REQUIREMENT ATTAINMENT

To determine the probability of reliability requirement attainment, it is necessary to make an estimate. Understandably we can make every consideration extremely optimistic during the estimating process, and the resulting estimate will have low probability of being correct. On the other hand we can use only pessimistic considerations, and again achieve an estimate with low probability of being correct, although it will likely be far different from the optimistic estimate. Depending on how we choose between optimism and pessimism during the estimating process, we can have a continuous spectrum of estimates with low value at either extreme, and some estimate in between which will be exactly correct although we may not be able to precisely identify which figure this is. Now if by chance the reliability requirement also falls exactly on this correct estimate, no further worry would be justified. However, at best we can only judge how far the reliability requirement seems to be above or below the figure which we feel represents our most likely estimate. If above, we must decide how much additional effort to put into development to make the attained reliability reach the requirement. Obviously, if the requirement is below our most likely estimate we need only make sure the requirement is attained.

Estimating techniques might be divided into three categories: gross estimating, rapid estimating, and detailed estimating. During the conceptual and early definition stage of avionic development, and especially when initially attempting to determine the probability of reliability requirement attainment, the assumptions and judgments already involved tend to prevent justification of any more effort at estimating beyond that required for a gross estimate. Such estimating usually employs one of these three techniques, or perhaps all three: estimating on the basis of similarity to other avionic equipment with known reliability; estimating on the basis of avionic complexity similar to other avionic equipment with known reliability; estimating on the basis of similar avionic functions, where known reliabilities for each of the common functions can reasonably be expected. The effort involved with any of these gross techniques is of the order of one or at most several man-days. The accuracy to be expected is perhaps an order of magnitude or even better. But such a gross estimate provides a basis for apportioning reliability amongst the several avionic subsystems in a practical way.

Frequently in the past the reliability requirement for an avionic system has been apportioned among its subsystems without regard to any estimate of the expected subsystem reliability. Because of the infrequency of an allocation on this basis being anywhere near the expected reliability, this technique sometimes has promulgated a feeling that those who assign reliability requirements do not understand the problem. In defense it is often stated that allocation was made on the basis that each subsystem was assumed equally critical and all are connected in series. Sometimes this method is refined by weighting subsystems in accordance with identified and varied criticalities, and sometimes relative subsystem weights are based on complexity. The point to be made here is that gross reliability estimating can be performed both easily and in the absence of detailed avionic data, it will avoid unsound allocations, and accordingly should be considered when allocating avionic reliability among subsystems even at the earliest point in the development program. Sound reliability allocations provide a guide for the development of reliability design goals, and provide subsystem reliability requirements for procurement specifications when subsystems are to be separately procured. These allocations provide valuable inputs for reliability feasibility analyses, preliminary reliability modeling, cost effectiveness studies, and any of many design trade analyses performed early in system development. But again, allocations are only valuable if the final allocated values are achievable, and an estimate is our greatest insight to this.

Gross estimating by similar equipment usually consists of the following steps. The new avionic unit is identified by general type, operational use, and other principal characteristics. Then an existing avionic unit that most nearly compares with the new equipment is identified. Next, experience data, field reports, and other information related to the probable reliability of the similar equipment is obtained and analyzed to provide an indication of the demonstrated reliability. Finally, differences between the new and the similar units are considered, and the probable reliability of the similar item is adjusted to reflect the probable reliability of the new development.

Gross estimating by similar complexity technique has been practiced for many years. A very common approach involves counting the expected number of active circuit elements (electron tube, transistor, or integrated circuit transistor equivalent) and comparing the total for the use environment (airborne) with compiled tables or graphs such as may be found in MIL-STD-756¹ or various reliability handbooks² which, in turn, then give expected failure rate.

Estimating by function is based on recently developed formulae which permit calculation of an estimated failure rate for a unit with an identifiable function, such as a radar display or a communications transmitter, in terms of key parameters (maximum pulse width for the display, power gain for the transmitter). In the near future, sufficient information may become available to permit this method to supplant gross estimating by similar equipment, and give much better estimates too.

Because estimating by parts count, and estimating by parts failure rate prediction (stress analysis) if done hastily can be performed (if grossly) in not much longer time than the aforementioned gross estimating techniques, they should be mentioned here even though they fall into the rapid estimating category usually used later than the concept phase (such as the acquisition phase). But then estimating the probability of reliability requirement attainment, will want to be repeated frequently throughout the development program, and the first time or two may not require much estimate improvement (at least in estimating technique).

Parts count estimating involves multiplying the average part failure rate for the kind of avionic item considered, when used in the expected environment, by the total number of parts expected to be needed in the completed avionic development. As the state-of-the-art improves, lower and lower average part failure rates are being achieved. The effort of making a reasonably good estimate of the number of parts expected to be needed may either require considerable effort or be quite approximate when performed very early in development. Yet this method of arriving at quantitative values for use in adjusting allocations may be well justified over gross methods. See Figure 1.

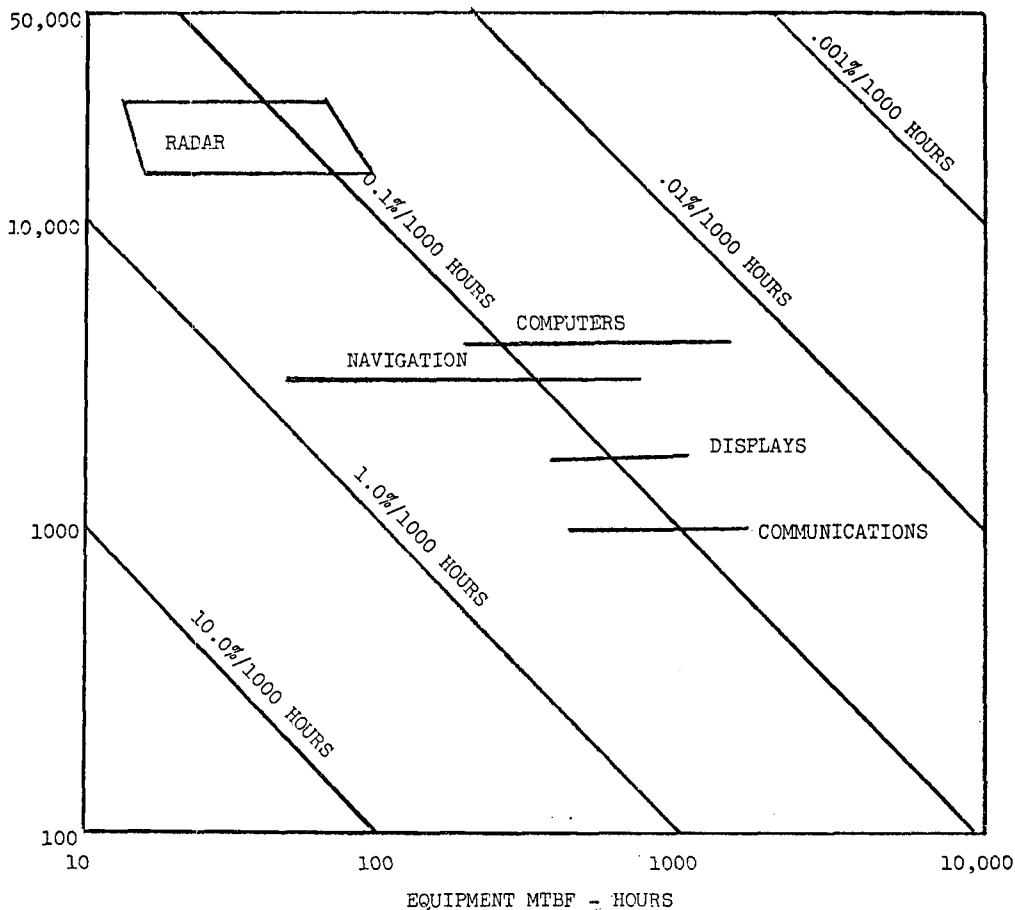
Estimating by parts failure rate prediction until quite recently involved no more than a knowledge of the part type, quantity, derating, and thermal environment. In the absence of accurate information on some of these parameters, a skilled practitioner could guess with considerable accuracy, with the result that such an estimating technique could be applied just about as fast as a gross technique with equal or better results. Today the failure rate of a majority of those avionic parts typically used can be estimated from a mathematical formula derived from a model specifically chosen for the part in question, and considerably more accuracy rewards the considerably more effort required for such estimating.²

When estimating in order to validate reliability allocations, estimating accuracy and estimating errors probably are not overly important, at least relatively. If estimating is performed as part of a bid competition for avionic development, and such is often the case, with no more detailed knowledge of the ultimate product than exists during early concept, then high accuracy in estimating is rewarding. An estimate which presents a figure considered very optimistic will not be believed, or if in error and chosen, it will become a requirement impossible to achieve and may result in costly penalties. An estimate overly conservative, or in error on the conservative side, probably will not compete well enough to acquire the business. It has been found that the past decade or so of experiences has made it possible for at least a few firms to do estimating that provides mean times between failures for as yet undeveloped products that are later borne out within twenty percent. Many companies presently achieve within fifty percent. And those with even rudimentary knowledge have little justification for error by more than three to one. But then there are ways to improve an estimate.

IMPROVING THE RELIABILITY ESTIMATE

The accuracy or validity of a reliability estimate will depend on how well the estimator can choose reliability quantities (e.g. piece part failure rates) that represent the avionic unit and its constituents for which the estimate is desired. An improved estimate can be achieved by a more appropriate or careful selection of failure rates, or conversely by an avionic design which more adequately employs those design considerations which yield the high reliability demanded by the estimating technique chosen. Early in development a knowledge of the details needed for a more accurate selection of piece part failure rates will not be available, and each best guess will only by accident fit later circumstance. As a consequence, high

FIGURE 1
 AVIONIC AVERAGE PART FAILURE RATE



estimating accuracy though hoped for is not expected at the very beginning of a new development program. As soon as details are available, estimates should be improved, and this improvement process should be iterative thenceforth and throughout the entire development program, finally stopping only when the existence of functioning hardware permits measurements and observations to replace estimates.

Once circuit design takes shape, the electrical stress on each avionic piece part can be calculated so that the broad rules for derating (e.g. resistor dissipation shall not exceed 0.5 its wattage rating) previously used when selecting failure rates can be replaced with actual electrical stress. Digital computer techniques for circuit analysis now permit analyses such as calculation of electrical stress to be accomplished rapidly and with relatively little manual effort.

As rapidly as an experimental model suitable for a thermal survey can be constructed, temperature measurements can be made providing a much better approximation of the local temperatures of each of the parts whose failure rates depend on temperature. Even prior to experimental thermal measurements, heat flow calculations for the paper design can yield more realistic approximations of temperature than probably were used in the initial estimate. Mechanical design details will take shape and permit circuit counting and improved failure rate selections for connectors. Improved resolution of anticipated use will lead to better estimates of the cycling to be expected for electromechanical devices such as switches, relays, etc., and this in turn also permits improved failure rate selection.

Probably the most significant of the new available information now that design has progressed is the need for new or unusual non-standard parts, items for which failure rate information is not available. In fact, any part for which there is no handbook failure rate information introduces unknown estimating error. Handbook estimating methods are available for capacitors, connections, connectors, transformers, inductors, coils, relays, resistors, motors, fans, blowers, semiconductors, switches, electron tubes, wire, cable, and newly to some extent for microelectronic devices (integrated circuits).² Relatively coarse figures, usually quite satisfactory, are also available for low population devices such as gyroscopes, vibrators, circuit breakers, fuses, lamps, meters, heaters, and microwave elements. Other items depend for failure rate information on other sources. Figure 2 is an example of typical data.

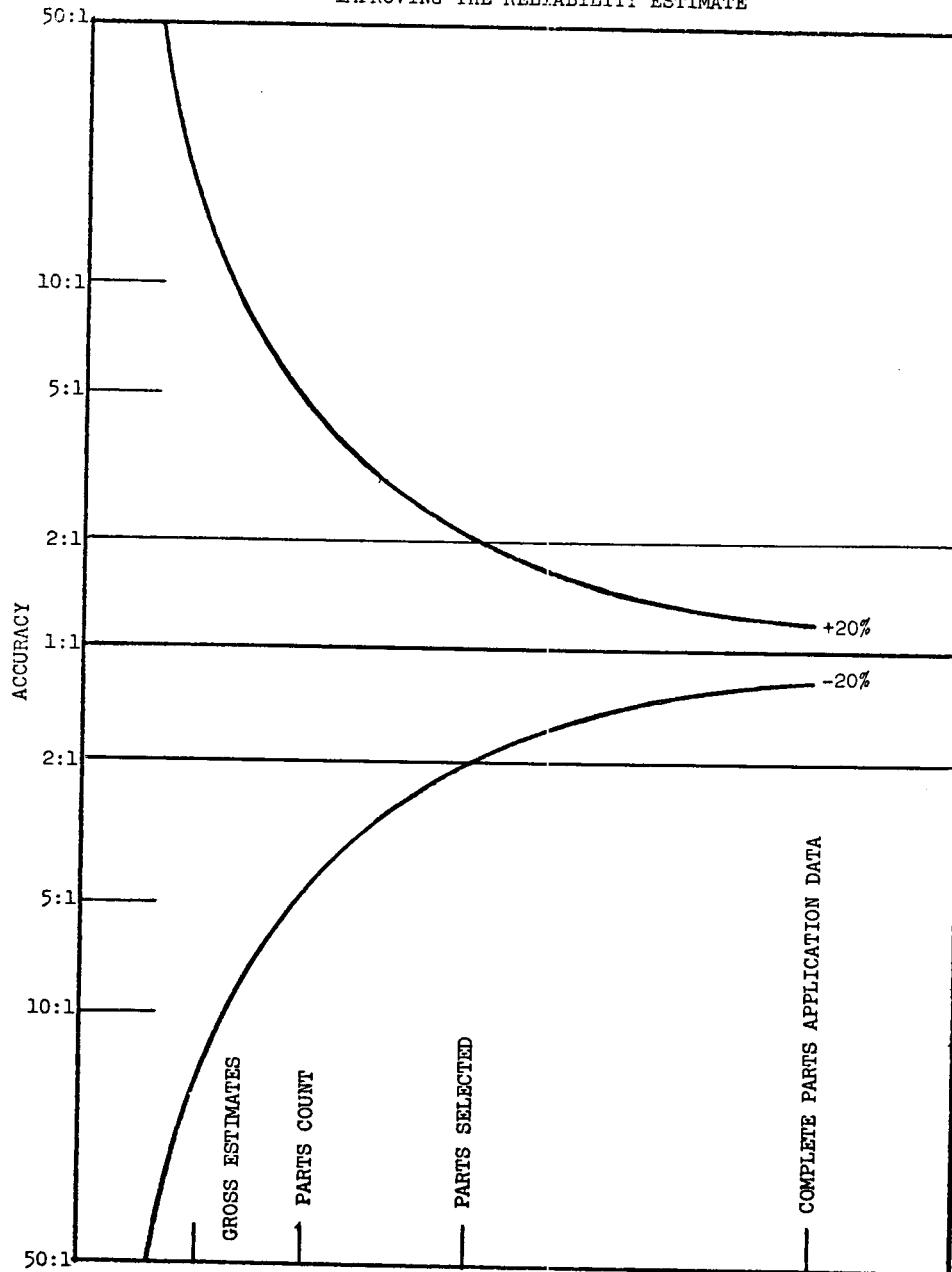
Vendor data often provide a prolific source of failure rate information. The obvious question is whether a vendor's desire to puff his product will make resulting failure rates overly optimistic, and this may well be the case. However, test data generated by large scale vendor-run reliability tests on high reliability parts will probably be quite trustworthy, and certainly any firm bothering to undertake overt large-scale reliability testing has more to gain by promulgating honest data than otherwise. In the U.S.A. vendor reputations are usually well known, and much trustworthy vendor data are available.

Another source of reliability data often tempting and sometimes very valuable is the quantity of test reports published by other programs and often quite germane to local problems at hand. This author has

ease of maintenance. Last but not least, the estimating procedure should make some sort of contingency allowance for the failure rates associated with items of oversight. The penalty usually paid when these factors are not adequately taken into account is the need for significant reliability growth between the time of first reliability observation and the time when user satisfaction must be achieved. Often the strenuous growth so needed places an extreme burden on the volume of failure analyses and corrective design change necessary.

It is contended that reliability estimating can be performed which yield accuracies of plus or minus twenty percent. I am sure there are many reliability practitioners whose experience refutes this. On the other hand, there are cases of good estimating which seem hardly to have been accidental. When an estimate is the result of several iterations over the important first portion of a development program, the twenty percent accuracy is likely a not impossible goal to shoot for. (Figure 3)

FIGURE 3
 IMPROVING THE RELIABILITY ESTIMATE

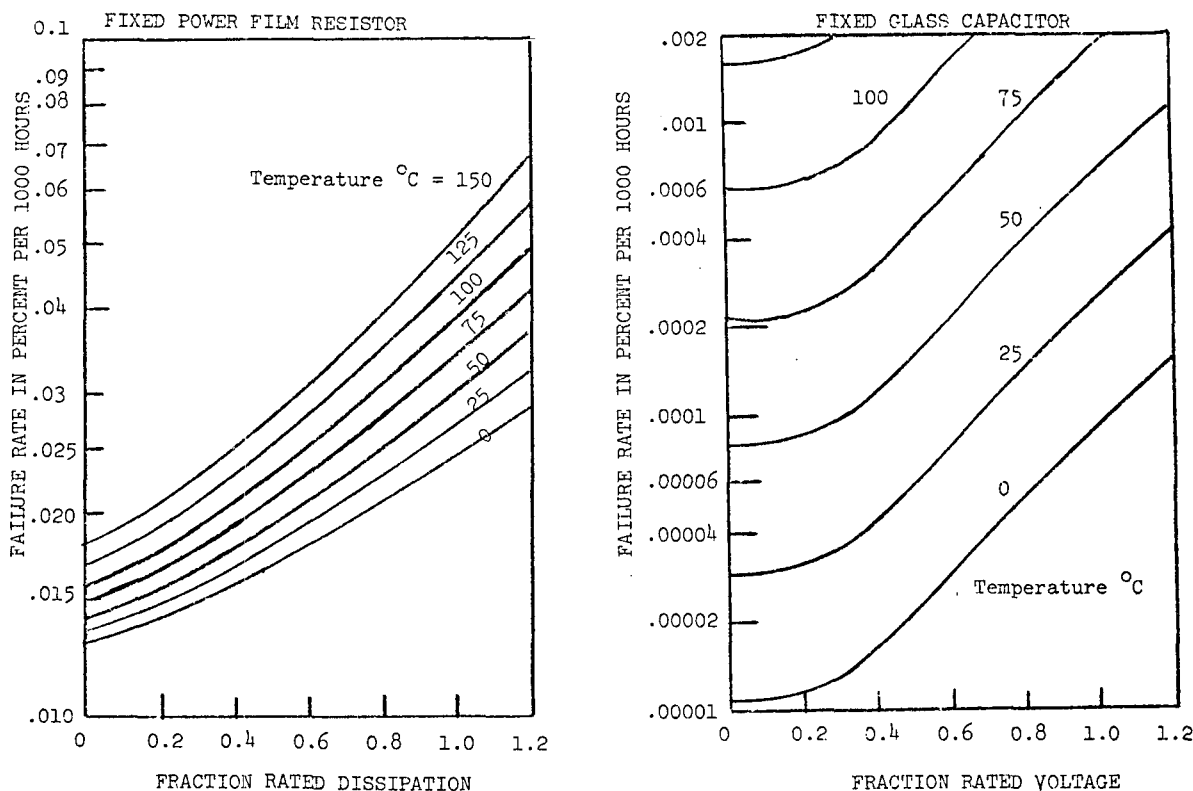


IMPROVING THE RELIABILITY

One very important technique for optimizing reliability which seems to receive far less attention than it deserves is the Failure Mode and Effect Analysis (FMEA). Additionally, there are the more common techniques for reliability improvement and these include review of parts selection, parts application, derating, redundancy, and operational effectiveness. The attention that the FMEA deserves has resulted in its identification in this paper's title, and the inclusion as Appendix A of an industry Standard Practice instruction for FMEA preparation.

The "Mode" in FMEA relates to the identification of how a failure occurs, and a FMEA identifies all the likely ways in which each system element can fail, causes for each mode, and frequency to be expected under the studied conditions of use. While the practitioner does not have means for ensuring that every possible mode is identified save by his long experience with hardware, diligence and experience in the preparation of

FIGURE 2



found that such source data can lead to reliable information but generally should not be used directly. It is quite valuable to arrange to review the material with its author or someone equally informed, and find out about the beginning and end of the project for which the data were obtained, about all the surrounding circumstances at the time, the probable accuracy of data presented, what subsequent though unpublished information of interest exists, and who else with what success has made use of the data. It will be recognized from these considerations that if such an exploration is to be made, it matters little whether the initial lead was a report containing apparently useful reliability data, or was a report without data but concerning a program which likely developed useful and unpublished reliability data. The frequency of need for such data searches in the U.S.A. has led to a camaraderie among reliability practitioners which greatly enhances data acquisition.

Sometimes, and not infrequently with new developments, there is a need for failure rates for items with no prior background, or where the sum total of experience is so limited that reliability is still unknown. Three possibilities are present. The item may be broken into its constituent raw materials and functioning elements, and a probable failure rate obtained by summation of the elemental failure rates generally associated with such materials and elements. As a second approach, the item may be viewed with respect to its similarities to other items of known failure rate, and a figure obtained by interpolation. This approach is much the same as the gross estimating approach used for equipments and systems and already mentioned. A last approach is the development of a failure rate by the conduct of special reliability life tests. This method is often costly, especially for very reliable items, because of the need for either many items for test, or for a lengthy test. The accuracy of the developed failure rate will depend entirely upon how many failures were observed. Thus for a new item that would contribute no more than a tenth of one percent to the unreliability of a system which possessed one thousand hours mean-time-between-failures, one could expect a test failure no oftener on the average than every million item operating hours, and several failures would need to be observed to give credence to a failure rate conclusion. Thus a thousand items on test simultaneously for nearly a year (5000 hours) might yield no more than five failures, and a useful estimate of failure rate if no errors were made in running the test.

It is very important when making a system estimate heavily dependent on the correctness of handbook failure rates for standard parts, that either the actual piece parts used in the design be exactly those for which the handbook failure rates apply, or the handbook failure rates be properly adjusted for the parts actually to be used. The greatest risk occurs when the attempts made to procure parts corresponding to handbook failure rates are not adequate. In the U.S.A., if parts are properly procured to correct military specifications as cited in handbooks, then at least the procurement specifications are those that have been tried and proven. On the other hand, if a military specification is not to be used, then it becomes almost mandatory, at least for the high reliability parts, to make up a specification that goes far beyond the specification used by the parts manufacturer. This is because there is important need to have the specification carefully define performance, environment, electrical operating conditions, material, constraints against material or process substitution, qualification and acceptance tests, methods of inspection, screening, identification means, and perhaps other factors.

The system or equipment for which an estimate is prepared must be designed to represent all the sound and proper design facets that are assumed by the reliability estimating technique used. Perhaps it goes without saying that worst case, sensitivity, and degradation analyses should be considered to the extent that the system has an appropriate allowable degradation before failure must be claimed. Similarly the designer must always strive for preferred environments for his system elements. If alternate mode operation is possible, provisions should be made. The design must be reasonable for good operator effectiveness and

FMEA's has shown that significant oversights tend to be the exception rather than the rule.

The "Effect" in FMEA relates to identification of the result of the failure and a FMEA includes a careful summary of the result of each kind of failure on system functioning and operation. Accordingly, some modes may affect human safety, others mission success, and still others only operating convenience. Most significant is the identification of each and every failure mode that will abort the mission as a result of a single failure. Obviously, if all such "single failure" aborts can be designed out of the system through redundant arrangement of equipment and operators, then the multiple simultaneous failures which will cause abort are much less likely and this yields significant increase in mission reliability. Actually, many single failure situations are usually found to exist in initial design, and a great proportion of these can be quite readily and conveniently eliminated by simple system rearrangement. Those that are not so easily eliminated nevertheless should get most careful consideration by the design staff, because reliability improvement obtained by this route early in the development program will provide the greatest improvement for the least effort.

The first FMEA for a system, often early in the concept phase, will justify many alternative design selections. The continuously updated FMEA shortly thereafter can become the basis for initial redundancy decisions. Not much later the FMEA can provide useful background to any decisions for special environmental control and operating profile.

A review of Appendix A will show that the FMEA is a methodical look at each system element at the lowest level possible at the time. While the system may initially be broken down to no greater depth than the assembly level, it is often desirable later on to update the FMEA to go down to piece part level. Early FMEA's may recognize only the more obvious failure modes, but later revisions will add most of the important subtle modes. The FMEA forms are designed to encourage ingenuity on the part of the analyst, and some FMEA's are very voluminous with good justification. In any case, the early preparation of an initial FMEA no matter how brief will be most important to the design effort. Continuous updating can later take care of missing embellishments.

The "computer age" of today makes possible "worst case" and "sensitivity" analyses of circuit design early in design evolution. In worst case design analyses, the computer examines circuit functioning when composed entirely of parts and components at each of the extremes of tolerance for every electrical and functioning characteristic. The degradation or failure of function resulting can then become the basis for readjustment of pertinent tolerances, or circuit redesign. Before the existence of computer programs for such analyses, the protracted effort for manual analyses usually limited the technique to high importance repetitive circuitry. Today absence of worst case analyses as a part of initial circuit design can hardly be justified when reliability is important. In a sensitivity analysis, the effect of variation of each electrical component characteristic on circuit function is studied, and circuit design is adjusted as necessary to exclude or minimize degradation and drift failures. With both of these types of circuit analysis as well as with the advent of microelectronics pushing the circuit designer toward circuit standardization, it becomes possible to much more easily justify a reasonable amount of exploratory reliability testing to prove that the applied design techniques actually result in the desired reliability.

Piece part reliability techniques that provide improvement and optimization through selection, application, and derating considerations, can be briefly summarized. In choosing an avionic piece part, careful consideration should be given to a justified need for premium cost high reliability parts which have established low failure rates. In this category are several types of capacitors, resistors, and semiconductors. The choice of a high usage part has the advantage that quantities of useful reliability data probably exist. Selection of a high stability part reduces the burden on sensitivity and worst case analyses to avoid functional degradation with gradual circuit failure. Selection of parts which are supported by large quantities of valid reliability data can permit substantiation of assigned failure rates. Selection of parts that are known to receive effective and significant vendor screening and thus do not include culls and rejects may tremendously reduce the need for close and never perfect detailed part inspection.

The technique of developing an application form sheet for each common category of avionic part, and then detailing all factors of electrical, mechanical, and thermal environment for each part on a separate line on the appropriate form sheet as it becomes a part of circuit design, with updating as necessary, has been known in the U.S.A. avionic industry for some time, but its benefits may be neglected on occasion. This technique when properly and comprehensively applied, gives instant identification to the electrical stress, the environment, the selected characteristics, source, and other important factors for all parts in a circuit design, and the layout is such that supervision and reliability personnel can easily review status so that application weaknesses can receive the early special attention they deserve. (See Appendix B).

Avionic part derating for a long time has been carried on principally by rote, and the reliability estimating process then assumes that each part category has the "regulation" derating applied. Actual stresses are seldom at the derated value; in fact, on not infrequent occasion stresses grossly exceed the derating limit. We know handbook failure rates often change rapidly with applied stresses and environments. Accordingly specific derating, and related specific handbook failure rate should be variables which are updated as the design evolves. Where experience dictates that desired failure rates cannot be obtained without special parts screening and burn-in, then these requirements must be established. At present, appropriate screening and environmental burn-in have become equally important with other specification characteristics in this micro-circuit age.

JUDGING RELIABILITY STATUS EARLY IN THE PROGRAM

Once functioning hardware becomes available to the development effort, even in the form of early breadboards, it is time to consider replacing failure rates derived from handbooks and other non-program sources with failure rates which take account of observed failures. Thus the effect of stresses in a breadboard model can show up oversights in early estimates (and oversights in FMEA's). Once the model construction reaches the point of providing representative thermal environment, closer correlation yet with failure rate estimates is possible (as is a check on worst case and sensitivity analyses). Later yet with the existence

of an engineering model to reflect the design in all respects except production tooling, pretty good insight to actual reliability is possible.

If functional observations from the breadboard and later models are to be useful, it will be necessary to write and file failure reports on the observed failures, to analyze those when the cause is not otherwise obvious, and to follow a routine for applying the findings to both design correction if necessary and to affected analyses as pertinent. While the operating time logged during this state of design evolution is nowhere sufficient to couple with observed failures to yield a calculated failure rate with any great confidence, it doesn't take many failures with limited operating time to establish that a failure rate is radically lower than that utilized in the estimate. If the critical surplus of observed failures can be blamed on workbench errors, improper test conditions, and other excusable causes, then well and fine. However, seldom can development proceed for long without producing one or more perplexing failures that uncover either an unexpected addition to the FMEA, to the part specification, to the circuit design, or to the failure rate estimate. By the time planning for a reliability demonstration test is to begin, either considerable confidence as to test success exists, or a strenuous exploratory testing effort is already underway to uncover the remaining causes and cures for unacceptable unreliability. There is little reason to embark on a reliability demonstration test in ignorance of the likelihood of passing it.

Reliability demonstration testing requires considerable advance planning. Not only do facilities that are adequate in every respect need to be secured and checked out, but it may be necessary to take many pains to properly achieve the required test environment. Test chamber thermal cycling to produce a specific and desired time-temperature relationship at specific point or points on a test specimen can seldom be calculated, assumed, or obtained by any means other than experiment. Test procedures must be suitable, acceptable to all, and understood, if an experiment is to validate the adequacy of the facility. Failure scoring during a test when great risks and responsibility hangs on the outcome will require comprehensive rules and even rehearsal. Decision as to which failures to count and which to ignore must be decided for every eventuality before test inception. Because a reliability demonstration test establishes reliability adequacy by observing a sample of failures and considering them indicative of future failures not yet occurred, a retest cannot be allowed unless the equipment design and configuration is sufficiently altered (improved) to become a first test of a new design. Any sampling process, if permitted to repeat indefinitely, will sooner or later give any desired outcome and the number of repetitions before the desired outcome occurs depends only on the likelihood or unlikelihood of the desired outcome. The reliability demonstration test usually called for will probably have been designed to judge acceptability and not most probable reliability. However, the test operating time and number of failures can be used to calculate the most probable observed reliability, and this can be used to indicate the extent of needed improvement if the test goes adversely.

When representative hardware reaches field use, field observation may give some opportunity for reliability calculation and comparison with reliability estimates. With field data it is important to remember several factors. Field application may not be to the extreme environments that were required for test and in the estimating process. Operating personnel judging adequacy of performance may vary among themselves, and their judgment of adequate performance may vary considerably from specification performance. Field maintenance personnel may be unskilled at troubleshooting and may claim an unjustified and excessive quantity of relevant failures. If avionic system repair is by field replacement of subsystem or other replaceable unit, with the faulty unit going to a remote repair facility, it may be difficult or impossible to associate the repair facility failure reports with the field failure reports. In fact many units may appear satisfactory when tested at the repair depot (the true complaint may lie elsewhere) with no means for discounting field reports accordingly. When field operations are on a sizeable scale, or when reliability personnel from the development program can personally follow the hardware into field use, then field observations can be quite useful and will likely correlate with development measurements and estimates when adjusted for operating conditions.

While in some cases reliability estimating begins and follows through to ultimate use observation with little or no discrepancy, and no more than 20 to 50 percent variation, there are many instances of far worse comparisons. In one program, paper estimates missed observed reliability during demonstration test by an order of magnitude, with field experience falling somewhere in between. Explanation would suggest that the extremes of test environment (worse than field environment) were not adequately taken into account in the estimating.

RELIABILITY GROWTH AND ULTIMATE RELIABILITY ATTAINMENT

In defense of a position of need for more reliability than could be estimated or forecast, there is always a large temptation to turn to claims for expected reliability growth, and to various ways to justify this expectation such as by pseudo-calculation. While few people will disagree with the philosophy that no one can get reliability improvement without an effort, many are tempted to quantify the expected reliability growth without quantifying the planned reliability effort.

In the early days many programs for reliability improvement were instituted that depended entirely on observation of failure, elimination of future failure repetition through design improvement, and more failure observation. It was suggested that by this means of slow but inevitable failure prevention, any desired high reliability could be obtained if the process was carried on long enough. The fallacy with this method can be seen by reference to the failure mode and effect analysis. For a complex equipment, say one that can be expected to suffer a failure reasonably frequently, a thorough and complete FMEA would list literally thousands of failure modes. If design correction were so perfect as to literally eliminate any failure repetition, it would still take observation over thousands of MTEF's to provide the failures to identify every failure mode and if the reliability were increasing as it ultimately would, this would mean an increasingly longer time to observe each successive failure. As a result, the fail and fix technique, effective though inefficient when reliability is abnormally low, becomes ineffective and reaches an apparent upper reliability limit when failure frequency is too low for further observation. This upper failure limit is probably not much above the reliability that a sound and thorough design and development effort could have achieved by meticulous attention to detail and without any dependence upon reliability growth.

There have been published attempts to show quantitative and predictable reliability growth without regard to magnitude of effort by plotting cumulatively on log-log graph paper cumulative system mean time

between failures versus total system operating time. This cumulative style of log-log plotting automatically provides heavy smoothing of the MTBF so that with reliability improvement effort the plots appears to follow a straight line with an upward reliability slope. Unreserved claims by others for the magnitude of upward slope and the straightness of the line regardless of what equipment and what program were to be examined led this author to plot accumulated data from several consecutive years operation of several different avionic equipments. It was found that the plot does not always show improving reliability. In fact, in half a dozen instances where the reliability effort had somewhat subsided, the plot went down hill. In other cases the plots appeared oscillatory (rather than straight line) especially in programs where the reliability effort applied was known to have fluctuated. Importantly, there did not appear to be any ready means to correlate quantitative reliability growth with any measure of reliability program effort. Therefore, an inevitable conclusion seems to be that reliability growth is possible, but its magnitude and rate are not predictable by any proven method relating to reliability program effort or any other reasonable measure of input. While significant growths have been observed, of twenty-five studied cases 40% showed unquestionable improvement (one case three to one improvement, one with two to one improvement, the rest averaging 40% improvement). Thirty percent of the cases studied fluctuated with total change seldom over 30%. The remaining thirty percent of the cases studied showed reliability deterioration. Reliability growth then does not appear promising as the means to achieve an important reliability requirement.

CONCLUSION

From the preceeding discussion, it can be seen that estimating or predicting reliability is a process that can regularly have great value in the hands of experienced engineers, or it can have little value when performed by the inexperienced. Many undoubtedly have the mistaken impression that estimates and predictions can be generated by following a "cookbook recipe," but the result is apt to be as unpalatable as the first attempt at dinner by a new bride. When estimating is performed by the expert, he may have difficulty explaining where the handbook technique stopped and his judgment took over. Thus in the avionics industry many reliability specialists ultimately become known by the accuracy and foresight of their estimates. In the long run, diligence and perserverence and attention to the many details noted herein will pay off and the estimates generated will gain and gain in accuracy.

REFERENCES

1. MIL-STD-756A "Military Standard Reliability Prediction," U.S. Government Printing Office, 15 May 1963.
2. MIL-HDBK-217 "Military Standardization Handbook Reliability Stress and Failure Rate Data for Electronic Equipment," U.S. Government Printing Office, 1 December 1965.

APPENDIX A

MCDONNELL AIRCRAFT COMPANY



STANDARD PRACTICE

NO: 8.503

PAGE 1 OF 5

DATE: 1 June 1970

SUPERSEDES:
ESP 8.503 dated
7 May 1969

ORGANIZATION: ENGINEERING

SUBJECT: FAILURE MODE AND EFFECT ANALYSIS

A. SUMMARY:

1. The purpose of the Failure Mode and Effect Analysis (FMEA) is to avoid costly modifications by ferreting out latent design and operational hazards in an early design stage.

B. APPLICABLE TO:

This procedure is applicable to all system design effort at MCAIR.

C. DEFINITIONS

1. Failure: The inability of a component or item to function as specified.
2. Failure Cause: The nature of the failure mode: what caused the component or item to fail?
3. Failure Mode: The nature of the failure: how can the subject component or item fail?
4. Failure Mode and Effects Analysis (FMEA): The FMEA is a systematic evaluation of a system or subsystem analyzed at the lowest level possible to identify and determine the possible hazardous failure modes and their effect on the system.
5. Fault Analysis (FA): A systematic evaluation of the results of the FMEA to seek out and eliminate any single failure that will be hazardous to the airplane. Provides fail-safe substantiation of the airplane in addition to FMEA information.
6. Hazard: Any real or potential conditions that can cause injury or death to personnel, or damage to or loss of equipment or property.
7. Hazard Classification: A qualitative measure of hazards stated in relative terms and based upon considerations of personnel error, environment, and design characteristics.
8. Safety Abort: The abort or discontinuance of a flight because of the failure or malfunction of a component that lowers flight capability to a point where the safety of the aircraft and crew is in jeopardy.

A safety abort can result from Category II hazards because of failure of critical subsystems with or without redundancy or emergency backup provisions, e.g., Fire Warning, Landing Gear, Hydraulic Components, etc., or failure of redundant subsystems or emergency backup provisions where such failure results in hazardous conditions.

9. Mission Abort: The abort or discontinuance of a flight because of failure or malfunction of mission oriented item(s) that lowers the air vehicle combat capability below that required to accomplish the specified mission objective.

A mission-oriented item is required to complete a specified mission, but its failure or malfunction does not necessarily jeopardize the ability of the air vehicle to fly safely, and hence a mission abort does not always result in a simultaneous safety abort.

D. REGULATIONS:

1. The FMEA shall disclose possible single failure situations. Passive and multiple failures that result in a hazardous condition must also be identified. Fault isolation technique for maintenance technicians should be noted for a likely condition requiring maintenance action, when known.
2. The FMEA shall be initiated by a FMEA Component List and Classification, (MAC 3413A) prepared as defined in Paragraph E.I.1. Each item on the component list is then analyzed on the FMEA form (MAC 3413).
3. The FMEA form shall be continually updated and refined to reflect the current status of the system design. The Component list and FMEA forms shall be contained in a MCAIR report approved and maintained per specific program requirements.

E. PROCEDURE I: FMEA COMPONENT LIST AND CLASSIFICATION (Figure 1)

1. The FMEA Component List and Classification is a tabulation of components to be considered in the analysis, their basic function and a classification under one of the following:
 - o Active element, without a back-up.
 - o Active element including a back-up.
 - o Active element, manually controlled.
 - o Instrumentation.
 - o Passive element.
2. This list is created to ensure that all components are considered. In this tabulation it is important that the following items are evaluated in the same perspective as the components:
 - o Electrical Wiring
 - o Fluid or Air Carrying Elements
 - o Linkages
 - o Cables
 - o Connecting an/or Attaching Hardware.

NO: 8.503
 PAGE 2 of 5
 DATE: 1 June 1970

FIGURE 1

MCDONNELL AIRCRAFT COMPANY
FMEA COMPONENT LIST AND CLASSIFICATION

SYSTEM COMPONENT	FUNCTION OF COMPONENT	ACTIVE				
		WO BACKUP	MANUALLY CONTROLLED WITH BACKUP	INSTRUMENTATION WITH BACKUP	PASSIVE	
Bus Tie Circuit Breaker (2 used)(42 AKC)	(1) Allows AC buses to be paralleled whenever the opposite main generator is off line (or failed). (2) Prevents a fault in the opposite bus and distribution system from causing shut-down of both main generators.					X
Transformer-Rectifier (2 used)(42 DBO)	Converts power from the AC bus to DC power.		X			
Transformer-Rectifier Circuit Breaker (6 used)	Protects each phase of each AC bus from faults in the DC system.					X
Current Limiter (42 DCC)	(1) Allows DC loading to be provided equally between the AC buses. (2) Prevents a fault in one side of the DC distribution system from overloading both generators.	X				
AC Present Relay	Provides "lock-out" signal to emergency generator hydraulic solenoid valve to prevent emergency generator from operating when main buses are energized from main generator.	X				

MAC 3413A (26 MAY 70)

MCDONNELL DOUGLAS CORPORATION

E. PROCEDURE II: FMEA FORM (Figure 2)

The FMEA form is the basic tool of the analysis. It contains the effect of failure and includes any possible corrective action that may be taken by the flight and/or maintenance crew. It is completed as follows:

1. Title Block

- a. "WUC/Component" - the Work Unit Code (WUC) number and the component name are extracted

from the FMEA Component List. This includes connections listed in Paragraph E.I.1 by specified callout.

- b. "Failure Rate" - The estimated failure rate is entered as failures per hour (e.g. 150×10^{-6}). Specify if the failure rate is based upon flying time, operating time, or number of cycles.

NO: 8.503
PAGE 3 of 5
DATE: 1 June 1970

FIGURE 2
FAILURE MODE AND EFFECT ANALYSIS (FMEA)

WUC/COMPONENT <u>Xfar-Rect Circuit Brkr.</u> FAILURE RATE <u>3.33 x 10⁻⁶</u> FUNCTION OF COMPONENT <u>Protects AC Bus from faults in DC subsystem (6 used)</u> PREPARED BY <u>James H. Shumate</u> DATE <u>8-21-70</u>									
SUBSYSTEM <u>Electrical</u> REVISOR BY _____ DATE _____									
1	2	3	4	5	6	7	8		
FAILURE OR ERROR MODE	FAILURE CAUSE (INCLUDE OUTSIDE FACTORS)	P H A S E	EFFECT OF FAILURE OR ERROR ON SYSTEM	H L A Z S	DISP INOP YES/ NO	(A) INDICATION TO FLIGHT CREW (C) HOW DOES FLIGHT CREW ISOLATE THE FAULT? (E) EFFECT OF LIKELY INCORRECT ACTION (G) HOW DOES MAINTENANCE CREW ISOLATE THE FAILURE?	(B) OTHER FAILURES WITH SAME INDICATION (D) CORRECTIVE ACTION (FLIGHT CREW) (F) IS FAILURE PREDICTABLE? HOW? (H) CORRECTIVE ACTION (MAINTENANCE CREW)	EFFECT OF ADDITIONAL FAILURES (PASSIVE, ZND, ETC.)	
Will not remain closed or gives false trip levels. (75%)	Mechanical Latch failure	A Less G2, G4	Negligible, causes slightly lower DC voltage output	II	No	A. None B. N/A C. Maint. crew isolates fault D. None E. No incorrect action considered likely F. No G. Use DC Bus BIT to recognize failure, note breaker trip indication H. Replace defective breaker		False trip of another breaker in the same input would essentially disable the transformer-rectifier requiring the other transformer-rectifier to provide all DC.	
Failure to trip under overcurrent conditions (25%)	Mechanical failure, open sensing - trip circuit, contact welding.	A Less G2, G4	Lower DC output voltage initially; then generator shutdown	II	No	A. "Generator Out" light illuminated B. Other generator and distribution system failures. C. Maint. crew isolates fault. D. Generator control will trip, disconnecting generator; bus tie circuit breaker will then trip, isolating AC Bus (if failure is on the left side, the emergency generator will come on). Pilot must make decision whether to continue mission with functions powered from disconnected bus unavailable. E. Reduced mission capability F. No G. Trace AC Bus down from known "good" points, the generator control unit, and the bus tie circuit breaker. H. Correct line fault and replace failed circuit breaker.		This failure would be significant only as a second failure.	
SYSTEM OPERATING PHASES (COL 3)	GROUND G1 TAXI G2 LOAD AND ANCHOR G3 START AND WARMUP G4 TRANSITION TO STOW AND ROLL OUT G5 AIRPLANE STATIC - SYSTEM OPERATING	ALL A	TAKEOFF T1 TAKEOFF ROLL - PRIOR TO ROTATION T2 TAKEOFF - AFTER ROTATION	IN-FLIGHT F1 CLIMB F2 GEAR UP F3 GEAR DOWN F4 CRUISE F5 DESCENT	APPROACH F6 COMBAT F7 OTHER (DESCRIBE) F8	LANDING L1 LANDING ROLL L2 GROUND ROLL BRAKING	HAZARD CLASSIFICATIONS (COL 5) CLASS I - NEGLIGIBLE CLASS II - MARGINAL CLASS III - CRITICAL CLASS IV - CATASTROPHIC		

NO: 8.503
 PAGE 4 of 5
 DATE: 1 June 1970

E. PROCEDURE II: FMEA FORM (Cont'd)

2. Failure or Error Mode (Column 1)

The component or hardware failure modes should be included on an individual basis and listed separately. For example, in the case of a valve, "Fails to open," "Fails to close." Failure mode generally answers the question of "how" it fails. An estimate of the percentage of the gross failure rate attributed to each mode should be entered when known. The analysis should include consideration of:

- a. Incorrect installation or adjustment.
- b. Damage in installation.
- c. Human error in observation, installation and adjustment.

3. Failure Cause (Column 2)

The cause of the failure or error made should be entered in this column. It answers the question of "what" caused the component to fail.

- a. Component Inherent Failure - These are all causes wherein the specific component fails inherently.

Error modes (human error) are most likely to occur as a result of a design deficiency. These causes may be placed in two main categories:

- (1) When characteristics of a subsystem design tend to place undue reliance upon operating personnel for check out and test.
- (2) When components or hardware in a subsystem are designed such that the component or part can be installed incorrectly.

- b. Component Failure due to Outside Factors - Two types of conditions should be considered. The outside environment, (i.e., temperature, relative proximity of adjacent components) or secondary failure due to an adjacent component.

4. Phase (Column 3)

The analyst should start with the airplane on the ground with engines OFF and mentally run through the operating regimes involved in making a complete flight. All possible combinations of inter-related elements or subsystems must be considered. Usually there is one obvious case that is relatively adverse. With this in mind, other possible operating phases can be rapidly compared.

Alpha-numeric designators listed across the bottom of the FMEA form may be used to identify various flight profiles. Each component should be considered in every phase.

5. Effect of Failure or Error on System (Column 4)

The analyst, having established the operating condition(s) at which the component failure or error mode is important, (i.e., has the most important effects on the system), should now

record a detailed narrative of the effect(s) of each failure. After completing the single failure effects narrative:

- a. Consider the effects on the system if the airplane is dispatched with the component inoperative.
- b. If the effects are different, enter a detailed narrative.
- c. If the effects are the same, no entry is required.

The schematic, wiring diagram or drawing, whichever is applicable, should be cross referenced to the narrative(s).

6. Hazard Classification (Column 5)

Assign a hazard classification to the component failure based on the end effect on the system or subsystem. In assessing the component failure for hazard classification assignment, do not include the benefit of corrective action by the crew. This provides a base line for system safety evaluation. For example, when a component failure is classified as critical, (Class III), an assessment of the corrective action, for the component failure, will determine whether or not acceptable minimums have been attained.

The criteria in Table II should be utilized in determining the classification number to be placed in Column (5). A condensed list of these are also on the bottom of the FMEA form. All Class IV hazards resulting from single point failures shall be eliminated. Class III hazards shall be minimized and controlled.

TABLE II

Class I - Negligible

Hazards associated with this classification can be termed "nuisances." These in all probability will not result in a "Safety Abort."

Class II - Marginal

Hazards associated with this classification will in all probability lead to a safety abort.

Class III - Critical

Hazards in this classification will in all probability result in an accident or injury unless immediate corrective action is taken by the operator. These hazards must include the appropriate detection systems and/or adequate warning devices to preclude progression to a Class IV hazard. Where the magnitude of the hazardous condition cannot be reduced by detection and warning systems, special emergency procedures must be made to reduce the probability of occurrence.

Class IV - Catastrophic

Hazards in this classification will result in death or severe injury to personnel and/or loss of the air vehicle. Therefore, Class IV single point failure conditions shall be eliminated through design or controlled through

NO: 8.503
PAGE 5 of 5
DATE: 1 June 1970

E. PROCEDURE II: FMEA FORM (Cont'd)

special procedures such that they fall within a lower hazard classification.

7. Dispatch Inoperative List (Column 6)

After completion of the component evaluation (obtained from an assessment of Column 4, "Effects of Failure or Error on System" and Column 8, "Effects of Additional Failures") indicate whether or not dispatch can be made with the Component inoperative by placing either the word "Yes" or "No" in Column 6.

An airplane can be dispatched only if acceptable level of safety is maintained.

8. (Column 7) - Indications and corrective action should be recorded in this column. All eight items should be addressed for each Failure or Error Mode. These items are:

a. Indication to Flight Crew (Column 7-A) - Describe the indication as:

- (1) Normal - An indication that is evident when the system is functioning normally.
- (2) Abnormal - An indication that the system has malfunctioned.
- (3) Incorrect - An erroneous indication due to indicator malfunction.

If no indication exists, note if (1) the failure critically affects the subsystem operation or (2) the failure jeopardizes the operational safety of the airplane.

If the first failure allows the system to remain in a safe state, the second failure situation should be explored to determine whether or not an indication will prevail.

NOTE: In order to effect proper corrective action, through correlation, it is sometimes necessary to call out normal indications as well as abnormal indications.

b. Other Failures with Same Indication (Column 7-B) - List other failures in the subsystem or other systems that will give the flight crew the same indications.

c. How Does Flight Crew Isolate the Fault? (Column 7-C) - List the most direct procedure that allows the Flight Crew to isolate the failure. The crew will know only the initial symptoms. The failure being considered in the analysis may be of lesser importance or likelihood than another failure that could produce the same initial symptoms and this must be taken into consideration.

Fault Isolation procedures require a specific action or series of actions, followed by a check or cross reference either to instrument(s), cockpit control device(s), circuit breaker(s) or combinations thereof. This procedure is followed until a satisfactory course of corrective action is determined.

d. Corrective Action (Column 7-D) - The flight crew corrective action is entered in this column. Determine the corrective action

that best satisfies the indication(s) observed by the crew when the component failure occurs. This sometimes requires the investigation of an interface system to determine the most correct crew action. Structural Mechanics and Aerodynamics Section inputs should be included in the corrective action whenever applicable. The diagnosis of an in-flight failure has to be derived from the indication(s). Therefore, the corrective action must be based on the indication.

e. Effect of Likely Incorrect Action (Column 7-E) - Enter the effects of any probable incorrect action that the Flight Crew might take in response to an abnormal indication, (Col. 7-A).

f. Is Failure Predictable? How? (Column 7-F) - Enter information peculiar to the component failure trends that is predictable in advance. If the failure is predictable, relate in terms of how it may be predicted, i.e., what parameters can be measured, parameters such as temperature, pressure, flow, position, wear, etc.

g. How Does Maintenance Crew Isolate the Failure? (Column 7-G) - Explain in detail how the failure may be isolated if the procedure differs from the flight crew isolation procedure. The maintenance technician needs explicit instructions in how to locate the malfunction. The approach to take is similar to the one discussed under Column 7-C.

h. Corrective Action (Maintenance Crew) (Column 7-H) - Indicate corrective action to be taken by Maintenance Crew including possible effect of failure on other systems.

9. Effect of Additional Failures (Passive, 2nd, etc.) (Column 8)

Failure considerations under this topic include:

- a. Failure of other components, hardware, wiring, linkages, etc., in the subject subsystem in addition to the single failure being analyzed. This includes active as well as passive failures.
- b. Failure of interface components that compound a single failure situation into a multiple failure.

The effects of multiple failure situations (active and passive) should be entered in this column. Single failure situations should already be entered in Column 4, "Effect of Failure or Error on System."

This column may also be used for remarks simply by adding the heading Remarks before the text.

F. REFERENCES:

1. Forms

- a. MAC 3413, Failure Mode and Effect Analysis
- b. MAC 3413A, FMEA Component List and Classification

[illegible]

APPENDIX B

TYPICAL DATA PARTS APPLICATION DATA SHEETS

Capacitors

Connectors

Electron Tubes

Inductors

Relays

Resistors

Rotary Electrical Devices

Semiconductor Rectifiers and Diodes

Switches

Transformers

Transistors

Zener Regulator and Reference Elements

[illegible]

1

1-Aprp. B-12

[illegible]

SWITCHES

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

CORRELATION BETWEEN ESTIMATION TESTS AND SYSTEM OPERATING DATA

M. M. Tall

RCA

In an article several months ago, Aviation Week and Space Technology⁽¹⁾ quoted a Pentagon official as saying that the "military avionics market in the 1970's will see increased emphasis on sound engineering rather than on the 'imagineering' which dominated our sense of values during the decade following Sputnik". In the early post-Sputnik environment, "any military official who even talked of using an old-fashioned airplane to drop an iron bomb on an enemy depot instead of considering the possibility of doing the job from space, was out of tune with the times". Industry, in response to its customers' new thinking, proposed all sorts of esoteric systems from installing long-range missile bases on the moon to deploying hundreds or thousands of orbiting satellites as an anti-ballistic missile system. The possibility of transporting small numbers of ground troops by ballistic missiles was publicly discussed. Although these proposed systems were not pursued, the enthusiasm that led to their proposal was reflected in a myriad of advanced approaches to the more conventional systems.

In the military avionics field, for example, the digital computer became the "magic genie" which could do anything and everything, relieving the military commanders of all but critical decisions in the command and control process. In retrospect, it is clear that the digital computer was oversold and the long, difficult and costly process of computer programming was undersold.

During the post-Sputnik decade, avionic suppliers stressed how much automaticity could be provided to relieve the flight crew of its admittedly heavy combat load. Neither the military user or the supplier seemed to recognize that this approach resulted in increased complexity and that the burden of higher failure rates fell on maintenance personnel - always in short supply.

Microcircuitry, first appearing in the early 1960's, led to optimistic projections of avionic reliability. But, in too many instances, microcircuitry spurred a major increase in equipment complexity which counterbalanced gains in overall reliability. Selby and Miller⁽²⁾, for example, found in their analysis of U.S. Navy avionics procured in the 1960's, that both reliability requirements and equipment complexity increased, on the average by a factor of 10 during that decade. The promise of major improvements in reliability was realized. Two orders of magnitude of improvement in reliability achievement was counterbalanced by an order of magnitude increase in complexity.

After a decade of stressing technological advances almost above all else, U.S. Defense Department officials are now placing primary emphasis on setting more modest performance goals which can be met, within cost and time constraints. Reliability and cost are the prime criteria.

Reliability, of course, has always been a consideration. Reliability problems in avionics were recognized since their introduction into aircraft in the 1920's. Failure mode and mechanism studies led to gradual improvement. However, avionics' primary function in the 1920's was communications. Since then, the application of avionics has increased rapidly. In the 1970's, avionics will be required to perform the combined functions of automatic flight control, navigation, fire control, automatic landing, performance monitoring, command and control communications, data processing, radar control, automatic checkout, fuel management, bombing electronic warfare and display in addition to some functions that have not occurred to me. But if these additional applications have not occurred to me, they will to someone else. The growth in avionic applications and complexity will mushroom over the next two decades. And with this growth, the problems of reliability and cost will be compounded. By cost, I am not only referring to the cost of initial procurement, but also to the cost of maintaining these equipments in an operational environment. These equipment maintenance costs are assuming larger and larger portions of the military budget. Unless their growth is controlled, they may well become intolerable as far as national budgets are concerned. The effect of variations in avionic reliability to force effectiveness may be difficult to measure quantitatively. However, its contribution to maintenance costs are more readily determinable. The achievement of still higher levels of avionic reliability is a necessity from both the operational and cost points of view.

Although reliability considerations were factors since the introduction of avionics, they received a major impetus during the post-World War II period. Electronic failure experience during the war was sufficiently dismal that the now-defunct Research and

Development Board formed an inter-service "Committee on Electronic Reliability". In turn, the conclusions of this committee led to the establishment of the Advisory Group on Reliability of Electronic Equipment, popularly known by the acronym, AGREE.

AGREE, a joint government-industry panel, was divided into nine task groups, each concerned with a specific aspect of reliability achievement.⁽³⁾ It was Task Group 3, that first introduced the current philosophy of reliability testing in 1957. Task Group 3 defined the basic test approach, which, through several evolutions, is now reflected in MIL-STD-781B, dated 15 November 1967. The current specification, as well as the original document, defines procedures to be followed in qualifying new equipment to a required MTBF level and demonstrating the same level of reliability periodically (monthly) during production.

This was an entirely new test approach in that reliability was to be demonstrated to a statistical confidence under severe environmental operating conditions.

A typical AGREE test environment is shown in Figure 1. This cycle is repeated continuously for as much as 3 months for each equipment involved. The number of equipment on test may range from three to as many as twenty at any given time. Daily performance measurements are made. Failures are repaired as they occur. The acceptance or rejection of the equipment is determined by a statistical evaluation of failures versus operating time.

Experience has shown that this test philosophy has been a major contributor to reliability growth during the past ten years. First introduced as part of military contract requirements in 1958, its adoption has grown to the point of being a standard item of many procurement contracts.

There are two points of view involved in reliability testing. The first is concerned with debugging the design and materials to assure the attainment of a high degree of reliability. The second is concerned with realistically assessing the expected performance of the equipment in actual use. The user is concerned that the equipment be at least as reliable in the field as was indicated during testing.

As a result, quite a few studies were initiated by both the military and industry to determine what, if any, correlation existed between predicted, test and operational reliability.

The G-41 Reliability Committee of the Electronic Industries Association (EIA) set up a study during the mid-1960's to determine the relationships between estimated, demonstrated and actual field reliability.⁽⁴⁾ They began the investigation by conducting a survey of member companies and associates of the G-41 Committee. Responses were received on 24 equipment types ranging from complex missile-guidance systems to small portable communications units.

A large difference in results was obtained. For example, test MTBF (mean time between failure) ranged from 0.09 to 20.4 times the estimated MTBF. Operational MTBF also showed a large difference in results ranging from 0.08 to 15.5 times the estimated MTBF. Because of the small sample of data available for the wide variety of equipments and extremes of mission application, the G-41 Committee found it impossible to correlate and analyze the data.

Concurrently, an investigation of the relationships between test and operational reliability was undertaken by Arinc Research for the U.S. Naval Depot in Crane, Indiana.⁽⁵⁾ This investigation was limited to avionics equipment. Although AGREE test data was available on 39 equipments, adequate operational and technical data were available on only 11 equipments. Still a small sample, but sufficient to demonstrate that a relationship exists between test and operational reliability. The basic statistical technique used in the study was multiple regression analysis. Several factors other than AGREE test results were recognized as influencing the prediction of operational results. These included equipment complexity and average mission length. Not included in the study was the effect of reliability growth as equipment problems were resolved during field use.

The 11 equipments studied had operational MTBFs ranging from 12 to 301 hours and test MTBFs ranging from 47 to 454 hours. As an average, a test MTBF of 100 hours yielded an operational MTBF of 58 hours - approximately 60% of the test results.

Vander Hamm⁽⁶⁾ found that on introduction to the field, avionics equipment MTBF performance was most likely to be in the range of 20-30% of predicted reliability - although in some cases it has been less.

Selby and Miller⁽²⁾ found that on introduction to the field, avionics of 1968-1969 vin-

tage had MTBFs typically 10% of the value specified in the contract.

Yet, Feduccia and Klion⁽⁷⁾, found that after extensive field use, 70% of the sample (110 equipment types introduced in the early 1960's) performed better than predictions. This is not strange, since the literature is full of examples demonstrating reliability growth during operational use.

Duane⁽⁸⁾ in 1962 found that reliability growth of complex equipment follows a mathematically predictable pattern which was expressed in the now well known Duane model. He analyzed test and operational data for programs with test times as high as 6 million hours on five divergent groups of products (two hydro-mechanical devices, two complex aircraft generators, and a jet engine). He found that reliability growth for a constant level of corrective action effort and implementation, closely approximates a straight line on log-log scales, as shown in Figure 2. Stated another way, he found that reductions in failure rate were approximately inversely proportional to the square root of cumulative operating time.

Selby and Miller⁽²⁾ have confirmed the applicability of this pattern to avionic equipment. Figure 3 indicates some of their findings on 1965 vintage equipment. It should be noted that the established reliability requirements were realistic since they were all eventually achieved. Initial reliability in the AGREE-type test for the newly developed equipment was approximately 8% of their specified requirement. Modified equipments with their reduced development risks achieved compliance in a more orderly and timely fashion.

It should be pointed out that all of these equipments were subject to extensive reliability programs, test evaluations and improvements.

RCA⁽⁹⁾, one of the first companies to apply AGREE testing to avionic equipment, has found that as a general rule, test results have been very similar. The first AGREE test on newly developed devices will demonstrate rather poor performance because all newly developed equipment will contain inherent defects in design, parts, material and assembly. These defects will exist regardless of the scope of the reliability program applied during the design effort. The opportunity for these defects to be present is compounded by the complexity of new avionic equipment and the prolific use of state-of-the-art parts and materials. RCA experience has been confirmed by many avionic suppliers. Vander Hamm⁽⁶⁾, for example, discusses experience on a UHF airborne transceiver. The initial AGREE test resulted in a measured MTBF of about 50 hours. Problems of parts, materials, and design were exposed during this and the subsequent test. The third AGREE test resulted in an MTBF of 420 hours, an improvement better than 8:1. Tests on production samples consistently showed MTBFs near 800 hours - an improvement of about 15:1 when compared to the initial test.

From the user's point of view, the proper application of AGREE testing during prototype or early production, and timely corrective action, result in operational MTBFs reaching their inherent values at a much earlier point in time. Figure 6 illustrates this point in a general way. Not only is the reliability of AGREE-tested equipment higher on introduction but achieves a higher operating level and at an earlier point in time. Indeed, the early experience can be moved back in time so that the indicated reliability growth can occur in development and early production phases.

Minner and Romero⁽¹⁰⁾ in their discussion of F-111A avionics, point out the effect of testing supplemented by an aggressive improvement program on three equipments.

Equipment A (Figure 5) showed no improvement from Test #1 to Test #2. Because of tight equipment delivery schedules, corrective actions resulting from Test #1 could not be incorporated on units for Test #2. However, substantial improvements were realized in Test #3 and #4 because these units received the full benefit of all improvements made following each of the preceding tests.

Equipment B (Figure 6) showed essentially no growth during the development phase. Corrective actions, determined as a result of Tests #1 and #2, were not incorporated until the start of the production programs. Corrective actions resulting from Test #3 were incorporated prior to Test #4. It should be noted that delaying the implementation of determined corrective actions delayed the achievement of the required reliability until the 30th production equipment.

Equipment C (Figure 7) showed a remarkable improvement from Test #1 to Test #2. However, development testing was stopped for approximately two months in order to incorporate design changes in the developmental models. This delay resulted in production without completion of the developmental tests. This, in turn, delayed achievement of the required reliability until the 33rd production equipment.

It should be noted that the reliability achieved during the test program surpassed the goals established for the test program. It would be expected that in accordance with Figure 4, that reliability growth in actual operation would continue to improve, if a constant evaluation and improvement program is maintained.

It is evident that although correlation exists between test and operational results, that other factors are highly influential in affecting the correlation. Insufficient data is available to precisely determine their quantitative effect. These factors include:

- (1) The scope and effectiveness of the reliability program applied during the design phase.
- (2) The scope and effectiveness of the test program. How early the test program starts; the number of equipments on test; the number of tests; and, the responsiveness in correcting indicated defects.
- (3) The scope and effectiveness of production quality to reduce the incidence of defects introduced by procured material, fabrication and assembly.
- (4) The scope and effectiveness of the reliability effort following introduction into the field. Evaluation of field performance and the responsiveness in correcting indicated defects on shipped equipment and in future production.
- (5) And it goes without saying, the knowledge and skill of operational and maintenance personnel in the field.

Failure to apply any of these factors in an effective manner highly influence the user's ability to attain the required reliability and at an early time. Thus, the correlation between the test results and the operational results will be materially affected.

Yet, one must ask himself, is the correlation of test and operational results the prime criterion? Is the demonstration of expected operational reliability through tests, the most desirable route to follow? Major advances in reliability will be achieved. And the overall gain in equipment reliability will be real even with major increases in complexity. The increased application of avionics, however, will accelerate the required reliability for these equipments because of both operational and cost considerations. With these higher orders of required reliability, the difficulty in demonstrating achieved reliability by test will become both costly and time-consuming. Thus, the emphasis will shift to improved estimation techniques during the design phase. Testing will become more severe. Accelerated testing techniques will be applied more frequently. The intent of this extensive testing program will not be to measure the achieved reliability but rather to shake down the design, and remove defects introduced by parts, materials and manufacture. The full follow-up programs of evaluation and corrective action are essential if the estimated inherent reliability is to be achieved or bettered in a timely manner. Admittedly, cost and schedule are impacted by an extensive test, evaluation and corrective action program. The alternative, however, of inadequate operational performance and much higher maintenance costs, is intolerable.

References:

- (1) Aviation Week and Space Technology, Military Concentrating on Reliability, Cost, December 28, 1970, Page 15.
- (2) J. D. Selby and S. G. Miller, Reliability Planning and Management (RPM), presented at ASQC/SRE Seminar, Niagara Falls, N.Y., September 26, 1970.
- (3) Advisory Group on Reliability of Electronic Equipment (AGREE), Report on Reliability of Electronic Equipment, Government Printing Office, Washington, D.C., 1957.
- (4) Electronic Industries Association (EIA), Relationship Between Estimated, Demonstrated, and Actual Field Reliability, October 12, 1966.
- (5) H. Dagen, Relationship Between Acceptance Test Reliability and Operational Reliability, Arinc Research Publication 538-01-1-696, November 15, 1966.
- (6) R. L. Vander Hamm, Environmental Testing - The Key to High Reliability, Annals of Assurance Sciences, Proceedings of Annual Symposium on Reliability, No. 2 Volume 1, January 1969.

- (7) A. J. Feduccia and J. Klion, How Accurate are Reliability Predictions, Annals of Assurance Sciences, Proceedings of Annual Symposium on Reliability, No. 1 Volume 1, January 1968.
- (8) J. T. Duane, Reliability Growth Models, General Electric Company, 1962.
- (9) RCA, Unpublished Notes.
- (10) E. S. Minner and H. A. Romero, Reliability Testing of F-111A Avionics Systems, Annals of Assurance Sciences, Proceedings of Annual Symposium on Reliability, No. 1 Volume 1, January 1968.

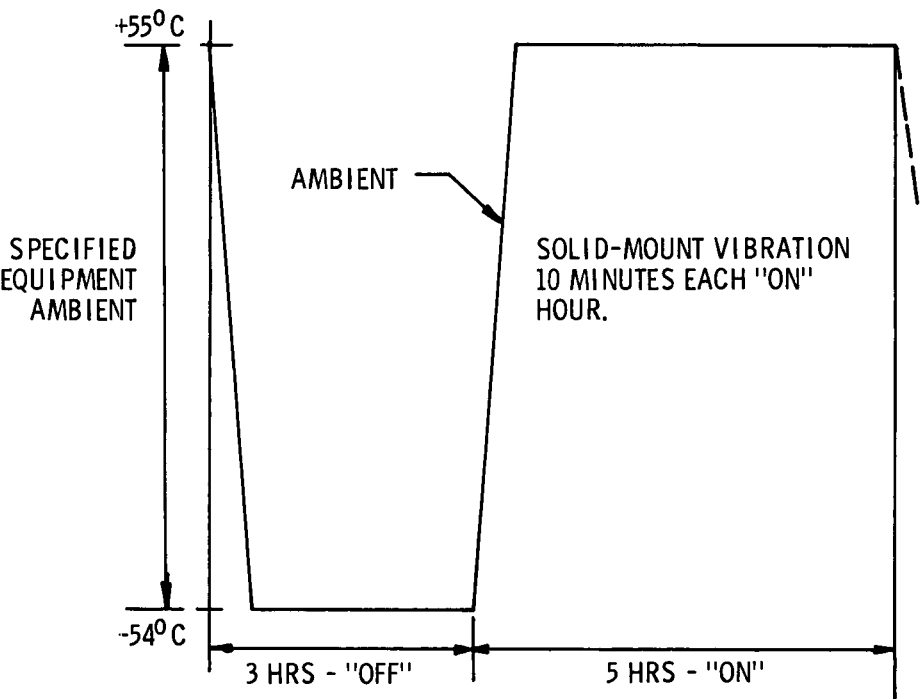


FIGURE 1. AGREE ENVIRONMENTAL PROFILE

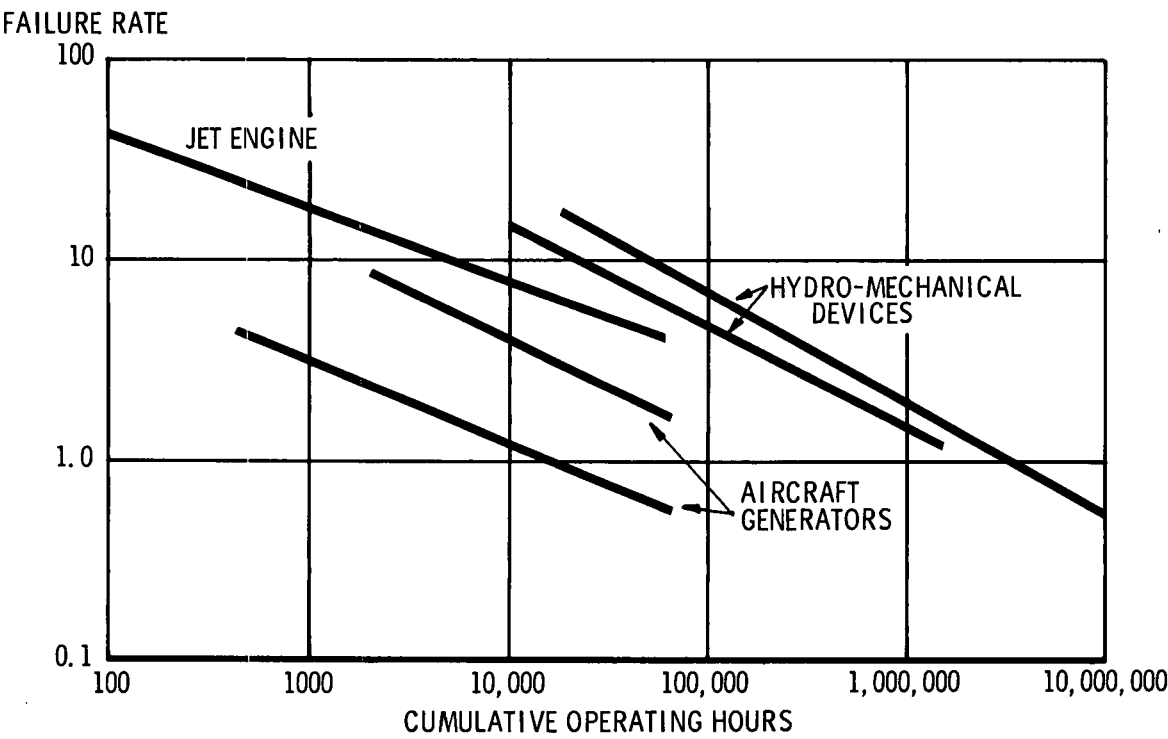


FIGURE 2. DUANE DATA

EQUIPMENT	NEW OR MOD	REQ'D MTBF	MEAS INIT DEMO HRS	% OF REQMT	SERIAL NO. COMPLYING WITH REQUIREMENTS											
					ROUTE			PRODUCTION								
					10	20		20	40	60	80	100	120			
FLIGHT CONTROL COMPUTER	N	300	25	8												
FORWARD LOOKING RADAR	N	134	11	8												
CENTRAL COMPUTER	N	560	32	5												
BOMB/NAV SET	N	243	8	3												
ECM RECEIVER	N	152	18	12												
AVOIDANCE RADAR	MOD	108	34	35												
LEAD COMPUTING OPTICAL SIGHT	MOD	300	85	28												
COUNTERMEASURES	N	150	25	16												
ALTIMETER	MOD	500														

GE COMPANY

FIGURE 3. RELIABILITY GROWTH

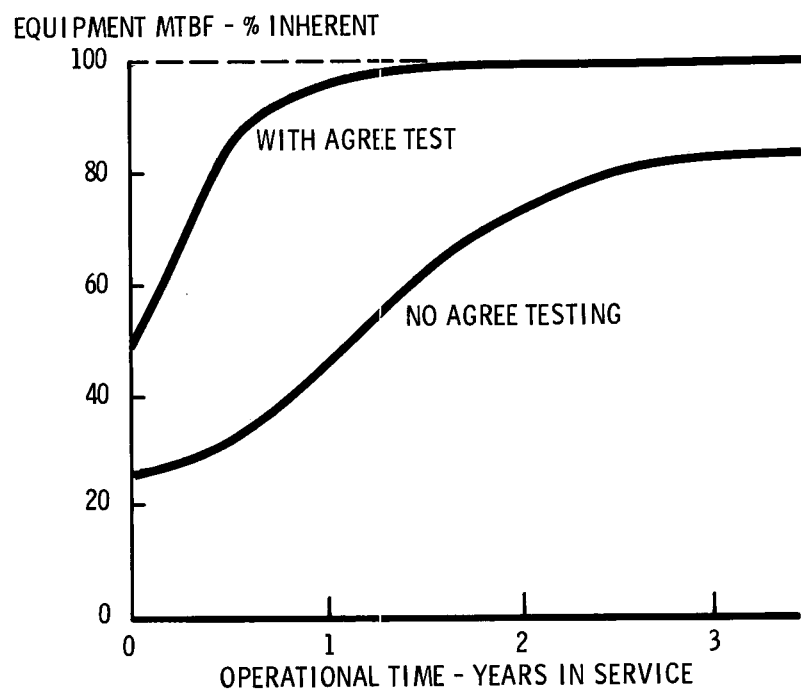


FIGURE 4. RELIABILITY GROWTH CURVES

MEASURED MTBF - HOURS

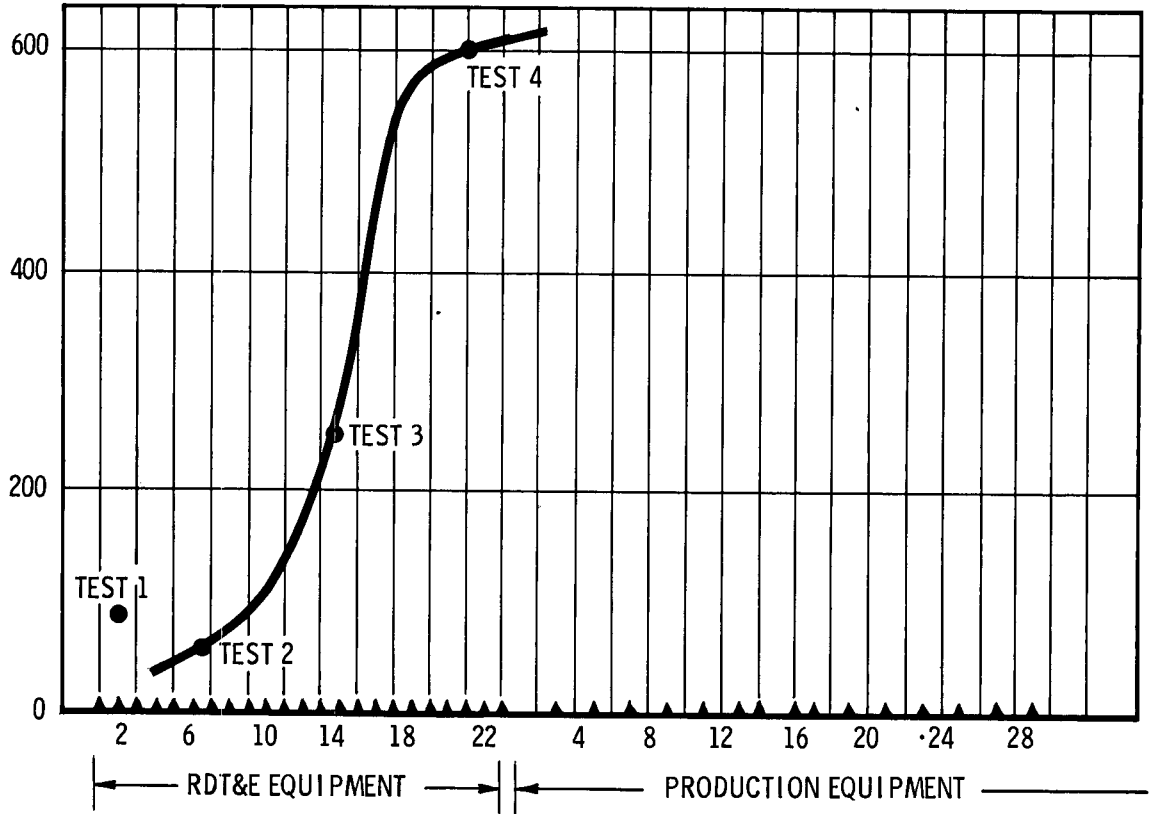


FIGURE 5. EQUIPMENT "A" RELIABILITY GROWTH

MEASURED MTBF - HOURS

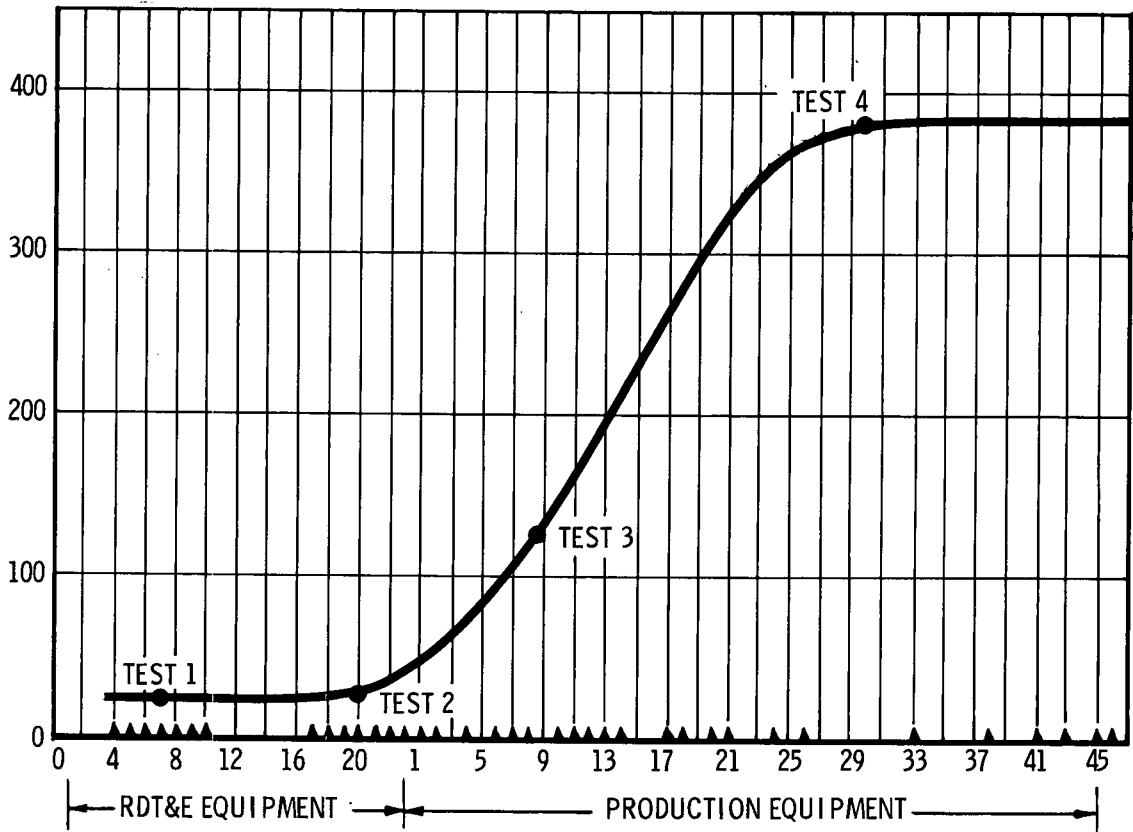


FIGURE 6. EQUIPMENT "B" RELIABILITY GROWTH

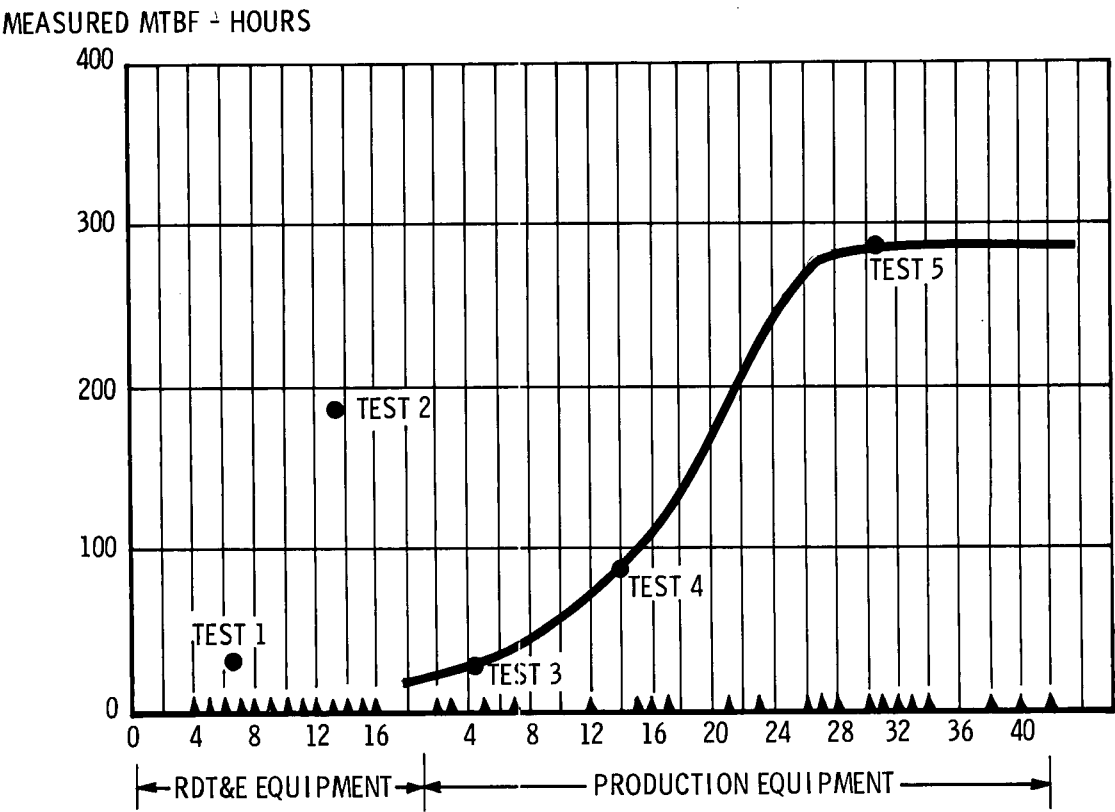


FIGURE 7. EQUIPMENT "C" RELIABILITY GROWTH

EFFECTIVENESS OF RELIABILITY PROGRAM ELEMENTS

W. T. SUMERLIN
Manager, Engineering Reliability
McDonnell Aircraft Company
P.O. Box 516
St. Louis, Missouri 63166, U.S.A.

SUMMARY

In most instances funding limitations place great importance on an understanding of the relative cost versus value achieved of the various elements of a reliability program. When that part of the customer's organization which establishes technical requirements is considerably separated from the funding source, functional requirements embroidered with reliability requirements often seem incompatible with available funds. Selectively choosing those reliability efforts which yield the most for the money then becomes extremely important. Apportioning available funds to subcontractors, to in-house reliability staffing, to computer operations and elsewhere must be performed wisely. An opinion is given of the probable relative importance of reliability program elements including reliability requirement evaluation and allocation, proof of attainment, parts control, design surveillance, failure analysis and design correction, and reliability progress measurement.

INTRODUCTION

Reliability programs for avionic equipment development will be examined with respect to the program elements which form such programs. Each element will be studied for its contribution to the attainment of required reliability versus its relative cost of inclusion in the reliability program. It will be assumed that a typical program includes a number of avionic items developed under subcontract and delivered to a prime contractor who integrates these avionic items into an aircraft avionic system. In this situation each subcontractor may be required to establish a separate reliability program for his avionic development, and the prime contractor also has a reliability program for his overall task. Because the subcontractor will most likely continue to be responsible for adequate demonstrated reliability after delivery of his equipment to the prime contractor for installation, and this in spite of his demonstrated compliance with a reliability requirement by test in his own plant, elements of the subcontractor's reliability program will first be considered, and thereafter elements of the prime contractor's reliability program. It is intended that such treatment will provide insight to maximizing reliability program cost effectiveness for both a subcontractor and for a prime contractor.

Preliminary to looking closely at what might constitute an avionic reliability program, some very important events must take place. First of all, reliability must be identified as a worthy problem very early in the development program and typically in the initial design phase. This problem must then be thoroughly studied and completely understood if reliability requirements are to successfully compete with the requirements imposed by all other design disciplines. By determining the flexibility or the rigidity of the reliability requirement, various basic design approaches and the probability of achievement of each can be reviewed. The magnitude of the reliability problem can be assessed and a sound allocation of funds for reliability effort may be made. Once a probable budget for a reliability program is identified then every effort can be made to select program elements which optimize the probability of desired reliability attainment within the funds available. Reliability program activity requiring funding will be divided into three categories herewith: (1) subcontractor reliability activity; (2) prime contractor reliability staffing and activity; and (3) reliability activity accomplished by the prime contractor's design staff directly, including the cost of computer facilities employed for reliability program benefit.

SUBCONTRACTOR REQUIREMENTS

While the reader might logically expect a reliability task to lead the activities of importance to hardware reliability during avionic development, such is not the case. Instead several more basic tasks are believed more significant. The following functions are listed in the author's opinion of descending order of importance:

1. Acceptance test requirements, adequate test procedures, and acceptable performance definition are first, as this collection of program elements establishes the base line for functional performance so that failure can be defined.
2. Qualification test requirements, procedures, and acceptable performance definition are second, as they establish proper functioning under all extreme conditions.
3. Adequate policy with respect to retesting (e.g. because of prior failure to meet test performance requirements), scheduling thereof and financial responsibility therefore is next because without explicit understanding as to the course which must be followed when an acceptance or qualification test is failed the risk of compromise is intolerable.

The above three items are not usually considered as part of the reliability activity and are not imposed because of difficult reliability requirements. Any special costs associated with these three items would likely not be chargeable to reliability. Nevertheless, their prime importance to reliability places them at the top of the list for surveillance by reliability program personnel.

Continuing in descending order of importance:

4. Requirements for reporting all functional failures suffered by any item of developed functional hardware, together with inclusion of ample details to permit analysis when the cause is not unmistakably apparent is fourth. In addition, requirements are needed relative to prohibition of

pattern failures. The occurrence of a second repetitive failure indicates that failure remedy for the initial failure is inadequate and not only must better corrective remedy be found, but the procedure to accomplish this must be strengthened. As a final addition to the failure reporting program, suitable, appropriate, and effective corrective action should be instituted immediately upon identification of each failure reported. It is often found essential to require that a subcontractor employ appropriate and adequate facilities in a failure analysis laboratory if he is to always adequately understand why the failure occurred. Requirements for at least temporary identification and preservation of failure specimens, and approval and dissemination of reports and documentation must also be established.

5. Requirements should be established for adequate and thorough reporting of all tests, together with requirements for approval (and resubmission as necessary) of test reports. Only through such reporting can a complete picture of the circumstances relative to reliability observations (observed failures) be obtained. With no other reliability program elements imposed, this much reporting is capable of giving indication of poor reliability in time to intercede in the delivery of an unsatisfactory subcontract item.
6. A policy should be adopted in the writing of subcontracts such that a significant portion of development funding, say 20 percent, is withheld by the prime contractor from payment to the subcontractor until the important testing has been satisfactorily accomplished, including the backfitting of any needed design changes into all units already delivered. It has been found that a financial incentive is often the only really useful means to persuade a subcontractor to pursue to a satisfactory conclusion qualification testing (and reliability testing) with reasonable dispatch. If the withheld funding is not adequately large, and if he is able, he may not really become concerned with adverse test outcome (and need for design correction and repeat testing) until the very end of the program, especially if he believes he will be ultimately excused from one or more difficult requirements and therefore will have reduced expensive backfitting to perform on delivered units.

While items 4 and 5 above require a subcontractor to assign personnel on a permanent basis to these functions and therefore permit identity with a portion of the subcontract development cost, the requirement for test reporting is customary, and failure reporting is rapidly becoming equally prevalent. When soundly organized, failure reporting can be handled at extremely low relative cost and failure summaries can be inexpensively compiled by digital computer. Thus so far, the above reliability program elements should not have significantly increased subcontract cost, yet they have provided basic structure of inestimable value to subcontract procurement of avionics if it is to have a quantitative reliability requirement.

Continuing:

7. Quantitative reliability requirement. There is some question and varied opinion as to the value of a quantitative reliability requirement unless a verification requirement is also included. The capability of and the acceptance of responsibility by the subcontractor undoubtedly can impute some value to a quantitative requirement without a demonstration test. In any case, the verification requirement can only be discussed if a reliability requirement is imposed, and it will be found as item 10 below. An important factor for consideration in levying a reliability requirement is whether the subcontractor's requirement should be stiffer than the prime contractor's need or whether it should be the same. If it were certain that the subcontractor would meet his requirement, and if no additional reliability were later needed to compensate for reliability deficiencies elsewhere in the overall developed system, then there would be no need to impose any stiffer requirement on a subcontractor than the reliability allocated by the prime contractor to the subcontractor's portion of the overall system. However, circumstances are seldom so satisfactory that the safety factor is not desirable. Historically, most equipment designs grow in complexity between onset of development and time for test, with a resulting tendency to decrease in reliability. Also, there is always some chance of adverse outcome from the reliability test because of the inherent producers risk present in all statistical sampling tests. It is usual to determine the probable difficulty a subcontractor may likely have in meeting a given requirement, and where difficulty is expected to be great, to minimize the added stiffening and the safety factor it provides. In a large system with many subcontracted portions, it is reasonable to require those subcontractors with least development difficulty and who are not being asked to push outward the reliability state-of-the-art to meet a quantitative requirement half again or twice the allocated mean-time-between-failures. Later in the program as difficulties develop, requirements can be readjusted downward if circumstances demand and safety factor permits.
8. Failure Mode and Effect Analysis. A requirement for an FMEA prepared by the subcontractor and submitted very early in his development effort should always rank high on the priority list, and in fact ideally following a requirement for quantitative reliability. The FMEA when properly and adequately performed in accordance with standard procedure will force the subcontractor to face up to a significant portion of the failure probabilities that will be designed into his product. True enough, the FMEA will not provide much insight to poor workmanship failures, or those caused by maintainability or personnel shortcomings, but it is a first-class means to get basic design consideration for eliminating single point failures, providing redundancies, derating, safety factors, and performance margins for transients, external failures, electromagnetic interference, etc. The subcontractor should be required to submit the completed FMEA for prime contractor approval, with resubmittals if at first unsatisfactory. The FMEA can be updated later in development if in insufficient detail for appropriate thoroughness when first submitted.
9. Design reviews should be required of the subcontractor. For a reasonably complex development, it may be desirable to require and schedule a formal preliminary design review, one or more formal intermediate design reviews, and a formal final critical design review. These meetings between working level subcontractor engineering personnel and prime contractor technical management are the principal means for two-way communication about development progress and developing problems. While need for formality is justified in order to provide an official record of status, formality should be minimized in the hope that technical problems will not be driven underground. These

reviews give opportunity to confirm and verify claimed accomplishment with supplementary data, and to remove misinterpretations and misunderstandings.

Item 7 above, the reliability requirement, may well have a cost impact on the overall price of the subcontracted development. When such an impact becomes too severe, one wonders just what reliability might have prevailed in the subcontracted product if no requirement had been specified. The risks associated with an unverified definitive reliability requirement will seem bigger, but then without a requirement for demonstration (which would take place late in development) there may be ample room to contend that the requirement has been met, unless of course reliability is hopelessly low. Costs associated with items 8 and 9 if significant should be pretty much in direct proportion to these items' value to the subcontract. All together the first 9 items will not often be found to be large cost adders.

Continuing:

10. Reliability Demonstration Test. Any observational means for quantitative verification of reliability will be cost significant for two reasons. First, the test itself involves use of facilities and services of personnel. Secondly, such a requirement involves risk of failure which means risk of added efforts and cost. Demonstration test costs can be held down. With austerity the subcontractor can be asked to propose a method of reliability verification by test, and with his proposal as a starting point, a set of least expensive test requirements can be established by negotiation prior to the award of subcontract. Requirement should be included for subcontractor preparation of reliability demonstration test procedure to be approved by the prime contractor well in advance of the scheduled test. If the subcontractor is inexperienced with reliability testing, special effort should be made to determine that he fully understands all test requirements, procedures and techniques. The cost of reliability demonstration testing is proportionate to the level of confidence in achieved reliability that it provides, and if the subcontractor's reliability requirement is somewhat stiffer than actually needed, less confidence from demonstration testing is needed. The cost of reliability testing is also somewhat proportionate to the magnitude of the mean-time-between-failures being verified. Thus, it is most economical to test as large an assemblage of functioning and interconnected avionic equipment as practical in order to reduce the MTBF test requirement to the lowest allowable value for the test. However, this savings seldom justifies deferring reliability test of complex equipment until after subcontractor delivery.
11. Progress measurement and delinquency penalty. If a subcontractor faces a demonstration test to prove that his product can meet a reliability requirement, it becomes quite important to devise means for assessing his probability of passing the demonstration test early in his development program so that he can have maximum opportunity to improve reliability if need is indicated. As the demonstration test draws near, means for anticipating test outcome should improve in precision. History is filled with cases where a subcontractor reached the day his reliability test was to begin with apparent great hope and expectation, only to find after a very brief interval of testing that his product was hopelessly below reliability requirement. In such cases no successful effort was made to measure reliability progress. Means must be devised to know with relative surety before beginning a reliability test that the test will be passed. From the moment that functioning hardware comes into being early in development onward, failures can be observed, monitored, and combined with estimates of operating time to calculate probable reliability. While such observations do not permit must resolution of high MTBF's, they give strong indication of low MTBF's, such as those indicative of gross reliability deficiency. Increasing evidence of inadequate reliability as time draws near for reliability demonstration testing can be the basis for imposing delinquency penalties by the prime contractor. Sometimes these are prescribed in the form of increased percentage of withholding of progress payments when earlier scheduled tests such as qualification tests, environmental tests, etc., reveal high failure rates.

Item 10 can and often will result in subcontract cost increase, but this has already been discussed under item 10. Item 11 may appear to the subcontractor to increase risks to himself and he may attempt to adjust costs upward because of this. However, in reality it does not increase his risks and really only formalizes a technique which he should use to advise himself as to the success of his development efforts.

12. Requirement for establishment and identification of a subcontractor reliability organization. If a subcontractor already faces requirements for demonstrating a quantitative reliability requirement and providing formal failure reporting and analysis he must adequately staff these functions to meet the schedule. Thus he probably has costed these efforts already. If so, the requirement of item 12, herewith, is only adding a need for visibility; identification of who has been assigned these tasks. Nevertheless, this requirement with the identification and visibility it provides will often seem greater justification for added scope and cost of subcontract than the work and cost actually imposed by the previous items. At this point in the list of subcontractor reliability program elements, the need for a reliability organization is inescapable. Since it must share in the design effort in a very flexible manner with engineering design, it is common practice to expect the reliability organization to be part of engineering, and in any case, have adequate status and recognition in the eyes of engineering and the designer. Lower caliber personnel assigned to reliability than assigned to design seldom is satisfactory. The means to constructively criticize complex design and offer acceptable suggestions require that reliability personnel have useful design capability, cooperative personality, and willingness to allow credit and acclaim to remain with the design staff.
13. Reliability Program Requirement. If a subcontractor identifies a reliability organization assigned to his development program, it is reasonable to ask him in the initial negotiations to propose a reliability program. His proposal should confine itself to well justified, useful, and cost efficient efforts. In fact, it can be adjusted to cover exactly those of the items herewith that are considered justified in view of related program requirements. It will permit the subcontractor to identify his cost of reliability so that he may consider special cost additions to the subcontract. If reliability program requirements are handled at the initial subcontract negotiation stage when competition still exists, the costs can be minimized.

14. Reliability Allocations and Mathematical Modeling. The first thing usually thought of when considering reliability programs, is the means to estimate or predict the quantitative reliability to be expected from the ultimate design. Thus the subcontractor should construct a mathematical model of the proposed design, and with the aid of this model allocate the unreliability permitted by his reliability requirement to appropriate portions of his design. Thus with established reliability requirements for each of the subdivided portions of his design he could consider the ease or difficulty in meeting these requirements with the piece parts, assemblies and design techniques available. If he finds that his initial choice of allocations imposes overly severe requirements on certain portions of the design, he will be at liberty to make a more equitable apportionment.
15. Reliability Prediction/Estimate. With or without a reliability allocation, the subcontractor's reliability staff can make reliability estimates based on the expected failure rates of the electronic piece parts to be selected for each development unit. Reliability estimating techniques today permit quite useful estimating accuracy, as has been discussed in a previous paper. With valid estimates of electrical and environmental stress, and appropriate selection of standard parts, failure rates can be obtained from published handbooks, summed, and an estimate of the overall reliability of the subcontract equipment obtained.

Items 12 through 15 are more apt to be considered collectively with regard to subcontract cost. The requirements of these four items are regularly contained in requests for bid on avionic subcontracts at present, and the magnitude of the added cost they impose is usually inconsequential, especially when compared with the costs of items 7 and 10.

Continuing:

16. Development Testing Requirements. The overall test program during development interfaces not only with reliability but with nearly every other development engineering discipline. Fortunately while demonstrating design integrity it can provide significant data inputs to reliability evaluation. This facet has been covered in item 11 above. In addition to reliability evaluation, well chosen development tests can establish that the design provides compatibility of one subsystem with another, that it is capable of meeting and performing under the environmental extremes of not only ultimate use but as imposed by the reliability demonstration test which may be worse, and that it is actually ready to be subjected to qualification and reliability demonstration tests. Overstress testing during development may be the only opportunity to truly identify the existence of essential design margins which will be needed to achieve the low piece part failure rates demanded by high-reliability complex-equipment development. Even more important than any of these factors is the opportunity presented during development testing to compare failure frequencies of localized portions of the design under various imposed environments to failure rates calculated during reliability estimating and prediction. Higher-than-estimated failure frequencies during any of this early testing should become the basis for extensive analysis to determine if failure rates used for reliability estimates and predictions are wrong and difficulty in demonstration can be expected, or if the design is inadequate and must be remedied. Because of this opportunity, later gross discrepancies between failure rates in reliability demonstration tests and those predicted are indicative of not only a deficient design staff but a deficient reliability staff as well.
17. Requirement for Parts Control. Selection, application, procurement, and screening of parts ranks hand in hand with circuit design as the most important controlling factor of complex avionic reliability. Many subcontractors who are both experienced and successful in developing avionic equipment at the limit of the reliability state-of-the-art do not need to be told by a prime contractor how to pick and choose parts. On the other hand, competition (and other factors) so restrict the flow of information concerning this process that it becomes essential to spell out parts programs in critical procurement documentation. Outcomes from preliminary reliability estimates can usually identify any need for high reliability parts. Requirements that justify such parts simultaneously for several subcontractors, probably justify a collective approach to a parts program for all subcontractors, sometimes identified as a Parts Control Board, and made up of representatives from each subcontractor and controlled by the prime contractor. Under such a program it is customary to intelligently establish timetables for each subcontractor so that he selects, designs for, procures, and employs all desired parts on time in accordance with a rigid development schedule. Non-standard parts require approval, and the granting of approval can benefit from the collective experience of all subcontractors. Needs and means for parts screening, burn-in, and other special requirements can be thoroughly explored with all subcontractors, and on occasion joint needs can provide a net benefit for all. The by far largest and principal source of equipment failure and attendant low reliability is parts failure, most of which can be avoided for a reasonable cost.
18. Reliability Training Requirements. Unfortunately very frequently it is found that both management and engineering design personnel think of reliability as a discipline involving unjustified use of statistics and inefficient application of low-skill personnel. They do not realize that the entire reliability job might be performed by and probably would benefit if it were performed by the designer. Unfortunately, a number of reliability techniques have evolved in recent years that are somewhat more time consuming than enjoyable for the designer, and separately identified engineering personnel can have the patience and tenacity to provide this capability to the designer's benefit. Depending on the appreciation of the reliability discipline already held by the subcontractor's management and engineering staff, it may be desirable to require that the subcontractor prepare a brief training program (for prime contractor approval) for exposition to a select list of subcontractor personnel. This requirement is not usually of significant expense.
19. Requirement for Worst Case Analyses. With the availability today of digital computers and suitable computer programs, it has become quite practical to require that a subcontractor perform worst case analyses on all his circuit designs to protect performance requirements against unfortunate tolerance accumulation. Such analyses should not only consider all combinations of circuit elements,

but should also consider all combinations of tolerances for adjacent interfaces, environment, transient generation, parts failure, trouble shooting, test, and repair. In fact the adequacy of such analyses will likely be indicated by the number of design changes needed thereafter to provide remedy to troubles that might have been identified during analysis.

20. Requirement for Sensitivity Analyses. For the same reasons that requirements for worst case analyses are now both reasonable and efficient today, requirements for sensitivity analyses are also worthy of consideration. The sensitivity analysis will permit study of performance degradation yielding crisp definitions of performance degradation failure and indication of related failure rates. The big problem with degradation failures has always been that reliability estimating with handbook failure rates does not permit adequate consideration of degradation failures.
21. Requirements for Additional Design Studies. Computer programming development has recently concentrated upon electronic circuit design. As a result there are now many computer programs that will perform various kinds of circuit analyses including: (1) d-c, a-c, and transient analyses of electrical networks; (2) linear system analysis by Laplace transform techniques; (3) d-c and a-c nominal, statistical and worst case circuit performance; (4) initial conditions and transient response of electronic circuits; and (5) circuit layout for microcircuit design.
22. Requirement for Equipment Environmental Burn-In. Burn-in is considered an important tool of the avionic manufacturing trade. It can be viewed as a debugging procedure employed to detect and remedy manufacturing discrepancies, workmanship, and installation errors which would prevent proper equipment operation and would cause abnormally high failure rates during early life. In addition to its ability to catch manufacturing induced faults, it will identify production process problems, defective parts and materials, and marginal design or critical interface problems. In reality it is a brute force method of accruing in the factory the operating time during which early failures tend to appear. By imposing environmental cycling during burn-in, it is possible to screen out an importantly large fraction of environmentally induced failures which may appear with disastrous results during a reliability demonstration test under extreme environment. Theoretically, it should be possible to screen parts to remove those with incipient failures, to control design and manufacturing to prevent undue early failures from related causes, and thus by available scientific means remove the early failure problem without recourse to burn-in. In some programs this appears to have been achieved. However, initial subcontract arrangements that provide for burn-in can always include options for later cancellation of burn-in requirement with attendant reduction in cost. The situation to avoid is the circumstance where a subcontractor by means of burn-in provisions which are extensive, attempts to acquire specified reliability by a fail-and-fix reliability growth process. Some subcontracts require that the final few hours of burn-in be failure free in the hope that this verifies the adequacy of the burn-in. However, if that sort of requirement is to be imposed on burn-in, it can be viewed more intelligently by considering that the failure free period is an all-equipment production reliability test, and risks and probabilities versus MTBF can be calculated.

Items 16 through 22 should be considered as requirements for those subcontracts where the reliability requirement is so imposing, either because it approaches the state-of-the-art, or because it exceeds the experience of the subcontractor, that added expense to achieve desired reliability is worthy of consideration. Obviously these items as well as the previous items can be more economically imposed on a subcontractor at the time of initial negotiations while he is motivated to compete with other subcontract sources. A requirement that separate items be separately costed sometimes reduces the cost, and of course it permits separate negotiation. The intelligent subcontractor, if faced with more detailed requirements than he feels are needed, will counter propose his preferred method of achieving high reliability. On the other hand he may be happy to be reminded of the existence of techniques that he has not previously practiced. More specifically, development testing (item 16) should be pursued as long as useful knowledge is gained. For estimating the magnitude of such testing beforehand, prior development experience is the principal insight. With respect to parts control (item 17), if many new or nonstandard parts are to be required, or very low failure rates are mandatory, then a parts control activity will be exceedingly useful and well worth its cost. Reliability training (item 18) should be provided to the correct extent. Too much training exposure is as bad or worse than too little exposure for management and design staffs forcefully required to attend training sessions. Judgment will have to be based on prior reliability experience. Design analyses (items 19, 20, and 21) are desirable to the extent that they yield unanticipated or otherwise unavailable design improvements. To some extent they are justified if only to provide confirmation of design adequacy without indication of needed change, but then the analyses would be abbreviated rather than extended. The value of burn-in and the need for such a requirement has been discussed in item 22.

23. Requirements for Production Reliability Tests. When there is concern that a subcontractor will unwittingly or otherwise let the reliability of his product slip from that initially attained and verified at the beginning of production, so that later produced units no longer have acceptable reliability, then it is worth considering a requirement that later production be reliability tested either on a sampling basis, or on an all-equipment basis. On a sampling basis it may be reasonable to require that enough equipments to permit a short test be drawn from each month's or alternate month's production and submitted to a reliability test similar to the initial reliability demonstration test except that it is usual to relax test requirements somewhat (accept greater risk). All-equipment tests for production reliability testing have been devised which are very similar to an extended environmental burn-in requirement, except that failures that occur become a criterion for continued acceptance or for halting production and requiring design remedy. It is usual to have requirements for production reliability tests separately priced, so that if production experience shows such testing no longer cost effective, further testing can be cancelled with a reduction in price.

To the extent that some or all of the above items are to be considered for a multiplicity of subcontracts, it becomes expedient to document in detail common requirements in a standard reference package which can be referenced as desired in individual purchase orders and subcontracts. Thus each subcontracted equipment is covered with respect to all common requirements (as well as its special requirements by its

individual procurement specification). The procurement specification refers to standard subsidiary specifications to a maximum possible extent, to special in-house created common documents for the remaining standard requirements, and to any specific or special requirements as needed. A common data submittal requirements specification for all subcontractors can be prepared. Likewise a specification on common subcontract management requirements can be prepared. Special agreements can be executed where last minute details must be settled.

PRIME CONTRACTOR RELIABILITY ACTIVITY

The reliability role of the prime contractor is quite apt to be somewhat different from that of the subcontractor, and it may be more difficult in some ways, easier in others. If the requirements imposed by the customer are difficult and must be passed on to the subcontractors without significant protection and safety factor for the prime contractor, then the latter may find himself uncomfortably at the mercy of some of his subcontractors. To the extent that he has been able to anticipate all eventualities and safeguard himself with contingency requirements in the terms of subcontracts, he may be protected. It is more usual to find that protection is not complete, and unexpected problems arise without simple recourse. In the discussion that follows, reliability program elements for the prime contractor are set forth in descending order of importance, but it must be recognized that there will need be a relationship between the number of elements judged necessary for a subcontractor and the number of elements which the prime contractor must correspondingly consider. The discussion will make reference to that already provided under similar subheadings for a subcontractor, and principally emphasize differences.

1. Foremost in importance is the need for careful study and complete understanding of the overall reliability requirement. It may be that the requirement exists solely in the form of a system MTBF to be averaged over extended field use, or a corresponding probability of mission success for a defined mission. The important consideration here is a knowledge of the field environment or range of environments, and the mission profile. Will field reliability be based on failures that have been carefully screened for relevancy, or will the failure count be contaminated with frequent invalid reports? In general, avionics equipment demonstrates a somewhat different reliability in every different use environment, such that not only are wide reliability variations found when installation is made in different models of aircraft, but also when like avionics is flown in identical aircraft in different locales, or even in the same locale but under different mission requirements. If the reliability requirement is a composite figure composed of the reliabilities of a number of equipments and subsystems in the aircraft, is there adequate understanding of different operational cycles for different equipments, different operating periods for ground checking, different failure criteria? Most important is the question of how rigid the requirement is and what will be the outcome if the requirement is not quite met. It has been found in reviewing circumstances when an aircraft requirement is not met, that a great quantity of data and data evaluation is needed to finally agree on just what reliability is demonstrated in the field. Much of this problem can be eliminated if explicit methods of precise evaluation are specified, but usually this yields a synthetic figure that is not particularly useful in determining the true worth of the reliability program. In any case, the desired understanding should be achieved before final contractual commitments are made.
2. Planning and funding a reliability program is the next most important element to the prime contractor, and it is possible to begin this process as soon as an opinion of the reliability requirement is formulated. At one extreme is the unlikely case where a contractor is able to pass essentially all of the risk and worry on to one or more subcontractors, and is willing to trust them without providing close surveillance. At the other extreme is the prime contractor who has so comprehensive a reliability program that he is able to step in when subcontractors exhibit deficiency even to the extent of changing subcontractors, with minimal reliability risk, and to rest assured that schedules will be met, costs will be held within budget, performance will meet requirements, and all reliability requirements will be suitably verified. In the more typical situation, the bulk of reliability risk is shouldered by subcontractors, whose subcontracts are controlled by the prime contractor's design staff and they in turn are advised by the reliability staff. The reliability staff is organized with adequate stature to be recognized by both design and management, and with sufficient personnel to carry out all of the tasks (herein described) that are considered essential and within the available funding.
3. The prime contractor must apportion reliability requirements among all the subsystems (including those subcontracted) that make up his end product (e.g. aircraft), and he must do so in such a way that the end product can meet its reliability requirement if all the apportionments are met. Further he must be ready to redistribute his apportionments in case it become apparent that one of the subsystems will not likely come up to expectations, and he must keep readjusting apportionments throughout development to keep risks minimal and equitably distributed. To perform these apportionments for complex systems he will need a mathematical model for continuous calculation of end product reliability in terms of all readjusted subsystem reliabilities. The extent to which this mathematical model simulates all subsystem interrelationships will be dependent on the needed accuracy of the overall reliability figure and the allowable discrepancy between subsystem requirements and overall system requirement. It is not unusual to require a mathematical model of such complexity that calculations are by a programmed digital computer, and adjustments and recalculations are performed frequently throughout the life of the development.
4. Subsystem reliability estimates or predictions are next in importance. The prime contractor's prior experience will permit him to make preliminary estimates using gross or rapid estimating techniques. The greater detail of a subcontractor's proposal prior to award of subcontract should greatly assist and expedite a rapid verification. The early estimating must show reasonable conformance with reliability allocation, and if the estimated reliability is not sufficient for the allocation, design approaches have to be altered while there is still time to do so economically. Above all, the prime contractor must rapidly develop confidence in the reliability estimate for each and every subsystem whether it be subcontracted or developed in-house. Subcontractor's estimates should be studied carefully and complete understanding and agreement should be reached as regards to the failure rates chosen for calculations, the contingency

allowances made, and general validity of the estimate. Each estimate should be updated as often as necessary to properly reflect suitable resolution of the reliability to be expected from each subsystem following design changes, during test, and later in field use.

5. Identification of reliability-critical subsystems and equipment and the establishment of special programs as added reliability protection is next in importance, and of considerable consequence in planning the needed reliability staffing which will be discussed next. Any not yet developed subsystem or equipment which will require reliability at or beyond the state-of-the-art is likely to be critical. Average part reliability as much as an order of magnitude (ten times) greater than customarily achievable is crowding the state-of-the-art. Likewise, any development in need of a not already developed critical piece part or special function is a good candidate for a critical label. Development within the state-of-the-art but requiring adherence to schedules that do not permit thorough analysis and test, and/or that require release to production prior to satisfactory completion of qualification testing may also deserve critical identity. Finally, any item requiring reliability growth to achieve its allocated reliability will likely be critical. The general purpose of identifying critical subsystems and equipment is to permit special emphasis on frequent reliability evaluation, fast problem resolution, and perhaps second source consideration. Prime contractor reliability effort may be required in large measure for subcontracted critical items as compared to less critical other portions of the overall system.

The five items just enumerated require initial reliability effort early in the development program, but in general do not in themselves require the support of a sizable reliability staff. However, they provide some of the basic background which influences plans for reliability staffing. In general, if reliability needs do not require consideration of all or more than the above five items, a reliability staff as such is probably not justified.

6. The reliability staff will function most efficiently if it is part of engineering and able to be closely integrated with engineering design. A design background is very valuable to a reliability engineer and is much more difficult to come by than special reliability mathematics. Hence, giving reliability assignments along with reliability instruction to design personnel can be very efficient reliability staff training provided they do not have prior vested interest in the designs which they must criticize. Means to add to the reliability staff as the level of effort expands is more desirable than to start with a large staff and create needless reliability work to keep the staff busy early in the program. In general it has been found that aircraft development and avionic development are most efficiently supported by a reliability staff numbering three to five percent of the total engineering design staff assigned.
7. Reliability training should be considered for those engineering and management personnel who will come into contact with the reliability staff if there is any question as to the need for reliability and reliability effort. This training or indoctrination can be as brief as an hour or two lecture presented under conditions of high credibility to key engineering and management supervision. Conversely, it can be a tutorial series of many lectures and class recitation if there is a willing and enthusiastic audience who will actually make use of what they learn. The need for some understanding of reliability by all personnel involved in development is so essential as to justify some educational exposure unless prior work assignments have already provided the training, understanding, and appreciation.
8. Reliability visibility for management by means of direct communication channels is next in importance. Communication via staff meetings where oral explanation can be extensive if desired is so valuable that the highest ranking reliability personnel should be a regular part of periodic management meetings and progress reporting. By these means, reliability problems of critical importance can be simultaneously brought to the attention of all supervision, and special cooperation and management support expeditiously obtained.
9. Document review and approval by the reliability staff must be established. With respect to subcontracted avionics, this function extends all the way from approving requirements documents (e.g. specifications) for all subsystems and equipment with a reliability requirement, constructively assessing all responding subcontractor proposals, to approving all subcontractor proposed reliability programs, test procedures, failure analyses, trade studies, and submitted reliability data. For in-house development assigned responsibility should permit similarly passing judgment on all prime contractor documentation that can or will affect reliability.
10. Failure reporting, failure analysis especially in a failure analysis laboratory with adequate facilities when necessary to correctly define the true cause of failure, appropriate corrective action to eliminate failure repetitions, and periodic summary documentation for project visibility is next in importance. Failure reporting forms preprinted with all the desired identifications for the information needed are most desirable, and often these forms can be combined with those for the control and review of discrepant material by the inspection and quality functions. The opportunity for a reliability-responsible engineer to judge if a failure analysis is needed in each instance of reported failure is vital. Appropriate analyses which identify the true mechanism of failure frequently indicate need for further design review, analysis, and study, with ultimate design change to eliminate entire categories of failure. Corrective action in the absence of knowledge of basic failure cause is of little value. An adequate failure analysis laboratory on the prime contractor's premises permits detailed sleuthing as to failure cause before anyone can do away with the corpus delicti and camouflage design weakness. Failures that are the responsibility of a subcontractor can be analyzed for cause by subcontractor personnel in the prime contractor's laboratory where complete visibility of the course of the investigation is possible. Such a laboratory should include facilities for 3-dimensional x-ray, dissection and microscopic examination of solid state devices, chemical and metallurgical analyses facilities and usual test and measuring equipment.

11. Qualification testing is a vital ingredient in any development program. As previously noted, it is considered second in importance only to acceptance testing when it comes to establishing sub-contract requirements. Accordingly the reliability staff should give sufficient priority to conducting review of and approving qualification test plans and procedures regardless of whether such testing is to be performed by a subcontractor or by the prime contractor. In fact, consideration should be given to having the reliability staff witness final qualification tests wherever conducted. Suitable qualification tests will soundly establish the capability of the tested sub-system or equipment to at least initially function properly under both use and test environments. Any critical need to perform qualification test in complex environments that simultaneously combine extremes or working levels of temperature, altitude, humidity, and vibration should be recognized, and such tests scheduled to be completed prior to the start of any reliability demonstration test. It is desirable to have the reliability staff familiar with the qualification test set-up in order to anticipate the capability of the tested item to withstand the environment, including operational cycling, to be encountered during the reliability test.
12. Reliability testing poses quite a load on the reliability staff, sometimes doubling the staffing requirement during test phases. Regardless of where such tests are to be conducted, all reliability test plans and procedures must be studied and approved to increase the likelihood that difficulties are anticipated and the necessary effort correctly estimated. Agreement must be reached on just what will constitute a relevant failure (as opposed to an uncounted non-relevant failure). When a failure occurs during tests prior decision must have been made as to what procedure will be followed with regard to removing the failed unit from test while allowing properly performing remaining units to continue test. Procedure for repair of the failed item to return it to its original operative conditions, or better (e.g. improved so that such a failure is not likely to repeat), and decision as to what criterion will be used to justify starting the test over, either when a reject decision occurs or when the outlook is poor and design improvement available, must be established beforehand. Practically speaking, past experience with reliability demonstration testing is the best insurance for anticipation and adequate precautions and for conducting the most efficient test under prevailing circumstances. Because of the need for frequent interpretation of rules and agreements in the presence of adversities, it is usually well to plan to have reliability demonstration tests continuously witnessed by the reliability staff. If such witnessing is initiated at the beginning of the test and the test goes well, a reduction of witnessing can be permitted to conserve limited funds and meager budgets.
13. Development testing plans should be reviewed by the reliability staff if the reliability budget permits. Development programs which push the reliability state-of-the-art, or are expected to yield very complex hardware with sophisticated functional requirements, should plan a sufficient quantity of development testing to indicate functional capability under later reliability test conditions. A knowledge by the reliability staff of the extent and limitations of development testing will give beneficial insight to reliability problems that have not been headed off and may develop later.
14. Next in importance is the establishment of a means for continuous or periodic evaluation of the probable reliability to be achieved. Even as early as initial development testing insight can be gained as to possible unacceptable reliability of a new, special, or unevaluated piece part which may seem irreplaceable because of unusual design dependence. Special emergency programs for evaluation of alternate choices can then be instituted early enough to have some chance of being effective. The penalty of delay in conducting a suitable initial thermal survey will be obvious to the reliability staff which has development testing under surveillance, and more emphasis can then be placed on the critical importance of an early thermal survey. Once engineering models of representative configuration come into existence, operating time and failure observations can be collected to permit early (if crude) assessments of MTEF. From this point onward, diligent collecting of failure and operating time data should yield ever-improving indications of achieved reliability. After initial design release, continued observation will provide indication of the reliability growth caused by redesign or by the "fail and fix" cycling so often practiced. Even after reliability demonstration test has begun but not yet resulted in acceptance, data monitoring can help with correct anticipation of test outcome. Continued monitoring of data will provide indication of the reliability to be expected in the field. To the extent this data collection and assessment process can be automated, it can be included without overburden to the reliability budget. A completely manual data processing operation if thorough will probably be uneconomical.
15. The reliability program (including those of every subcontractor) should be reviewed every quarter and a status report issued to advise both management and the customer of the benefits obtained therefrom. Somewhat less frequently it may be desirable to consider modifications and alterations to the reliability program plan to provide such streamlining as may be possible after major difficulties have been surmounted and to recognize the need for special efforts.

RELIABILITY ACTIVITY BY THE DESIGN STAFF

A number of reliability activities if carried out by the reliability staff must be pursued jointly with the design staff. When funding available to the reliability program is extremely limited, the functions which follow will be performed, if performed at all, by the design staff. With ample reliability funding reliability personnel will share the work. However, the design staff will in all cases retain both an interest and some participation. Thus, these activities are separately grouped to emphasize this flexibility.

The presentation herewith implies maximum support by the reliability staff but this can be reduced to zero by shifting all work to the design staff. The presentation herewith makes this emphasized grouping for the prime contractor reliability activity but it is to be understood that the identical tasks performed by a subcontractor have essentially the same flexibility. Because of this, paragraph numbering has been continued rather than started over.

16. In any development program with strong demands for high reliability, the benefits to be obtained from a Parts Control Board (PCB) should be seriously considered. The PCB permits all or many of

the subcontractors to share the load of choosing parts with appropriately high reliability. The yield from a PCB is not only an important benefit to high reliability but a significant benefit to parts standardization and complete specification, both of almost inestimable value to field servicing. In a typical program the PCB will consist of an identified parts specialist from each or a selected group of the subcontractors. These specialists will meet frequently at first, less often later, to agree on a preferred parts list from which all subcontractors must choose the parts they use. Approval to add to the preferred parts list or permission to deviate from the list is the final prerogative of the prime contractor. If the prime contractor includes his parts specialists as part of his reliability staff, then this staff must provide the essential representation at all PCB meetings, and he must provide the manpower to approve all submittals from subcontractors, as well as to suggest solutions to the more difficult problems when subcontractors need help. If the prime contractor's parts specialists are not part of the prime contractor's reliability staff, then the reliability staff can limit its support of the PCB to surveillance through nominal representation at PCB meetings, and availability for assistance as needed. This latter responsibility represents a level of effort insignificant as compared to the value of having a PCB.

17. The reliability staff should participate in design reviews. To the extent that the staff possesses design talent, and to the extent that budget permits, the reliability staff can be very effective in making detailed studies of pertinent portions of the design prior to and as homework for formal design reviews. Above all, it is important to remember that the reliability staff cannot afford to confine its design interest only to reliability questions. Instead there must be a diligent awareness of existing design difficulties of all sorts, proposed means for surmounting, probability of success, and alternatives remaining if success is not immediately achieved. A reliability staff has a wide choice as to the level of its effort in connection with design reviews.
18. The reliability staff should review all design trade studies performed. The well-staffed reliability program will undoubtedly make many trade studies of its own. Any trade study wherein the design approach trades other parameters against expected reliability can be of concern to the reliability staff, but such studies when of primary importance should be at least initially performed by the design staff which must develop faith in the approach to be followed. Tertiary trade studies can be made by the reliability staff when the design staff does not feel able to justify its further effort in pursuit of questionable benefits. Hopefully, all trade studies involving reliability should be pursued with close joint cooperation between reliability and design staffs.
19. The conduct of failure mode and effect analyses by the reliability staff has been left almost to the end of this listing, not because such analyses have low importance but because they should be made by the design staff with assistance from reliability personnel only as necessary. Then unexpected modes of failure will come to the attention of the designer through his own study, permitting him to find remedy, if such is possible, early in the design effort. If the design staff insists that failure mode and effect analyses be conducted by the reliability staff rather than by themselves, then it is essential that the reliability staff provide this service, but the work should be performed in very close conjunction with responsible designers. Once an analysis has been made, it must be updated when design changes are made. The source of effort for such updating can be selected for convenience provided adequate information is made available.
20. Design analyses can be of many types, and in some developments it will be more important to get appropriate analyses made than to worry about who makes them. It may be the lot of the reliability staff to make these analyses if the talent is present and the staffing budget permits. The kinds of analyses for consideration range all the way from parts application studies to circuit performance analysis by computer. Computer analyses can include those for worst case, sensitivity, drift, tolerance, electromagnetic interference, and others.

CONCLUSION

The foregoing has attempted to identify the many items of significance in a comprehensive reliability program for avionic development, with listing and comment in descending order of budgetary importance. Perhaps most significant of all to an avionic development program is the capability of the management, design, and the reliability staffs to recognize and understand the particular importance of each of these items. In any financial planning one must decide what is to be done, how much effort is required for each task, how much this effort will cost, and finally whether this cost is justified. Diligent planning of a reliability program, including staffing levels and budgetary costs, will all be valueless if program management does not believe the recommended work to be necessary. Experience may be the best teacher. This paper is intended not so much to educate the reader, but to remind him of some of his past experiences, and to invoke present consideration with full view of often forgotten past experience. In the long run no one should have to talk about reliability in order to achieve it. Really it is an element of comprehensive design excellence. To the extent that these reminders will lead to this end, then the paper will have achieved its purpose.

COST EFFECTIVENESS OF BUILT-IN TEST PROVISIONS

M. M. Tall

RCA

The continuing growth in both number of applications and the complexity of avionic equipment is posing problems in achieving required operational effectiveness of aircraft. As a result, a great deal of attention has been devoted to improving avionic reliability and the logistic support of these equipments. This attention has naturally turned to consideration of built-in test provisions (BIT) as a means of improving operational effectiveness.

Built-in test provisions, or BIT, is defined by MIL-STD-1309⁽¹⁾ as "Any device permanently mounted in the prime equipment and used for the express purpose of testing the prime equipment either individually or in association with external test equipment". BIT's primary purpose is to indicate to the user if the prime equipment is operating satisfactorily. As such, it provides information upon which a decision to abort, modify or continue a mission may be based. Of particular importance, is the application of BIT to passive devices since it may be the only indication of their state of readiness. In highly complex equipments, BIT may indicate degraded performance of portions of the equipment as well as catastrophic failure and indicate the use of alternate modes of operations.

As important as performance monitoring is to the conduct of a mission, the contribution to maintenance may well determine whether or not BIT is to be incorporated and, if so, to what degree. BIT can materially improve maintenance functions such as failure verification, fault isolation and equipment check-out. This improvement leads to more cost effective maintenance and to a reduction in turnaround time. From a cost point of view, the value of BIT may be assessed against the reduction in the cost of maintenance and its justification predicated on this basis alone. Thus this paper will deal primarily with the effect of BIT on maintenance.

The introduction of a complex equipment into the field requires review of all aspects of integrated logistics if the equipment is to be supported during its operational life at reasonable cost. An important aspect of integrated logistic support is the early establishment of a maintenance policy because of its effect on equipment design. For example, which maintenance actions will take place at the flight line and depot? What maintenance actions will take place - replacement or repair - and at which equipment level - unit, module or part? What skill levels are required? The impact of considerations such as these on equipment design and the cost of logistic support is evident.

To facilitate the establishment of a suitable maintenance policy, RCA developed a system of computer programs called CO-AMP, Cost Optimization and Analysis of Maintenance Policies.⁽²⁾ CO-AMP compares both prime equipment and support system alternatives on the yardstick of life cycle costs of ownership. This valuable tool provides data and supports analyses leading to better decisions in such areas as:

- Reliability requirements.

- Maintainability requirements.

- Equipment discard level.

- Degree of BIT incorporation.

- Package design.

- Maintenance capability at various support levels.

- Amount and location of spares.

- Replenishment procedures.

The logistic support alternatives which CO-AMP considers comprise 20 basic maintenance policies. Four support levels are considered: flight line, organization, intermediate and depot. It accommodates three levels of maintenance capability: Check-out at Unit Level (COU), Fault Isolation to Defective Module (FIM), Fault Isolation to Part (FIP). By using the CO-AMP programs, the designer may explore possible support options for various candidate designs including a variety of BIT configurations. It enables the designer to quickly determine the cost optimized combination of equipment design and maintenance support.

A matrix of the various maintenance policies is shown in Table 1. The four support levels are shown vertically. Equipment level is equivalent to flight line. It will be noted that at the flight line, maintenance actions are limited to equipment check-out (COU) and to replacement of a failed module (FIM). Higher support levels may involve replacement of a failed part on the module. Policies 1 and 2 discard the unit at failure, the only difference being that the decision to discard is either made at the flight line (Policy 1) or at the organizational level (Policy 2). In a like manner, Policies 3 through 8 repair units by module replacement and discard defective modules. Policies 9 through 20 repair modules and discard defective parts.

It is apparent that the decision to include BIT in a system design can have a major effect on the selection of the appropriate maintenance policy. The built-in ability to verify a malfunction, to isolate a failure to a given level and to replace at that level, and to check out the equipment affects the required skills and facilities at each support level. At the flight line, it determines whether the technician replaces the entire unit or a module.

BIT, of course, varies in complexity and thus in ability to fault isolate. For example, at the unit check-out level (COU), a suitable sensor at the end of the system to indicate the presence of an adequate output is a simple version of BIT. To isolate a failed module, additional sensors may be incorporated at various intermediate points in the circuitry. In the future, large scale integrated arrays (LSI) may have test circuits incorporated on each chip to assist in both performance monitoring and failure isolation.

Recent designs of complex systems provide for the monitoring of individual modules, many of which may incorporate a single circuit function. One such design concept provides a data acquisition unit for each group of modules (5-10). These units maintain performance status of a number of test points on each of the monitored modules. The data acquisition units may then transmit out-of-limit readings to a central computer or report such readings when interrogated periodically. Another system, involving digitized signals, provides for a test tone to be transmitted along with the other signals through the prime equipment.⁽³⁾ Variations in the phase shift of the test tone indicates equipment malfunction. This system provides essentially continuous monitoring of the prime system although the degree of added complexity may be considered objectionable in some cases. A more detailed example of the use of BIT on the AN/ARC-142 is shown in Appendix A.

BIT, whether its quite simple or rather complex, involves added circuitry and includes additional component parts, each with its own failure rate. As a result, the overall failure rate for a prime equipment with BIT can be expected to be greater than that for one without BIT. Well designed BIT provisions will employ high impedance, passive, low failure rate sensors so connected as to effectively decouple themselves upon failure with no adverse effect upon the prime system. BIT may improve the availability of the prime equipment by indicating imminent failure and by decreasing the turnaround time through improved maintenance.

In spite of the slight degradation in reliability, the use of BIT may yield an apparent gain in reliability by reducing the number of maintenance actions required. Maintenance histories reveal a large percentage of equipment removed from aircraft as a result of a trouble report which test good. Adequate performance monitoring through BIT should reduce the number of such unnecessary removals. For those equipments requiring repair, BIT materially assists in the fault isolation process. As a result, the probability of the correct maintenance action being taken is enhanced. Field data has indicated that as much as 30% of maintenance actions may be repeated because the malfunction had not been corrected during the initial action. BIT also tends to reduce trouble-shooting probing by maintenance technicians. Experience has also shown that extensive probing of equipment increases the possibility of damage and thus accelerates the occurrence of the next malfunction. Further, BIT, by reducing the number of maintenance actions and the time required for each maintenance action has a significant effect on turnaround time. Thus, the equipment performs more closely to its inherent reliability and availability.

BIT, by indicating the appropriate replacement, reduces the skills needed, particularly at the lower support levels. Part replacements, if desired, may be accomplished at the higher levels, such as base or depot.

However, from the maintenance point of view, the major contribution of BIT is in enhancing accurate troubleshooting and in reducing the time required for this function. Figure 1 shows the distribution of active repair times for the AN/ASB-4 equipment.⁽⁴⁾ It may be seen that malfunction verification, fault location and final test account for 62% of the active repair time. It is in these areas that BIT can have a major impact.

Let's examine the effect of BIT on maintenance costs. Assume that 500 avionic equipments are to be procured. Research, Development, Test and Evaluation (RDT&E) amounts to \$6 million. Production costs are \$200 thousand per unit for a total of \$100 million. Total acquisition costs are \$106 million. The inclusion of BIT adds 5 percent to RDT&E costs, or \$0.3 million, and 10 percent to production costs, or \$10 million, for a total of \$10.3 million.

Two reliability levels are considered. The first has standard reliability, with support costs of \$60 thousand per equipment per year for a total of \$300 million over the ten years. The second has high reliability with support costs of \$20 thousand per equipment per year for a ten year total of \$100 million.

It has been estimated that manpower costs amount to 50 percent of maintenance costs. Thus, for the standard reliability equipment, manpower costs \$150 million and for the high reliability equipment, \$50 million.

Assume conservatively that BIT reduces the time required for malfunction verification, fault isolation and equipment check-out by 50 percent. Since these factors account for 62 percent of maintenance time, a savings in time of 31 percent ($.5 \times .62$) is achieved. Time and manpower may not be directly relatable. For the sake of the example, assume that the time savings result in a 25 percent manpower savings. Thus for the standard reliability equipment, a net savings of \$27.2 million ($37.5 - 10.3$) results; for the high reliability equipment, we're close to breakeven, a net savings of \$2.2 million ($12.5 - 10.3$) is obtained. Table 2 summarizes these results.

The net savings noted are fairly conservative. Not considered in the example were the savings resulting from minimizing false removals, improper maintenance actions and maintenance damage. Further, the advantages of performance monitoring are not included. One may argue with the specific values employed in the example, feeling that the cost of BIT was understated or that the savings were overstated. However, the cost effectiveness of BIT, when considered from the maintenance point of view, cannot be disputed.

Despite its cost effectiveness, BIT is still a controversial subject among equipment designers and users. Some resist the inclusion of any extra circuitry with a passion. Others desire to incorporate BIT to a degree that would rival the prime equipment in complexity. Fortunately, the majority favors the incorporation of BIT, although variations in the degree of BIT exist. The current state-of-the-art leads to customizing BIT for each application. This is due in part to the paucity of standards and design guidelines. Effort directed toward the further development of standards and guidelines will tend to reduce the variations in approach to this important subject.

BIT is cost effective. It should certainly be a consideration in the design of any but the simplest avionic equipment. For complex equipment, it is a necessity.

APPENDIX A

AN/ARC-142 Radio Set

The AN/ARC-142 High Frequency Sideband Radio Set, developed by RCA, is a small, 1000 watt, lightweight, highly reliable, multi-purpose transceiver incorporating a self-test system.⁽⁵⁾ A block diagram is shown in Figure 2. The radio incorporates automatic dynamic system-readiness testing and fault location which can complete the total test cycle in five seconds. The self-test feature costs less than 5 percent of the selling price of the equipment.

The self-test programmer is composed of self-test detectors, a 1.5-kHz tone generator, voltage comparators, fault-indicator drivers, and a sequencer that permits performance of the tests in the desired order. The programmer is illustrated in Figure 3. The operator initiates the sequence which begins the automatic dynamic testing of the transmitter and receiver circuits. The transmitter is modulated and connected into an internal dummy load. A modulated r.f. signal is injected into the receiver antenna input, whereupon the functional assemblies generate normal outputs that are measured for correct magnitude. One indicator on the radio set control signifies satisfactory completion of the self-test sequence; another is actuated if a fault is detected. All functional assemblies contain self-test detectors whose outputs are sent to the self-test programmer for comparison with reference voltages. If the detected output is abnormal, the appropriate magnetic latching fault indicator is set.

Planned for subsequent designs are light emitting, failure indicating diodes on the equipment panel, expansion of the readiness information presented during flight, and compatibility with VAST (AN/USM-247), the computer-controlled automatic check-out equipment which will monitor most electronic equipment on carrier aircraft.

References:

1. MIL-STD-1309, Definitions of Terms for Automatic Electronic Test and Check-out, December 20, 1966, Department of Defense, USA.
2. Ernest C. Seaberg and Wendell A. Triplett, The Economics of Integrated Logistics Support, presented at the National Aeronautic and Space Engineering and Manufacturing Meeting, Los Angeles, California, October 6-10, 1969. Document 690632, Society of Automotive Engineers, Inc., Two Pennsylvania Plaza, New York, N.Y. 10001.
3. J. A. Jurenko and J. W. McNabb, Built-in Test Equipment Using Automated Diagnostic Procedures, presented at the Avionics Panel XVIIIth Technical Symposium and published in Testing of Airborne Avionics Systems, AGARD Conference Proceedings No. 51.
4. Charles W. Postlewaite, Thomas F. Dwyer and Ronald Virgilio, A Guide to the Application of Built-in Test to Navy Avionic Equipment, Publication 562-01-1-866, ARINC Research Corporation, 2551 Riva Road, Annapolis, Maryland 21401, USA.
5. Irving P. Magasiny, AN/ARC-142 HF Transceiver, Digest of U.S. Naval Aviation Weapons Systems, November 1969, NAVAIR 08-1-503, Naval Aviation Engineering Service Unit, Philadelphia, Pa. 19112, USA.

TABLE 1

CO-AMP Deployment Matrix

SUPPORT LEVEL	TEST EQUIPMENT FUNCTION	MAINTENANCE POLICY NUMBER																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
EQUIPMENT	COU	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	FIM			●						●	●	●									
ORGANIZATION	COU		●		●		●		●	●			●	●	●	●	●	●			
	FIM				●					●			●	●	●						
	FIP									●			●								
INTERMEDIATE	COU					●	●				●			●		●	●		●	●	
	FIM					●	●				●			●		●	●		●	●	
	FIP										●			●		●			●		
DEPOT	COU							●	●			●			●		●	●		●	●
	FIM							●	●			●			●		●	●		●	●
	FIP											●			●		●	●		●	●
LOGISTIC DISCARD LEVEL		UNIT		MODULE								PART									

TABLE 2

Cost effectiveness of BIT

	Standard Reliability \$10 ⁶	High Reliability \$10 ⁶
Acquisition Costs:		
RDT&E	6.0	6.0
Production (500 Equipments)	100.0	100.0
	106.0	106.0
Additional Cost for BIT:		
RDT&E (5%)	0.3	0.3
Production (10%)	10.0	10.0
	10.3	10.3
Total Cost of Maintenance (10 Years)	300.0	100.0
Cost of Manpower	150.0	50.0
Savings in Manpower (25%)	37.5	12.5
Net Savings	27.2	2.2

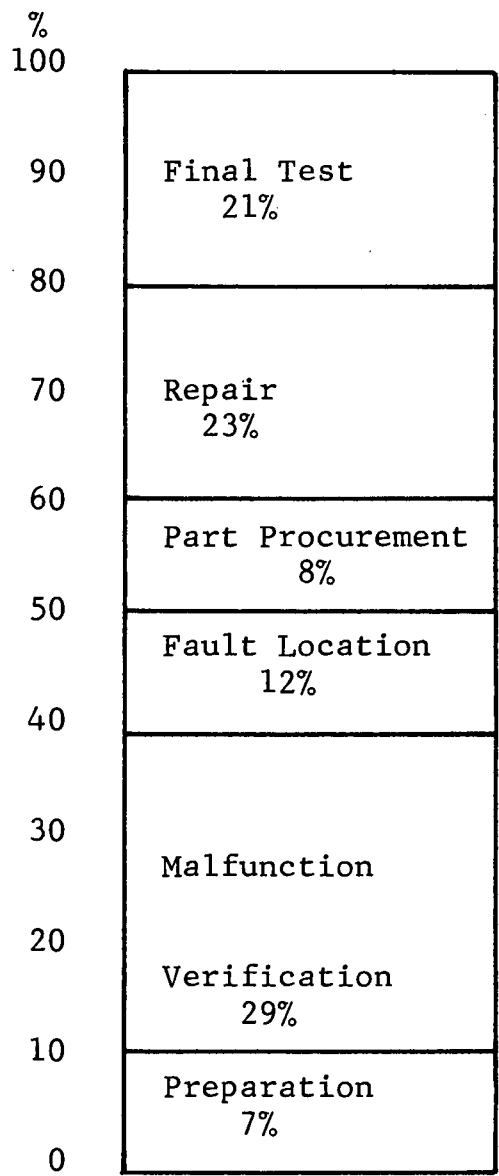


Fig.1 Distribution of active repair time AN/ASB-4

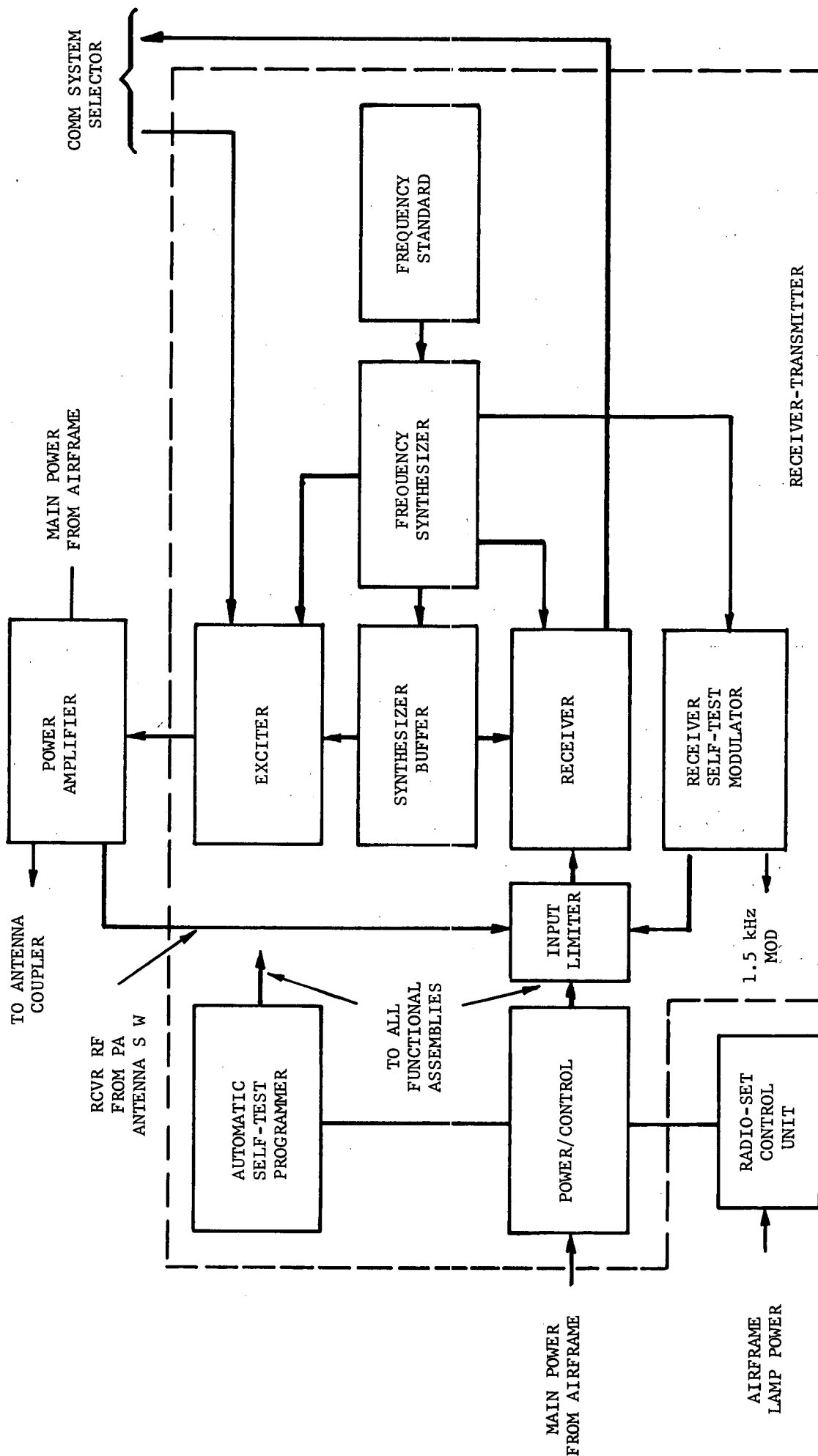


Fig.2 AN/ARC-142 radio overall block diagram

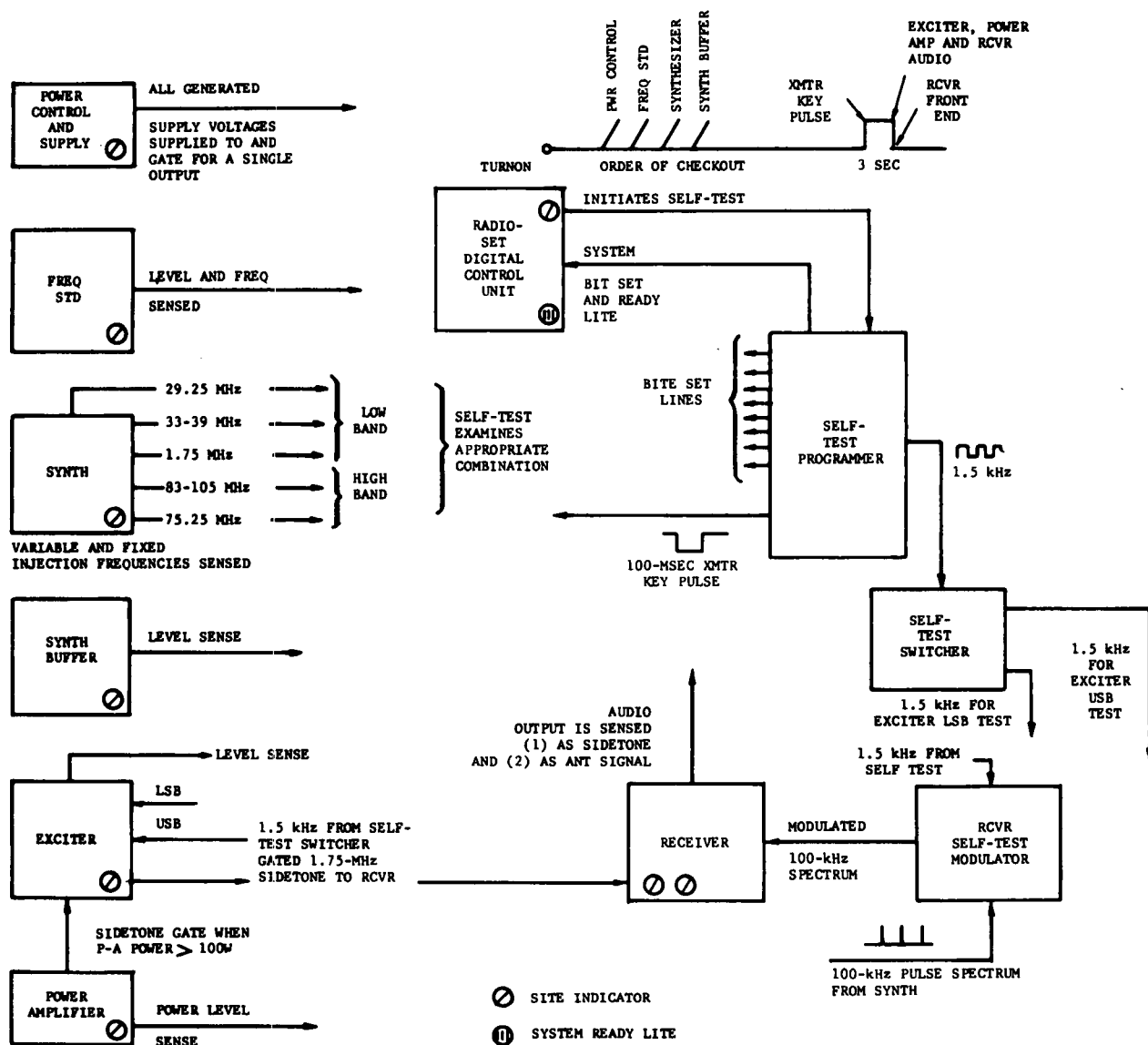


Fig.3 AN/ARC-142 Radio self-test programmer

HIGH RELIABILITY DESIGN TECHNIQUES APPLIED TO THE LUNAR MODULE

by

J. J. Bussolini

Director of Engineering Operations and Administration
Grumman Aerospace Corporation
Bethpage, New York

SUMMARY

In July 1969 Astronauts Armstrong and Aldrin accomplished history's most fantastic feat by gently lowering the Lunar Module onto the Lunar surface, allowing man for the first time to explore an extraterrestrial body. The national and international emotion that followed this historic event tended to shadow the real accomplishment of the entire mission, the ability of American technology to produce the vehicle and men necessary to do this job.

The design techniques applied to the Lunar Module cannot be considered unique when viewed individually in relation to normal industrial technology growth. However, when examined in their system combination, it becomes obvious that system reliability resulting from the combination of a variety of previously untested techniques was the real challenge.

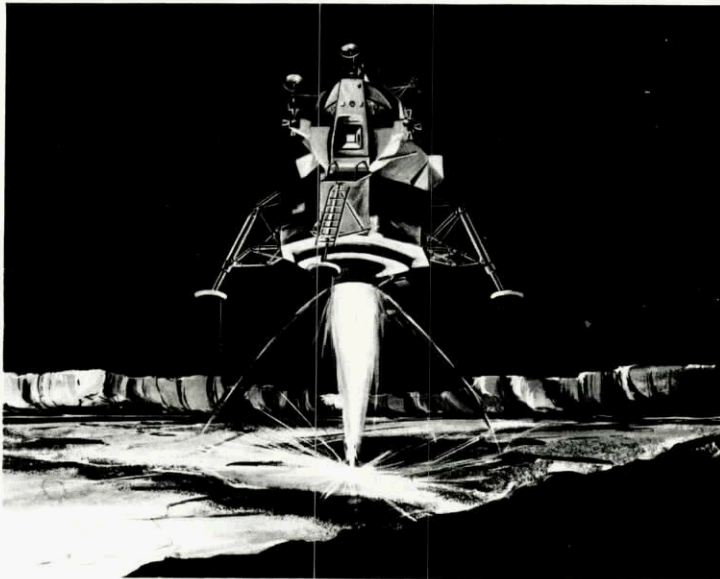
This paper describes many of the more significant design techniques applied to the Lunar Module to attain system reliability. The use of system work-arounds, functional redundancy, hi-rel parts screening, successive stage building block testing, vehicle testing, overstress testing, failure mode and effect analysis and many other techniques are described, illustrating their relative importance toward the success of the program.

INTRODUCTION

The history of aerospace reveals many technological challenges that were successfully met. One event in the last decade, however, has overshadowed past accomplishments and focused a new light of public awareness on the ability of world technology to challenge and solve literally any scientific problem. In July 1969 when Astronaut Neil Armstrong became the first human to set foot on an extraterrestrial body, brought there in a rather awesome looking vehicle called the Lunar Module, American technology proved that it was capable of designing reliable man-rated vehicles for unknown environments.

Man's first Lunar landing certainly captured world emotion more than any other such event in history and created a public awareness not only of American technological capability, but of the benefits of a reliable, well designed vehicle incorporating both automatic operating features and the ability to effectively utilize man in the loop.

The design techniques that were applied to the Lunar Module cannot be considered unique when viewed individually in relation to normal industrial technology growth. When examined in their system combination, however, it becomes obvious that total system reliability from the combination of a variety of previously untested techniques was indeed a significant challenge.

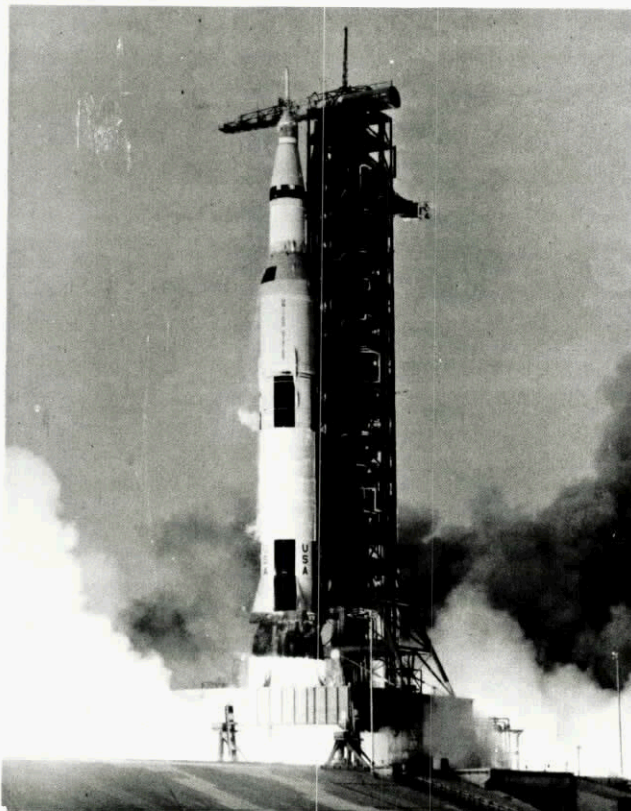


LM is a two-stage spacecraft weighing 16 tons. The upper, or ascent stage, is the habitable stage. It carries the ascent engine, the crew compartment, and all the equipment necessary to sustain the men during the time they are separated from the Command Module. The astronauts depart from the Moon in the ascent stage using the lower, or descent stage, as a launch pad. This stage has the descent engine and landing gear with which the men make a safe, controlled landing.

THE CHALLENGE OF SPACECRAFT DESIGN

The Lunar Module is the first manned spacecraft designed to function solely in the environment of space. Its role is to transfer two astronauts and their scientific equipment from lunar orbit to the lunar surface, provide sufficient environmental control to permit completion of their scientific experiments and safely transfer the crew, some equipment and lunar samples back to the orbiting command module.

The initial objectives of the Apollo Program were achieved with the successful lunar landing of LM-5 (Apollo 11). There were many varied challenges which had to be overcome in the years prior to this landing to develop the LM to meet the Apollo objectives.



*Major factors contributing to spacecraft reliability are simplicity and redundancy in design; emphasis on testing; a disciplined system of change control and closeout of all discrepancies. George W. Low, Apollo Program Manager, NASA.

To properly describe the elements of the LM reliability program, it is perhaps necessary to examine the types of reliability problems that are peculiar to manned spacecraft as contrasted to the more familiar ground based electronic, aircraft and missile systems. Basically, any reliability program consists of three major phases: establishing reliability requirements, design assurance and reliability demonstrations. With respect to reliability requirements, spacecraft usually require higher levels of reliability than do most other systems. Aside from crew safety considerations, the major reasons are shown in Figures 1 and 2.

Considering these constraints, therefore, the initial challenge was to develop a method of establishing a meaningful reliability program for a manned Lunar Module. Based on the initial definition of the Apollo/LM mission and original system configuration, reliability predictions, considering random failures only indicated that the target probability of success could be achieved. Thus, the basic approach taken was to root out design and quality weakness by analysis and test on subsystems and then on individual spacecraft. The approach focused on individual flight vehicles to assure that at the time of launch the only failures likely to occur were truly random and not due to the more conventional reasons for failure which were experienced in other programs such as interface problems, misapplication of parts, faulty checkout procedures and so forth.

RELIABILITY ASPECTS OF THE LM PROGRAM

At the outset of the LM program, it was recognized that there were major technological and mission-oriented problems that could severely compromise system reliability. These areas of major uncertainty are summarized in Figure 3. Because of these uncertainties, an extremely large portion of the system reliability effort was devoted to both the mission and a compatible system design which recognized the interrelated requirements of all subsystems.

ENVIRONMENT	LUNAR SURFACE MICROMETEORITES AND RADIATION VACUUM ENVIRONMENT ON EQUIPMENT
MISSION-ORIENTED	RENDEZVOUS AND DOCKING MAN-IN-SPACE
TECHNOLOGICAL	PROPULSION SYSTEMS POWER SYSTEMS

Fig. 3 Some Early LM Program Uncertainties

The basic approach taken to maximize mission success and crew safety reliability included:

- A time-phased program designed to successively build up confidence in achieving mission success.
- An overall design approach for mission flexibility and adaptability to change with minimal program impact.
- Placing man-in-the-loop to enhance safety and success.
- Use of proven components and/or design for simplicity even at the expense of some performance capability.
- Elimination of potential single point failures, where practical, that could jeopardize the crew or result in loss of primary mission objectives.
- Strong subcontractor reliability control program.
- Comprehensive integrated test and assessment program.
- Adequate understanding of the cause of failures and rationale for their closeout, based on design or operational impact and adequacy of corrective action.
- An analysis and test program designed to assess reliability with contract end-item reviews at major milestones for effectiveness decision-making.

GROUND BASED ELECTRONICS	CONTINUOUS MAINTENANCE PLUS LACK OF WEIGHT CONSTRAINTS TO ALLOW REDUNDANCY CAN ASSURE ALMOST CONTINUOUS UP-TIME WITH RELATIVELY LOW EQUIPMENT MTBF'S
AIRCRAFT	SHORT MISSION DURATION, MULTI-MODE CAPABILITY, SQUADRON SIZE, POST-FLIGHT MAINTENANCE CAN ASSURE HIGH SYSTEMS EFFECTIVENESS WITH RELATIVELY LOW MTBF'S
MISSILES	SHORT MISSION DURATION, CONTINUOUS OPERATIONAL READINESS CHECKOUT, AND MULTIPLE LAUNCH SITES FOR TARGET ASSIGNMENT, LACK OF MULTI-MODE CAPABILITY, WEIGHT CONSTRAINTS AND SINGLE-SHOT SYSTEMS REQUIRE MTBF'S HIGHER THAN ABOVE
SPACECRAFT	LONG MISSION DURATIONS, UNKNOWN ENVIRONMENTS, SOPHISTICATED HARDWARE TECHNOLOGY, WEIGHT CONSTRAINTS, REQUIRE HIGH MTBF'S

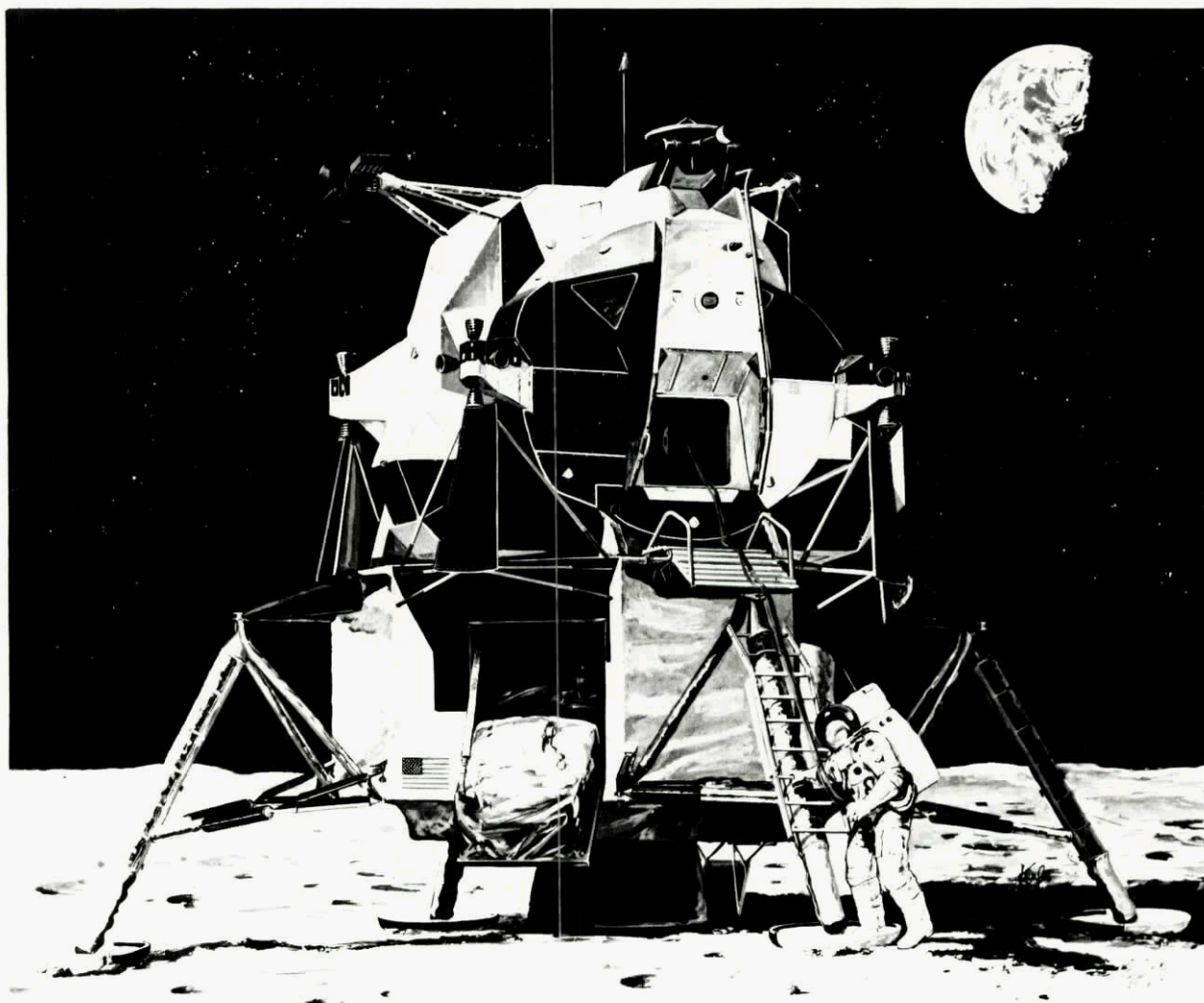
Fig. 1 Differences in Reliability Requirements Associated with Different Use Applications

GROUND BASED ELECTRONICS	CAN STATISTICALLY DEMONSTRATE AVAILABILITY, MAINTAINABILITY AND RELIABILITY DURING ACTUAL SYSTEM OPERATIONAL USAGE UNDER FIELD CONDITIONS SPECIFIED
AIRCRAFT	CAN STATISTICALLY DEMONSTRATE IN-FLIGHT RELIABILITY, TURN-AROUND TIMES, MAINTENANCE MANPOWER PER FLIGHT UNDER OPERATIONAL CONDITIONS OR SPECIFICALLY DESIGNED FLIGHT OR MAINTAINABILITY TESTS, IF LARGE PRODUCTION QUANTITIES CAN DEMONSTRATE SUBSYSTEMS
MISSILES	CANNOT STATISTICALLY DEMONSTRATE IN-FLIGHT UNDER OPERATIONAL CONDITIONS BUT CAN SIMULATE BY NUMBER OF MISSILE FIRINGS AND DEMONSTRATE OPERATIONAL READINESS. LARGE PRODUCTION QUANTITIES CAN DEMONSTRATE SUBSYSTEMS
SPACECRAFT	CANNOT STATISTICALLY DEMONSTRATE IN-FLIGHT RELIABILITY OR SIMULATE IT OTHER THAN THROUGH COUNTDOWN SEQUENCE. LOW PRODUCTION QUANTITIES CANNOT DEMONSTRATE RELIABILITY OF SUBSYSTEMS

Fig. 2 Differences in Demonstration Associated with Different Use Application

Ground based electronic systems and aircraft can achieve a high level of systems effectiveness with relatively low equipment MTBF's. Missiles, on the other hand, cannot. But, the fact that their usage time is short, and the fact that a number of missiles can be directed at a target, makes it possible to obtain the effectiveness required, with low equipment MTBF's as long as the cost is tolerable. With manned spacecraft, on the other hand, effectiveness involves long mission times, an uncertain environment, complex and sophisticated technology (much of which is developmental) and severe weight constraints which limit the use of redundancy. Thus, in order to have any reasonable degree of assurance of mission success, higher orders of MTBF are required than for the other systems.

As far as design assurance is concerned, there are no reliability problems peculiar to manned spacecraft that are not inherent in the development of other systems. Aside from requiring higher levels of MTBF than other systems, manned spacecraft pose the additional problem of statistically demonstrating achieved reliability. Reliability demonstrations on ground based electronic and aircraft systems can be obtained under operational usage conditions, and where large production quantities are required, even earlier on a subsystem basis. In the case of missiles, the combination of large production quantities and the demonstration of operational readiness can provide a high degree of confidence in the system even if its effectiveness cannot be demonstrated under operational conditions on a statistical basis. With manned spacecraft, the problem involves limited production quantities where it becomes impractical to perform reliability demonstration tests on subsystems and equipments, and the sample size based on actual missions will never be large enough to statistically assess reliability with any reasonable degree of confidence.



"One of the most challenging problems in the design of the Lunar Module was designing a vehicle for landing on a surface whose characteristics were virtually unknown." Joseph Gavin, LM Program Director, Grumman Aerospace Corporation.

TIME-PHASED PROGRAM FOR SUCCESSIVE CONFIDENCE BUILD-UP

As indicated in Figure 3, there were initially several areas of uncertainty. Primarily due to the environmental and mission-oriented uncertainties, great reliance was placed on the completed programs such as Mercury, Gemini, Ranger and Surveyor. While Mercury was the first man-in-space program, it was Gemini which validated a two week duration manned flight experience, rendezvous and docking capability, Apollo type abort procedures, as well as valuable experience on hardware performance for Apollo type missions. Similarly, the Surveyor soft lander provided the knowledge needed about the bearing strength of the lunar surface required for the design of the LM landing gear. Other NASA programs provided more accurate models of the micrometeorite and radiation environment required for the design of the outer skin as well as the evaluation of the acceptability of certain semi-conductor material whose performance was radiation sensitive.

The LM program itself was programmed to take a step-by-step approach to resolving uncertainties inherent in its systems.⁽¹⁾ In most cases, ground tests were adequate for validating the performance and for yielding confidence in LM systems. The major exceptions were propulsion firings in a vacuum environment and a lunar landing descent, neither of which could be adequately simulated on earth. Thus, before

a manned lunar landing, an unmanned earth orbital mission was required to verify ascent and descent propulsion system performance in a vacuum environment. To assure crew safety there, a firing of the ascent engine in close proximity to the descent stage, called Fire-in-the-Hole, was also required. This served to simulate an abort maneuver during a manned flight. The other area that could not be simulated completely was the actual lunar landing on earth under representative conditions. No methods have been found to cancel air drag and the difference in gravity. From a reliability viewpoint, it was necessary that a well-planned, well-defined, and well-integrated program be established to continuously assess areas of uncertainty. It was also important that a meaningful and systematic measure of the degree to which these uncertainties were eliminated be made before a commitment was made. It was within this framework that the Reliability Program Plan was developed and implemented.

DESIGN FOR MISSION FLEXIBILITY AND SYSTEM ADAPTABILITY

In the specification of requirements of any system, one generally lists the things that are desirable which become design groundrules. In the design of the LM these included:

- The vehicle had to have a 48 hour operational lifetime.
- The vehicle had to possess the capability of landing either in earthshine or sunshine.
- The vehicle had to be in line-of-sight communications during critical powered phases of the mission.

The combination of these types of groundrules served to define "sizing" requirements. For example, they defined the consumables required--oxygen, water, etc. They also served to provide an initial design reference mission, giving time-lines and required vehicle Δv maneuvers (change in velocity requirements) to be used as a basis for propellant tank sizing. Similarly, there were requirements for such constraints as reliability and weight. On a vehicle such as LM, one is interested in its weight at separation from the CSM, since the maximum allowable is a function of the specific impulse of the descent engine, and the vehicle weight at lunar launch where the maximum allowable weight is a function of the specific impulse of the ascent engine. As is often the case, when attempting to combine the design groundrules with weight and reliability constraints, they are not always compatible. The problem thus becomes one of asking, "What capability is really required and at what level of reliability to be compatible with the control weight of the vehicle?" There were two basic approaches used for handling this type of question: parametric analysis of all the relevant variables, and establishing mission worth assignments.

Situations which lend themselves to parametric analysis are those that can be quantified where the sensitivity of one variable on another can be assessed. For example, if it is possible to allow the mission time to increase, it might be possible to carry less propellant for Δv changes, and thus allow the decrease in reliability due to longer mission times if the weight saved in propellant can be used for redundancy in certain critical areas. A similar situation arises in the sizing of an electrical power generation system as an example. The power/energy levels established are basic to defining whether equipment can be completely operating during a mission, cycled on and off, the flexibility of switching alternate equipments and their allocation of primary and secondary busses to minimize the effects of failures. In both these situations parametric curves were generated which related reliability achievable for alternative design or operational conditions.

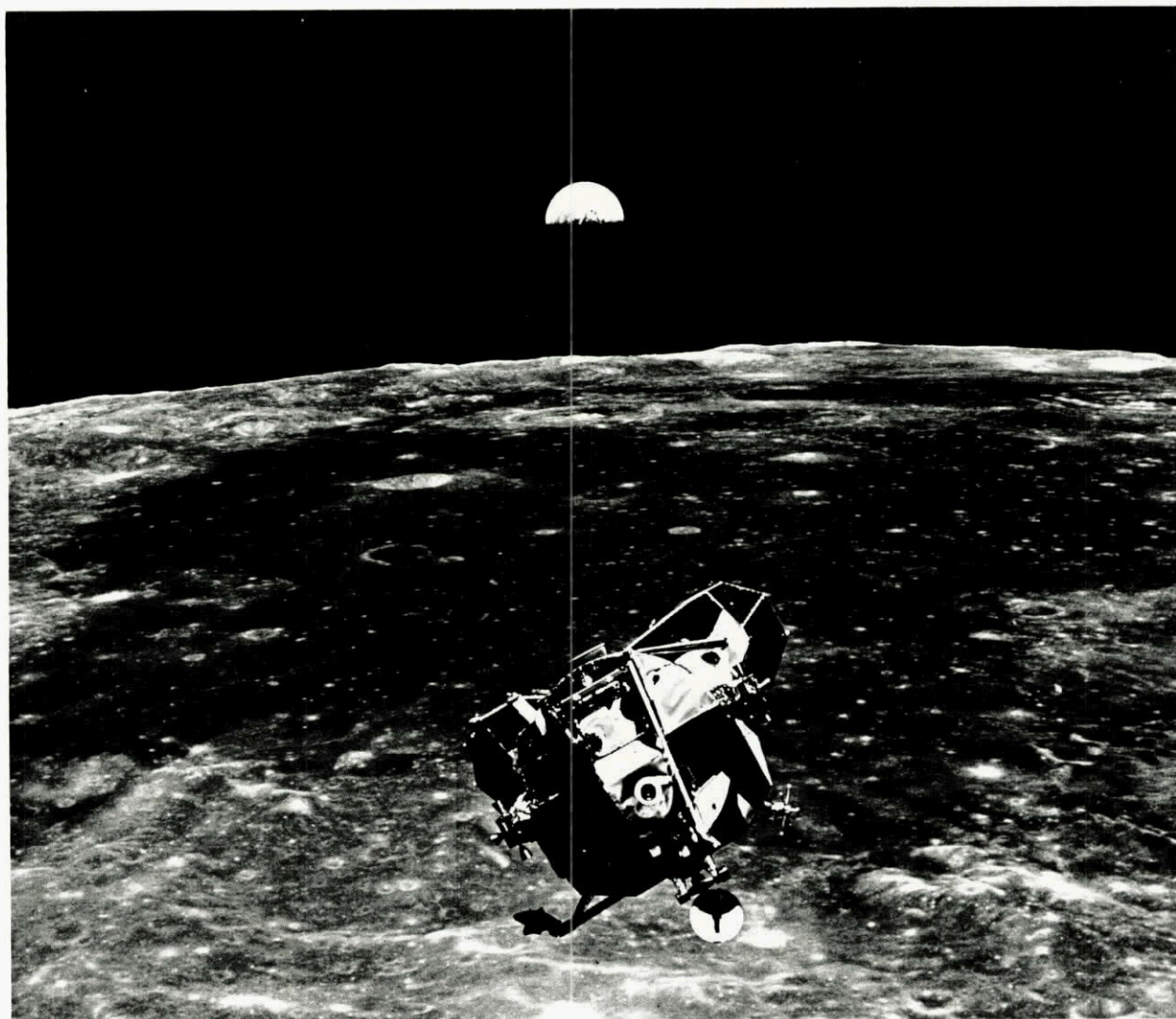
In many cases, however, it is often necessary to establish mission worth assignment in some rank order. An example of this case might be: Due to uncertainty of terrain, it is necessary to provide immediate and random launch capability from the lunar surface. Thus, this requirement might be given a high measure of priority even recognizing that reliability would be increased if systems could be depressurized while on the lunar surface and thereby minimize the opportunity for leakage. Depressurization could preclude the capability of immediate and random launch. Another situation might be the case where it is deemed important to maintain continuous direct earth communication with the vehicle to enhance safety and chances of success of future flights, even though the latter system is not essential to the success of an individual mission under consideration. The method by which one establishes measures of mission worth are obviously subjective. Since they relate to the relative importance of accomplishing the various mission objectives they can only be established by program management independent of the design effort. From a reliability viewpoint, it is always necessary to provide management with the risks to be taken for a particular set of mission worth assignments.

One of the tools which aided in the selection of alternate LM subsystems configurations were the weight-reliability optimization studies. Early in the design process a range of five configurations for each subsystem was established, each yielding a different weight and reliability estimate. To optimize weight and reliability on an overall system basis, it can be seen that 10^5 combinations for system design existed. In this case analytical optimization tools such as Dynamic Programming proved most helpful. Aside from the mathematical rigor in obtaining optimum solutions, the techniques lend themselves to a systematic evaluation of alternate configuration definitions. Recognizing that system development was an evolutionary process, it was necessary that initial mission and system definitions be flexible and adaptable to change in light of the many uncertainties at the beginning of a program. Thus, it was required that reliability be considered as an integral part of the systems engineering process.

PLACING MAN-IN-THE-LOOP TO ENHANCE MISSION SUCCESS AND SAFETY

There has been much discussion in recent years on how to quantify the increase in a systems reliability with man-in-the-loop as an active operational element and decision maker. While there may be no adequate methodology at present for quantifying man's contribution to system effectiveness, there is no question that he enhances it, if the proper balance of man-machine tasks can be defined. This has been proven on many occasions in the U. S. space program, highlighted on each of the Lunar landings and put into prominence on the Apollo 13 mission.

It was recognized that for earth orbital operations a large portion of the command and control capability could be earth-centered relying heavily on telemetry data to perform caution and warning functions, abort instructions and so forth. Manned missions, however, required that a large share of the command and control activity be on-board. On LM all primary modes of operation can be performed automatically with the provision for manual override. Alternate modes can be performed by the crew with varying degrees of degradation.



The importance of "man-in-the-loop" is emphasized by the LM-CSM rendezvous and docking phase which is a fully manual operation. The spacecraft commander orients the LM so that the CSM is visible in the overhead docking window. A reticle on board LM is aligned with a docking target on the CSM to provide a means of assuring proper contact.

The major reason that man-in-the-loop enhances mission success is that his existence allows for the definition of a number of alternate paths (redundancies) that would otherwise not exist. Examples of the additional number of alternate paths as a result of man being in the loop can be found in the Navigation and Guidance areas. With the use of the optical telescope, the crew can supplement the inertial system and provide updated position and velocity information for the computer via a keyboard. Additionally, the crew with the hover capability provided, can select alternate landing sites within the translation capability of the vehicle; and man is essential for performing intricate docking maneuvers.

USE OF PROVEN COMPONENTS AND DESIGN SIMPLICITY

The design approach on the LM program was intended to be conservative, that is, utilize relatively proven components and simple designs. With regard to electronic systems, there are some novel designs in the radar systems, and communications at S-Band frequencies is relatively new, but on the whole required little in the way of technological development that presented reliability uncertainties. The use of Hi-Rel parts was required and their use strictly enforced. Items such as analog integrated circuits were restricted, with certain exceptions, not because they did not ultimately promise a high degree of reliability, but rather because they were at that time developmental items. Digital integrated circuits, where there was sufficient history to warrant their use, were used in digital subsystem where large numbers of identical units were required.

A major area of technological or design uncertainty was in the propulsion subsystem. To achieve the powered descent, a soft landing and provide the necessary manual control and hover capability, the descent system was required to have a gimbaled, throttleable engine with ablative thrust chamber to provide the necessary cooling. The engine has a proportional thrust control of 10 to 1 and develops a maximum of 10,500 lbs. of thrust. The ascent system, which is basic to crew safety, is designed for simplicity, as a fixed, constant-thrust engine which develops 3500 lbs. of thrust in a vacuum. Because of the uncertainty of the descent engine design, two distinctly different throttling approaches were evaluated and one approach finally selected after a long development process. The other problem inherent in both the ascent and descent engines was the use of ablative material for cooling. One of the major difficulties with these engines is that their ablative materials are consumed during operation, so that non-destructive testing presented a real problem. The reliability problem was to assure the engine life required by not obtaining premature burn-through of the ablative material due to hot spots (impurities in the material) and uneven spray of propellant and oxidizer.

A significant early technological stride in the Apollo program was the use of fuel cells as the primary power source. In this case weight savings were so great over conventional power sources that the development risk seemed justified. While fuel cells are used on the CSM, development problems on the LM program could not justify the advantage they provided in weight, and batteries are now the prime power source.

ELIMINATION OF POTENTIAL SINGLE POINT FAILURES

A task which proved most valuable during the design phases of the LM program was the Failure Mode and Effect Analysis (FMEA) from which a list of potential single point failures which would incur loss of mission or crew was generated. FMEA is a methodology which systematically considers each functional element of the system--postulates a failure mode--and asks what happens to the mission in the event of failure. It considers methods of failure detection, the degraded modes the mission can be continued in, as well as if, and how, aborts should occur.

For the technique to be effective, it was started in early design phases on a functional basis, compatible with the level of drawings generated, and progressively proceeded to lower levels culminating in circuit analysis. The requirement to perform FMEA's was placed with all subcontractors. Since a subcontractor could only carry his effort to the outputs of his equipment, the effort required integration into a vehicle level analysis for each mission. When this was done, all potential single point failures affecting safety and success were established. This then served as a basis for areas requiring further attention. If the likelihood of a single point failure was high, some form of redundancy or alternate path was developed where practical. The basic objective was to reduce the list to a limited number which was considered tolerable. The list also served as a basis for strict control of failures and test history. Thus, greater attention was paid to the adequacy of qualification testing, failure history, parts selection and application for items deemed potential single point failures. Due to the many environmental uncertainties in space, it was important that possible failure modes be adequately identified and corrected.

SUBCONTRACTOR RELIABILITY CONTROL PROGRAM

It is now fairly commonplace that government agencies and major systems contractors generate reliability requirements for their subcontractors and suppliers. On the LM program there are about 250 subcontractors and suppliers of which about 25 to 30 considered major subcontractors. Since the LM program was established in accordance with NPC-250-1, reliability "boilerplate" specifications were generated and became part of every contract. The extent of the specification differed for major and minor subcontractors.

Each subcontractor was required to generate a reliability program plan to be approved by Grumman. Similarly, the extent of the funding allocated for reliability was part of the normal negotiations. The following items cover the major part of the Subcontractor Control Program instituted:

- Reliability rating of alternate subcontractors prior to selection
- Approval of reliability program plans
- Reliability audits
- Scheduled design reviews and data package requirements
- Data Package requirements:
 - Reliability apportionment, predictions and assessments
 - Configuration analysis
 - Failure mode and effect analysis including circuit analysis
 - Failure mode predictions on overstress tests
- Acceptable parts list, de-rating policy, part selection and application approval.
- Deviation and contract change control
- Developmental and qualification test plan and test report approval
- Closed-loop failure reporting, analysis and corrective action system.
Generally, manning estimates for reliability as compared to total engineering averaged overall Apollo contractors ranges between 3 and 5 percent

Performance of the above tasks did not in itself assure an adequate reliability control program. In consonance with the performance of these tasks a closed-loop management control system was required to assure that the information generated was effectively used and corrective actions taken as required. Simply stated: "Real" problems and reliability risk situations were brought to the attention of management who weighed these risks with overall program impact. The seriousness with which a subcontractor considers a reliability risk is a direct function of the emphasis placed in it by the procuring activity. The emphasis placed on reliability by NASA need not be overemphasized, NASA policy dictated that "every possible practical means be employed to achieve high system reliability at the earliest stage of system development." This policy was thus reflected in the requirements and attitude of the major Apollo contractors as well as their subcontractors.

COMPREHENSIVE INTEGRATED TEST AND ASSESSMENT PROGRAM

The overall test program was designed to root out design weaknesses in the overstress and qualification test programs, quality weaknesses in acceptance testing, interface problems in system integration tests, and the minimization of chances for flight failures, by a comprehensive and rigorous ground test program. It was the basic approach of a well-planned, timed-phased program to ferret out weaknesses and problems, and continuously perform reliability assessments, which was intended to assure successful achievement of reliability goals.

It was recognized in the initial stages of program planning that a statistical demonstration of reliability would not be feasible. The reason for this being that the combination of units and/or time to run the tests, to demonstrate apportioned reliability goals, were not feasible on a cost and schedule basis. Thus, the approach taken was to develop an overall integrated program designed to successively build up confidence in the equipment by combining the results of analysis (predictions) with test data in making an assessment.

Prior to equipment qualification, overstress tests were run on critical items. The purpose of these tests was to provide a sufficient insight into failure mechanisms at environmental stress levels considerably above the mission levels. The approach was to run an equipment through one mission cycle and then step-stress it to failure. Prior to performing these tests, subcontractors were required to perform a prediction of the failure modes they expected. While it was not necessarily possible to correlate stress with time to statistically demonstrate achieved reliability, on an accelerated basis, the tests provided much engineering confidence in the hardware, and also served as a means of assuring qualification tests would be passed. This was important to prevent the situation where, in the middle of the qualification test program, reliability problems would be detected.

From an overall systems viewpoint, it was recognized that consistency was necessary in the qualification test requirements for the many different equipments and their suppliers. Consistent with the requirements of the overall vehicle level Design Certification Review, a Certification Test Requirement

(CTR) effort was established on the LM program. The combination of the requirements being established and controlled by reliability engineers, as well as the sign-off on the endorsement that qualification has been passed, served as an extremely effective means of subcontractor control and failure close-out. Adequate reliability controls imposed during the course of system development, helped produce the situation where it was desired that the only failures that should occur in flight were random failures. However, since no test program can combine all environments simultaneously, adequately reflect all interfaces, and investigate all possible areas of quality defects, a rigorous ground test program was required to assure that flight failures, if they occurred, were restricted to the regime of random failures. Thus, the ground test program was designed with this in mind and made sufficiently comprehensive to screen out potential problems before a costly flight.

FAILURE REPORTING, ANALYSIS AND CORRECTIVE ACTION PROGRAM

As part of the reliability subcontractor control program all suppliers on the LM program were required to prepare failure reports during all development and production phases. An automated closed-loop system was maintained to assess status of open items as well as close-out information. A major program groundrule was that the cause of each failure be completely understood, its impact evaluated, and an assessment made of differing alternative corrective actions. A failure was not closed out until agreement was reached on a corrective action.

It was realized that failure reporting, analysis and corrective action programs could easily turn into a record keeping affair of up-to-date status of failure if both the cause and impact of a failure was not understood. Additionally, with the pressures of schedules, it was important that the ability to close-out open items be controlled by an activity independent of those responsible for design delivery. This was necessary to provide management with the visibility necessary on the true status of equipment, particularly at scheduled program milestones.

On a program the size of LM, it was understood that there could be thousands of open failures at any one time. Therefore, it was necessary to filter them to decide how the effort of reliability engineers should be allocated. Generally, a large number of items remained open because they deviated slightly from specification. In a large percentage of cases these deviations could be "tolerated" since specifications sometimes required tighter performance than was absolutely necessary. The intent of the data system was to highlight hard-core program impact problems. When these were adequately identified a concentrated effort was directed toward their close-out.

RELIABILITY PARTICIPATION IN CONTRACT END-ITEM REVIEW MILESTONES

Both the AFSC 375 series documents and NPC 500-1 as part of the Systems Management effort required that contract end-item (vehicles) reviews be held as the system develops, and in the case of Apollo, prior to launch, and after the mission has been completed. While there are differences between the Air Force and NASA review systems, on the LM program it has evolved as a sound discipline for bringing the necessary information to provide sufficient visibility on the status of design, manufacture and test, for decision-making by NASA and contractor program management.

The six key checkpoints or program milestones were:

- PDR - Preliminary Design Review
- CDR - Critical Design Review
- FACI - First Article Configuration Inspection
- CARR - Customer Acceptance Readiness Review
- DCR - Design Certification Review
- FRR - Flight Readiness Review

The progression through each milestone was dependent upon the availability of documentation and hardware upon which to conduct the reviews. The PDR was a technical review of the basic design approach conducted early in the detail design phase. The CDR was a technical review of the basic design approach conducted prior to release for manufacturing. The FACI was an examination of a particular manufactured end-item against specifications and drawings and validated the acceptance testing. The CARR was a planned review prior to vehicle delivery to evaluate the acceptability of the end-item for shipment to the mission use site. The DCR and FRR were primarily internal NASA reviews with contractor support since they pertained to the total space vehicle (the integrated effort of all contractors and centers). The DCR certified the design of the total space vehicle and emphasized the status of qualification tests, failures and their dispositions and certification that the item was qualified for manned flight. The FRR validated that the total system was operationally ready to perform its mission objectives and not crew safety requirements.

APPROACH TO THE DESIGN

There are many typical examples that can be presented illustrating how all elements of the LM developmental process blended together to generate design decisions resulting in a reliable man-rated vehicle.

At the initiation of the LM Program, one of the most challenging problems was that of designing the vehicle for landing on a surface whose characteristics were virtually unknown.⁽²⁾ Neither the structure nor the soil mechanics or thermal properties of the lunar surface could be predicted with any degree of confidence. It was not known whether flat or sloping terrain would be encountered, what the frequency and distribution or given size and depth of craters would be, whether the surface would contain rocks or dust and whether the reflective properties of the terrain would allow visual determination of obstacles at the landing site.

We were committed to the challenge of designing a vehicle for lunar landing, and early basic design decisions were required if the schedule was to be met. In conjunction with NASA, a series of "best guess" assumptions were made regarding the lunar surface characteristics and a range of values assigned to these for design purposes. Thus, coefficients of friction and bearing strength of the surface were specified to allow design of the landing gear pads. Maximum slope, crater depth and rock height at the points of landing gear pad contact were assumed in order to establish the stability boundaries of the vehicle at landings. It was assumed that no visual determination of altitude and velocity near touchdown would be possible and an impact velocity design envelope was specified based on a purely instrument landing. This envelope was used for design of the landing energy absorption system and for the structural design of the critical load bearing paths in both the ascent and descent stages. A descent engine thrust tailoff function was specified in order to establish the pressure and temperature regime of the landing gear and base of the descent stage and thus to be able to provide adequate thermal protection and structural strength.

We had to make sure that for the range of design conditions specified, the vehicle structure would safely survive the landing shock, would not tip over upon encountering the worst configuration of impact conditions and that no overpressure or overtemperature situations would occur. Intensive studies were undertaken which included:

- Analytical computer studies of thermodynamic, structural, stress, dynamics and propulsion parameters.
- Manually controlled simulation programs (cockpit, controls and computer math models).
- 1/20th scale model touchdown tests performed in Grumman's 7' x 7' vacuum chamber.

The results of these analyses provided sufficient preliminary data to proceed with the design in work which included four "landing gears," four lunar contact probes, a basic descent stage structure and a basic descent engine envelope with what was felt to be adequate thermal protection.

Statistical studies were then performed to determine the probability distributions of the occurrence of the various combinations of design conditions to assure that no undue weight penalties were being paid for overdesign of the vehicle.

A major problem arose late in the program when full-up descent stage propulsion testing disclosed that the descent engine thrust decay was much slower than originally assumed. This caused a variety of problems in the structure and thermal insulation areas. Since significant propellant flow still would exist at touchdown, the intersection of the exhaust plume with the ground resulted in higher pressures on the base heat shield and greater heat rates and higher temperatures on the landing gear struts than has been designed for. Increasing the length of the lunar contact sensing probes helped alleviate the problem somewhat, but could not provide the whole answer, since lengthening the probe also increased the impact velocity and thus could cause greater structural problems than it was trying to solve.

Several technical approaches were considered at the time to overcome this difficulty with minimum weight and schedule impact. In addition, an extensive test program was undertaken to determine the failure mode of the engine due to internal overpressurization. These tests showed that no problem would exist in this area, since the engine bell would fold back in accordion fashion and thus prevent internal overpressure and rupture.

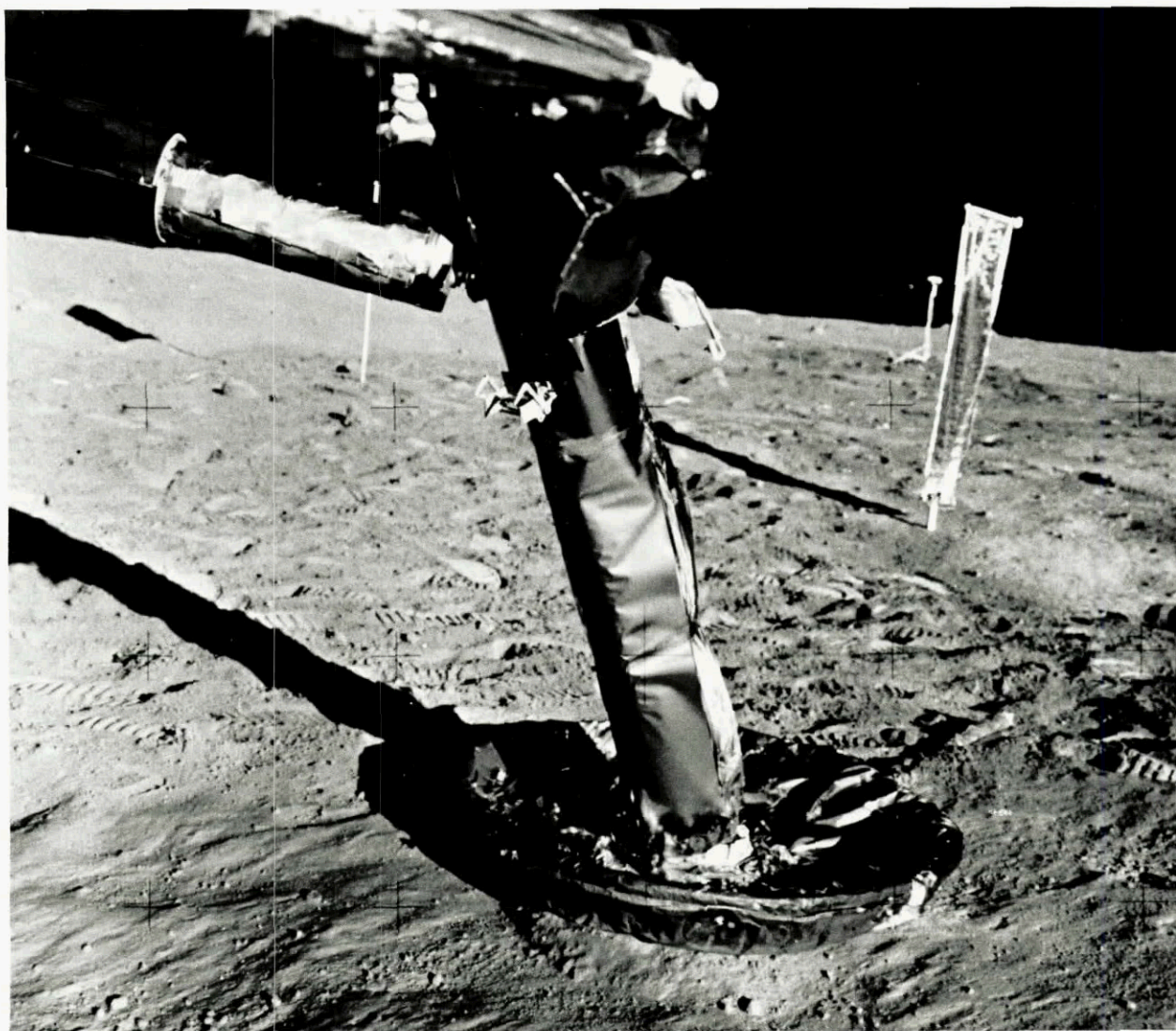
Finally, shortly before LM-5 delivery to Cape Kennedy, it was decided that structural and thermal beef-up of the descent stage and landing gear was required and the extensive redesign, manufacture and installation of the modified base heat shield and thermal insulation was accomplished without significant schedule effect.

Additional studies were implemented to evaluate the interaction of the thermal effects of the lunar surface, LM descent engine plume, and the LM reaction control system. The results of these studies created concern over the potential thermal effect on the landing pads and gears. We felt the need for a conservative approach and concluded that a redesign of the LM thermal protection in this area should be implemented. This decision was made just weeks before the final liftoff of LM-5 (Apollo 11). At that

time, LM-5 was on the launch pad loaded with propellants and in its final preparation for launch. During these final weeks just prior to launch, we developed, tested and verified new thermal protection designs. Engineering problems were manifested due to the sensitivity of having a hypergolic loaded vehicle on top of the booster in cramped working conditions in the SLA just inches above the booster tanks. Implementation of a thermally protected LM was accomplished without loss of scheduled time, such that the lunar liftoff occurred on schedule.

The lunar landings accomplished to date have proved the LM design to be far more than adequate for all lunar terrain encountered to date.

The thermal design of the landing gear received its most severe test on Apollo 11, where Descent Engine shutdown was delayed until landing pad touchdown rather than at probe light activation. From crew inspection after landing, and from analysis of photographs taken of the landing gear during EVA, it was determined that no thermal damage took place.



Landing gear members, like much of the outer structure, are insulated to maintain temperatures in structural components and honeycomb cartridges within desired limits during mission "hot soak" and "cold soak" periods. Additional insulation is required for plume impingement protection from LM reaction control systems firings and the descent engine during its fire-until-touchdown where temperature exposure could reach 1400°F.

LM MAINTAINABILITY

The maintainability considerations on the LM were quite different from those previously experienced with conventional aircraft or as a matter of fact for any other previously designed space vehicle. Design concern here was not for periodic maintenance, turnaround or overhaul. Once launched, the LM was considered non-recoverable and did not return to be retrofitted. Maintainability, however, was considered an important factor in the LM design. The maintenance concept initially was that the LM must facilitate smooth flow of operations from vehicle assembly through pre-launch checkout and ultimate launch. Routine servicing procedures had to be optimized. Major malfunctions had to be capable of being isolated with repair and replacement, where feasible, had to be accomplished in the shortest possible time. The launch window constraints which were inherent to the program and the use of a huge worldwide ground complex available for retrieval operations focused even more importance on the ability of the spacecraft to be in an operating condition at the time of its demand.

These constraints led to the considerations for trade-offs between reliability of hardware and possibilities for maintenance during pre-launch and post-launch. If malfunctions did occur, they had to be capable of repair within the time constraints of the launch windows. Failed equipment once removed from the vehicle had to be capable of immediate analysis and repair so that the cause of failure could be completely understood before committing the vehicle to its mission. No malfunction could be left unexplained. Repair had to be expedited so that a malfunctioning equipment could perhaps be made available as a spare. Spare hardware had to be minimized due to its high cost.

Maintainability analyses borrowed many of the analytical techniques developed for reliability analyses and also utilized data collected for the reliability analyses. Maintainability studies evaluated the likelihood of any assembly requiring replacement during each phase of the pre-launch operation. The analysis also evaluated the proposed pre-launch checkout operations and their plans and procedures.

The failure mode and effect analyses prepared by reliability engineers indicated potential modes of failure for each assembly and the predicted failure rate for each mode of failure. The maintainability engineer using this data constructed a pre-launch operating profile for each assembly in order to determine relative degradation and reliability during each phase of the operations. The probability of replacement of each assembly was predicted on the basis of the cumulative unreliability of each assembly during each phase. This permitted the maintainability engineers to rank the relative accessibility and ease of replacement required for each assembly on the basis of its likelihood of failure. This analysis provided substantiation for any recommendation for needed design changes for maintainability. Typical of the problems resulting from maintainability analysis was the access hatch to the interior of the LM. Analysis showed that the opening was not large enough to accommodate one of the replaceable hardware equipments from the environmental control system. The analysis was performed early enough to facilitate a redesign of the hatch configuration.

Access to inertial measurement unit of the primary guidance system also presented a problem due to interference of the service module engine bell. Full scale mockup tests were run which determined that the inertial measurement unit could be removed if the engine bell could be gimbled a few degrees. Coordination between NASA, Grumman and the Command and Service Module Contractor established that it was feasible to gimble the engine if needed and replacement of the IMU was made feasible.

The LM batteries also presented a challenging maintenance problem. They are relatively heavy and they must be installed within the last few days before launch. Special hoisting and handling equipment was developed and tested using full scale mockups in order to verify the maintainability related to the installation of the LM batteries.

Ideally, all the spacecraft hardware should have been checked at the instant prior to launch. This check would provide maximum confidence in the ability of the system to operate when called upon during the mission. This was not, however, feasible or possible. As the vehicle was assembled the equipment was individually checked prior to installation and it was again checked as part of the normal vehicle system test. Subsequent checks were made at higher and higher levels of assembly, most at system end-to-end checks. Certain modes of failure inherent to the hardware could not be checked as part of the system test. This is particularly true in cases where either hardware or functional redundancy was utilized.

Because of the involved process of assembly and checkout and the actual design of the spacecraft, some equipment could not be checked at all for any modes of failure for considerable periods of time prior to launch. Checkout of some systems while the spacecraft was on the launch pad was also not feasible. As an example, it was not completely possible to check the radar systems on the pad because the radar antennas were blocked by the shroud. Obviously, rocket engines could not be functionally tested once the spacecraft was physically made into the launch vehicle.

Electronic equipment in the aft equipment bay was mounted on "cold rails" which were extruded flanges with an integral tube for the flow of water glycol through the system for thermal control of the electronic equipment. Mounting electronics on these cold rails called for a specific form factor to be used in the equipment design. The form factor chosen was analogous to the shape of a loaf of bread and came in sizes ranging from small to large. The major variable dimension was the length of the box. Flanges on the box mounted to the cold rails with attachment approximately two inches on center. These flanges were the primary thermal path for the replaceable assemblies. Internally, the replaceable assemblies were designed to carry the thermal paths to the external flanges.

Modularization was also adopted as a design concept for the electronics hardware. The initial design concept called for the use of cordwood component modules, wire wrapped into multi-layered wiring assemblies on mother boards. This concept was ideal for internal maintenance, but weight constraints forced most designers to use other techniques which would provide the required levels of reliability in the thermal characteristics needed to meet mission requirements. The level of throwaway, type of interconnection technique, type of encapsulation, type of mounting for thermal and structural consideration all became candidates for trade-off studies which produced several alternate methods of design.

IN FLIGHT MAINTENANCE CONSIDERATIONS

LM system reliability could have been significantly increased if it were feasible for the astronauts to accommodate repair in flight. This approach, however, required considerable failure detection and isolation capability, the selection and storage of spares, and maintenance tasks. Repairs in a gravity free-environment by astronauts that are constrained by pressurized space suits presented several problems. In-flight repair would have necessitated anti-reaction type tools designed to prevent the astronaut from turning himself instead of turning the bolt or screw. Although such tools have been designed, they were not considered feasible within weight constraints for the LM mission.

Task times required to replace failed units with spare units were another consideration. Task times required compatibility with the time available to the astronaut to effect a repair. Mission time lines revealed that time available for repair would be minimized to a point where repair was not considered feasible. Also, the weight penalty in designing for in-flight modular replacement and the additional fault detection and isolation capability for carrying spare units could not be justified. Studies indicated, therefore, that in-flight repair for the lunar landing mission was not feasible, instead emphasis was placed on increased reliability through redundancy and simplicity.

LM RELIABILITY PROGRAM PLAN

The LM Reliability Program followed the rather detailed procedures of a Grumman-NASA negotiated reliability program plan.⁽³⁾ This plan has, of course, undergone many revisions as program requirements changed - necessitating appropriate changes to the details of the reliability program.

The LM Reliability Program was generally tailored to comply with NASA publication NPC-250-1 dated July 1963 and the NASA Quality publication NPC-200-2 dated April 1962. Reliability on the LM was considered an inherent product characteristic. It was not considered a commodity that was separate from the product. The concept was, therefore, that reliability must be designed and manufactured into the product and that reliability control, to be effective, must be integrated into the basic design and development of the hardware. In order to provide adequate degrees of assurance that the stringent reliability requirements required for mission success and crew safety of the LM had been met, a program of reliability control engineering was formulated in detail in the program plan. This reliability engineering program was designed to run concurrently with and to complement the LM design and development of all associated LM hardware.

PROGRAM CONTENT

A summary of the LM Reliability Program activities includes:

- Specification and purchase order review and approval
- Vendor negotiations
- Customer liaison
- Associate contractor liaison
- Review of reliability requirements
- Review of environmental requirements
- Design analysis and control of the design phase
- Participation in project design reviews

- Parts application and standardization
- Reliability surveillance of all test programs
- Subcontractor direction and monitoring
- Reliability review of the fabrication phase
- Failure reporting and corrective action
- Failure mode and effect analysis
- Failure mode prediction analysis
- Review of checkout, countdown and post-launch plans and activities

SUBCONTRACTOR AND SUPPLIER CONTROL

Early in the LM program, reliability engineers had apportioned the LM mission success and crew safety goals which were established by contract to each subsystem and equipment that was contained in the system. These apportionments were made in relation to system complexity and mission criticality. The apportionments established specific goals for LM equipment to be subcontracted and included these goals in the detailed design specification.

For all flight hardware which did not specifically contribute to mission success or crew safety, reliability goals of lesser magnitude were considered. The associated reliability program, however, which was imposed for this flight hardware was the same as for essential hardware.

For equipments such as ground support equipment which did not have reliability goals imposed, reliability program requirements were imposed in accordance with the ground support equipment criticality classifications.

The reliability program requirements for major subcontractors were included in the detailed design control specification and purchase orders solicited for specific subcontractors. The boiler plate reliability program included in this specification contained the following items:

- Reliability program planning
- Reliability assurance plan
- Reliability apportionment
- Reliability estimates
- Maintainability analyses
- Configuration and circuit analyses
- Failure mode and effect analysis
- Failure mode prediction analysis
- Failure reporting and analysis
- Reliability data lists (electronic parts)

RESIDENT RELIABILITY REPRESENTATIVES

Grumman established resident offices at most of its subcontractor installations. These offices were generally staffed by full-time Grumman reliability engineering representatives and full-time quality control representatives. The technical responsibilities of Grumman's engineering representatives included the monitoring of specific reliability tasks. Technical liaison was maintained with the base LM Reliability Group and the resident engineering representative. Periodic visits were also made to subcontractor facilities by LM reliability engineers.

CONTROL OF GOVERNMENT FURNISHED PROPERTY (GFP)

Where the system included components and equipments furnished to Grumman as a result of direct NASA contracts to associate contractors or components or equipments were furnished directly by NASA, Grumman used the best available reliability data obtainable to existing NASA reliability apportionments and predictions for the overall system. Wherever examination of these data or actual system test results by

Grumman indicated an incompatibility between the reliability of the GFP with the overall reliability requirements, NASA was formally notified with recommendations for appropriate action.

END-ITEM ENGINEERING

End-item engineers were assigned to follow each of the LM test and flight articles. This individual followed the factory build-up and checkout at the Bethpage facility and was then moved to Houston to follow the test program. For flight articles the end-item engineer followed the factory build-up and checkout at the Bethpage complex and the pre-launch and launch activities at the Merritt Island launch area at Cape Kennedy, Florida. He also participated in subsequent mission and post-mission activities related to his particular end-item. The reliability end-item engineer was a member of the engineering team assigned to each specific vehicle. He was, therefore, responsible for reliability liaison with test team leaders and vehicle managers.

DESIGN SPECIFICATIONS

The LM Reliability organization participated in the preparation, review and approval of all LM specifications, vendor change requests, specification drawings, purchase orders and all subsequent revisions and amendments. Reliability's direct responsibility in this area included:

- Numerical reliability goals
- Mission profile and mission success and crew safety reliability predictions
- Quality assurance provisions
- Reliability program requirements
- Reliability documentation requirements

RELIABILITY ASSESSMENTS

A continuous evaluation of program status was performed by assessing the readiness of each subsystem and the LM end-item itself. These assessments were performed prior to the movement of hardware to successive test for flight phases. These assessments were in consonance with the major program and vehicle milestones. The assessments were qualitative and represented an evaluation of the failure history and corrective action including the deviation history and the summation of failure mode and effect analysis data.

FAILURE MODE AND EFFECT ANALYSIS

Analyses were performed of potential failures and their affect on mission capability of each system. These analyses were conducted during a design phase in order to uncover critical reliability areas and to direct appropriate engineering attention to these areas. In the early phases of design, the analyses considered consequences of failure at higher levels of assembly. In the later phases of design, the analyses became progressively more detailed and ultimately were conducted at both equipment and functional levels. The results of these analyses were reflected in a design which was substantially fault free in its earlier phases. The FMEA analyses also served as a basic troubleshooting guide which became useful in later design of test and checkout equipment. A failure effect analysis was performed on each design and each change to that design. Reviews of failures during test were also conducted and the actual effect of these failures were compared to the predicted effect listed in the FMEA's.

FAILURE MODE AND PREDICTION ANALYSIS

This analysis indicated the anticipated modes of failure that could or would occur during overstress tests which were planned for the design verification program. Each mode was predicted as it related to specific environments where the failure would be anticipated. Failure mode prediction analyses ranked anticipated failure modes in two ways: likelihood of occurrence and the seriousness of the consequence of failure. Where analyses methods or past experience were sufficient to make a reasonable prediction of failure modes, other portions of the development program were implemented to probe the failure modes in order to support these predictions. Although, it was realized that failure modes due to overstress may not be identical to those analyzed in the failure mode and effect analyses, they were at the same time considered extremely valuable. Failure mode prediction analyses were included and submitted with each of the detailed test plans.

SINGLE POINT FAILURE SUMMARIES

Single point failure summaries were prepared and submitted and were essentially extracted from system level failure mode and effect analyses. The review cycle for single point failure summaries was such that all single point failure possibilities required the review and ultimate approval of the LM engineering manager.

ENVIRONMENTAL EFFECTS ON RELIABILITY

Each major hardware supplier was required to determine the effects of storage, packaging, transportation, handling, maintenance and operational environments on the reliability of his equipments or components. These studies included a determination of the effects of all environments that were specified in LM work statements.

These environments were considered both singly and in combination. Where applicable, both operating and non-operating modes were considered. Environmental usage factors were established as a result of an extensive survey of literature available and specific experience. This research resulted in the establishment of specific K factors or multipliers to be applied to basic equipment part failure rates as they were measured under laboratory or ground conditions. Failure rates as modified by the applicable K factors were used for the reliability apportionments and predictions during the earlier phases of LM equipment design and subsystem configuration studies. All articles which had endured an environment known or unknown such as unplanned shock or vibration, thermal humidity or other similar environments were recorded and listed as suspect failures. All such hardware was serialized and set up under separate special failure data reporting criteria.

CONFIGURATION ANALYSIS (TRADE-OFF STUDIES)

Configuration analyses were prepared to assist the design engineers in making decisions which would tend to optimize each design. Configuration analyses compared alternate design configurations, logical designs, functional arrangements or any other schemes that might affect the reliability and/or maintainability of the equipment. These studies were made in such a manner so as to assist the designer in selecting an optimized design configuration. A systematic approach was established which would consider all possible schemes and arrangements before specific design decisions were made. In each configuration which was examined, significant parameters were evaluated and identified. Included in these parameters were items such as cost, performance, life, maintainability, reliability, schedules and fail-safe features.

The various configurations that were considered usually consisted of different arrangements of components or functions which all yielded the same result in the main operating mode, but which could have involved different degrees of redundancy and different degraded modes of operation. The significant affect of each parameter was evaluated quantitatively by using failure rates or estimates of failure rates based on complexity, the configuration or the operational profile. Where sufficient equipment operating data was not available, figures of merit were estimated and applied to failure rates. However, relative values indicating the importance of the parameter within the scope of a particular investigation were sometimes used for purposes of establishing optimum trade-offs and thus arriving at the best configuration.

CIRCUIT ANALYSES

Where appropriate, circuit analyses were conducted at various phases of design. These analyses were aimed at the ensurance of optimum application of component parts and the proper functioning of the particular circuit under worst case conditions. Tolerance variations of parameters, signal inputs, environmental extremes and so forth were included as part of the designer's engineering notebook. Where circuit analyses were not performed on specific circuits, justification for eliminating the analyses was always required. Justification for this omission was included in the engineering notebook material.

DEFINITION OF FAILURE

A failure was defined as the inability of a system, subsystem, component or part to perform its required function within specified limits under specified conditions and for a specified period of time for all failures even though the cause might have been other than an inherent part fault. This type of cause could have been an item such as: failure of another part, human error in handling, and failure of test facility or instrumentation.

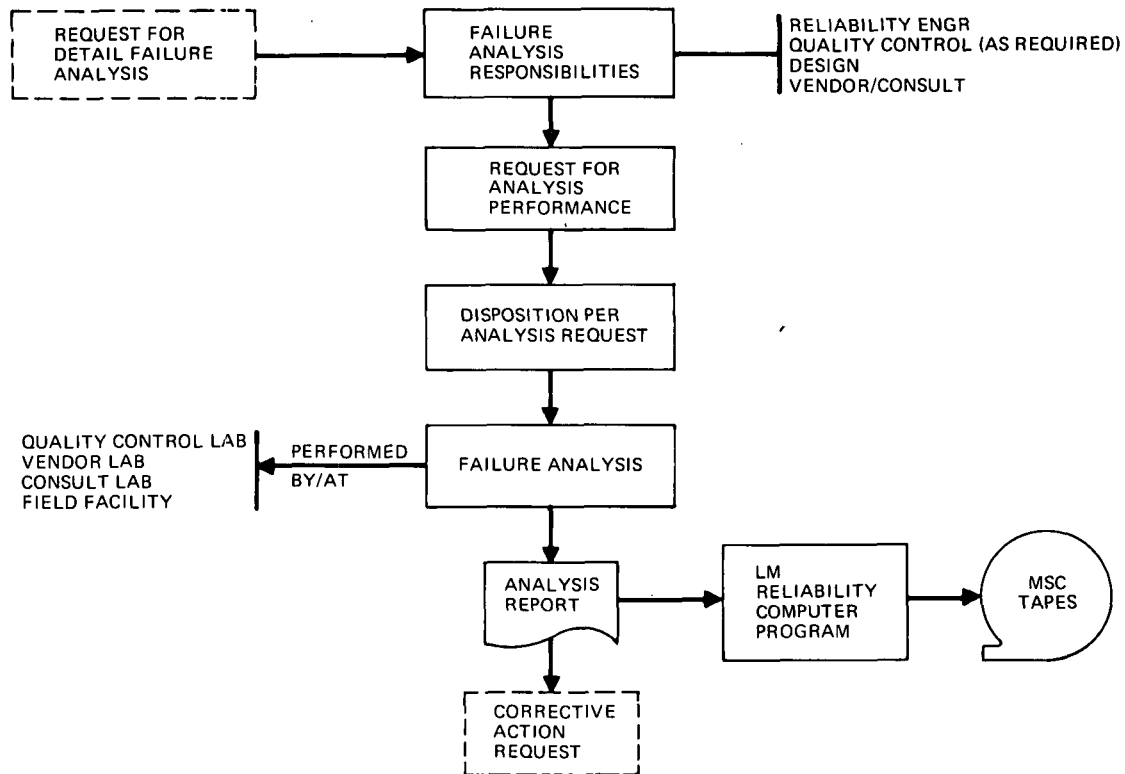
Failure types were categorized as follows:

- Primary - self-induced by the failed item
- Secondary - induced by outside action--not an inherent fault of the failed item
- Suspected - an initial classification which required additional analyses
- Off-Limits - caused by intentional overstressing
- No Failure - a classification designated when there have been no equipment damage or degradation in performance by test

- Failure Criticalities - failures were ranked in order of criticality in the following manner:
 - (1) failure resulting in subjecting crew or ground personnel beyond emergency limits
 - (2) failure resulting in an abort or launch delay
 - (3) failure resulting in lesser incidents (degradation in mission objectives)
 - (4) none

FAILURE ANALYSIS REQUIREMENTS

One of the most extensive elements of the LM Reliability Program was the program of failure analysis. All failures which occurred during the design verification testing, qualification testing, system integration checkout, and flight and ground test were analyzed and the results of these analyses were reported to both Grumman and MSC. For each failure occurring in these program phases, detail analyses were performed. In some cases these analyses were paper analyses, in other cases they were hardware analyses, or in some cases special tests were performed. Subcontractors were assigned the primary responsibility for performing analysis of failures at their facility with Grumman reliability or subsystem engineers monitoring this activity. All analyses require documentation with the results fed to the LM Failure Data Group which, in turn, distributed the analyses to the appropriate organizations which were then alerted by a failure report (refer to Figure 4).



CONTRACTOR CONTROL OF THE FAILURE ANALYSIS PROCESS OFFERED END-TO-END
 VISIBILITY OF FAILURE AND CORRECTIVE ACTION INFORMATION

Fig. 4 Failure Analysis Determination and Sequential Activities

The LM reliability organization assumed the responsibility for proper and prompt initiation of failure analysis. The analysis itself was sometimes a joint effort or a team effort with the team composed of cognizant subsystem engineers in addition to engineers from quality control and reliability supplementing vendor representatives. The cognizant hardware engineer was responsible for the technical accuracy and adequacy of the analysis. He was also responsible for establishment of sound basic conclusions related to the failure. Reliability engineers were also required to concur with the technical validity of the analysis and assume that the corrective action so indicated was actually implemented.


```

graph TD
    Vendor[VENDOR  
FAILURE REPORT  
FAIL. ANALYSIS  
CORRECT. ACTION  
OR RECOMMENDED  
CORRECT. ACTION] --> ReliabilityFIR[RELIABILITY  
F/R GROUP  
FAILURE REPORT  
CONTENTS  
PHONED]
    ReliabilityFIR --> ReliabilitySSE[RELIABILITY  
S/S ENGINEER  
TRANSMITTAL  
REPORT  
RECEIVED]
    ReliabilitySSE --> CognizantSSE[COGNIZANT  
S/S ENGINEER  
COPY]
    CognizantSSE --> RASPO[RASPO  
COPY]
    Vendor --> ValidationCenter[VALIDATION  
CENTER]
    ValidationCenter --> ReliabilityFDR[RELIABILITY  
FAILURE  
DATA  
GROUP]
    ReliabilityFDR --> ReliabilityTransfer[RELIABILITY  
TRANSFER DATA  
TO TRANSMITTAL  
SHEETS]
    ReliabilityTransfer --> ReliabilityComputer[RELIABILITY  
COMPUTER  
PROGRAM  
PREPARE  
TRANSMITTAL  
TAPE]
    ReliabilityComputer --> MSC[MSC  
WEEKLY  
RECEIPT TRANS-  
MITTAL TAPE]
    ValidationCenter --> STD[STD DIST  
COGNIZANT  
ENGINEER  
QC ETC]
    STD -- RESPONSIBILITY --> FollowUp[FOLLOW-UP  
OF FA & CA]
    ReliabilityFDR --> CognizantCoord[COGNIZANT  
RELIABILITY  
COORDINATION  
AND OTHER  
PERSONNEL]
    CognizantCoord -- MONITOR & CONCUR --> FollowUp

```

Fig. 5 Vendor Failure Reporting Data Flow Vendor Acceptance and Qualification Test Failure

As a final link in closing out the failure reporting program, effective corrective action was required in order to ensure that no failure ever remained "open" at critical program milestones. It was the responsibility of the reliability organization to monitor the status of all corrective action and to pursue those items requiring necessary and timely technical close-out. The definition of corrective action used was varied and was considered as the action by which a failure was resolved or by which the recurrence of the failure was minimized or eliminated. Immediate corrective action was defined as that action taken immediately after the non-conformance was first identified. An example would be: "removed for failure analysis--replace with spare to continue test." This action was generally applied to an article which has suffered an induced failure or a secondary failure. Final corrective action had to be applied to the cause.

Final corrective action meant that the application of recurrence control taken to eliminate further repetition of the cause was implemented. Final corrective action was usually applied to primary failures where the failure mode was inherent to the article suffering failure and was self-induced.

PARTS AND MATERIALS PROGRAM

A rather extensive program for component part control of electrical parts and materials was undertaken (refer to Figure 6). This control program provided for the approval of parts selection which included vendor selections, part application, part specifications, determination of part qualification status and the performance where required of qualification tests and the review of failure data. The materials program was under the cognizance of the Systems Structural Analysis Group. Mechanical parts and components were selected and reviewed for application in the specific subsystem design and analysis areas rather than allow the creation of a separate Mechanical Reliability Parts Group.

PARTS SELECTION

Wherever possible, parts were selected on the basis of adequate data history and/or demonstrated reliability. Knowledge that the components were qualified for given application and selected from sources with good manufacturing procedures was also considered very important. As a general rule, parts that were already qualified as applicable MIL-STD or hi-rel parts were used. Parts selection and approval cycle included the review and approval of all parts by the Reliability Parts Group. This review is required on all production and all components used in production flight equipment. These reviews examine both the capability of the part to meet the LM environment and the capability and experience of the part vendor. In order to assist in this review, non-preferred part approval requests were submitted to the Parts Group as soon as the need for a particular part was recognized. The requests were accompanied by available test data to verify that both the part and the vendor were acceptable. In the process of selecting parts or of acting on parts approval requests, reference was generally made to available data from the Interservice Data Exchange Program (IDEP), other Apollo usage and any other data sources for references that were available.

The implementation of parts standardization was augmented by the establishment of an acceptable parts list (APL). Parts selected from the APL had automatic selection approval when they were procured from the vendors that were listed as qualified. The APL was updated, as required, depending generally upon the status of new or marginal parts. The APL contained only parts which were considered acceptable for use on all equipments. Unless a component met those requirements, it was not listed even though it might have been approved for use on specific hardware.

PART APPLICATION

The application of components within circuits was also approved by the LM Reliability Parts Group before the part could be utilized in a production flight equipment. To accomplish this approval process, all parts were listed on a reliability data list (RDL) and submitted with schematics for design reviews. The review of the data lists included a review of the part application for compliance to the LM rating policy - a check on the part selection status of all parts listed.

PART SPECIFICATIONS

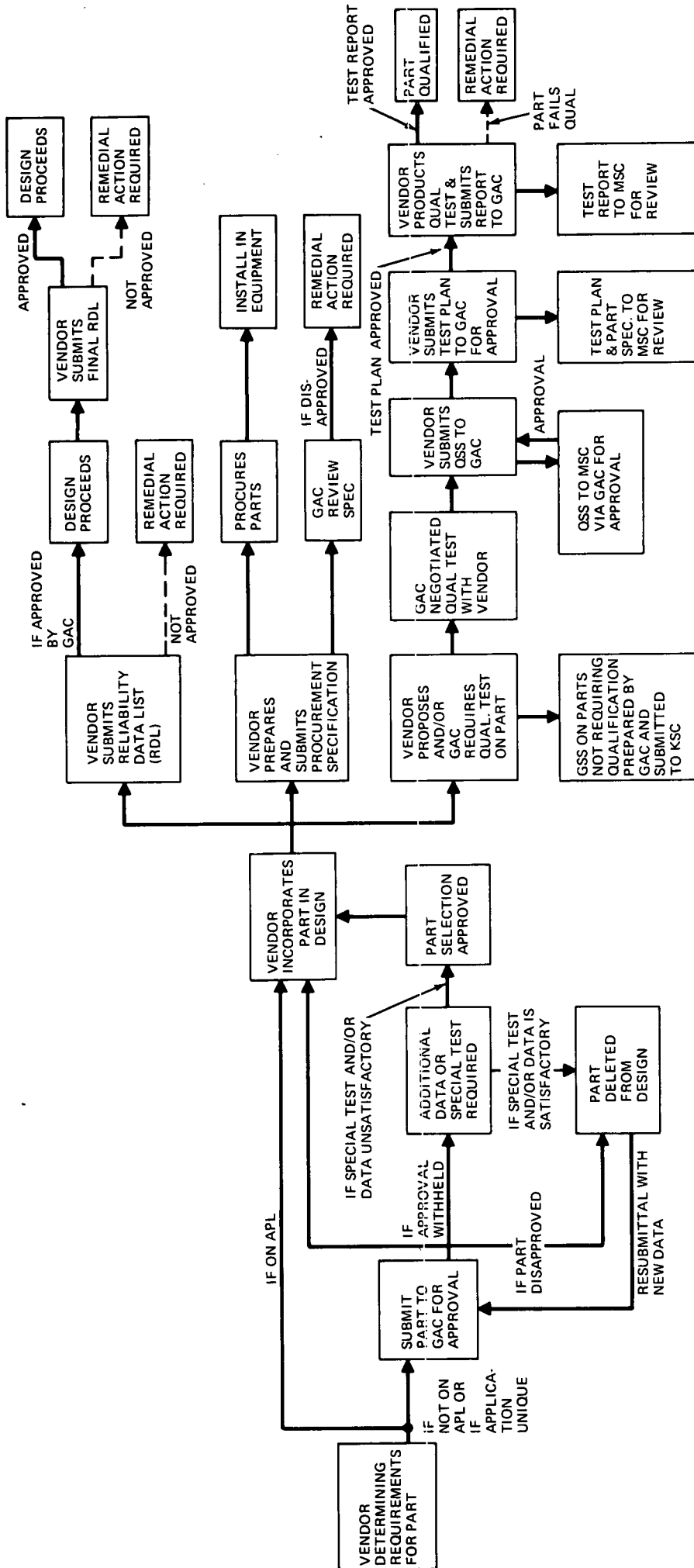
All Grumman and subcontractor parts specifications were reviewed by the Parts Group to assure that the parts that have been approved for use on LM were properly procured. The part specification review was designed to determine that the specification adequately covered such areas as:

- Performance and environmental requirements for the application including where applicable tolerances and parameter changes with life and environment
- Identification and data provisions compatible with the approved traceability requirements
- Complete qualification requirements - in general, part qualification requirements paralleled the requirements of the applicable military specification with appropriate additions or modifications, where necessary, to verify performance under a specific LM environment.
- Reliability and quality assurance provisions such as screening and burn-in to eliminate potential failures and to stabilize, where appropriate, the part characteristics

PART QUALIFICATION

All parts used on LM production flight equipment were qualified. Qualification status was decided upon by the Reliability Parts Group by comparing available data on the part to the requirements of the part procurement specification. Data sources used to conduct this evaluation included:

- Parts reliability information center (prints)
- Mil-specifications and QPL's (i.e., MIL-R-390000 series)
- Interservice Data Exchange Program (IDEP)



THE FOUNDATION OF THE LM RELIABILITY PROGRAM WAS THE PARTS CONTROL PROGRAM. ALL REQUESTS FOR PART USAGE WERE CAREFULLY REVIEWED BY THE CONTRACTOR AND TESTS REQUIRED IF NECESSARY TO VERIFY PART ACCEPTABILITY

Fig. 6 LM Parts Control Program Flow

- Other Apollo contractors
- Contractor in-house testing
- Electronic Component Reliability Center (ECRC)
- Tests conducted by the manufacturer as specification requirements
- Apollo parts information center
- Parts and materials master file

The generalized goal of the LM program was, of course, to utilize parts which had adequate reliability background which would then tend to minimize the need for special qualification testing. Where analyses showed that a part was in need for qualification testing, a decision was generally made to qualify the part by testing it to necessary environments or to qualify the part during a higher level of assembly qualification test.

Subcontractors were not allowed to qualify components until they were so directed by Grumman. Lists of parts which were in need of additional qualification testing were transmitted to NASA for approval and concurrence.

Failures during part qualification testing were reported and analyzed and suitable corrective action was taken within the parts qualification program. Action impacting equipment was dependent upon the numbers of failures experienced, the mode of failure, the usage of the part and the equipment, and the impact of the part failure on the success of the parts qualification program. Close out of part failures were accomplished only after completion of a detailed failure analysis and determination and implementation of corrective action.

TESTING AND RELIABILITY EVALUATION

The LM test program was planned to provide practical maximum amount of reliability assurance within given Apollo program constraints of schedule and cost. The LM reliability evaluation was implemented in two basic ways: by making maximum utilization of all test data to support and to periodically upgrade reliability analyses and by providing estimates of selected equipment operating time experience during testing.

Qualitative information gathered from the results of tests were compared with the assumptions that were made during reliability analyses. These comparisons were made to determine whether a significant difference existed either in terms of the mode or mechanism of failure or the failure consequences. Where major discrepancies existed between the test results and the analysis, analyses were updated to account for the test results.

TEST PROGRAM SCOPE

The test program was planned to provide a thorough test evaluation during the design and development period in order that equipment would enter the qualification test program with the assurance that they would pass without the need for a major significant redesign. The basis of the testing and evaluation program was that a comprehensive test program at the equipment and subsystem level would also reduce to a minimum the likelihood of costly schedule delays and integrated system test and further delays in the flight development program. The program of reliability evaluation also assured program management that the LM design was verified at each significant program milestone and that problem areas were brought to light and given the proper attention befitting their importance.

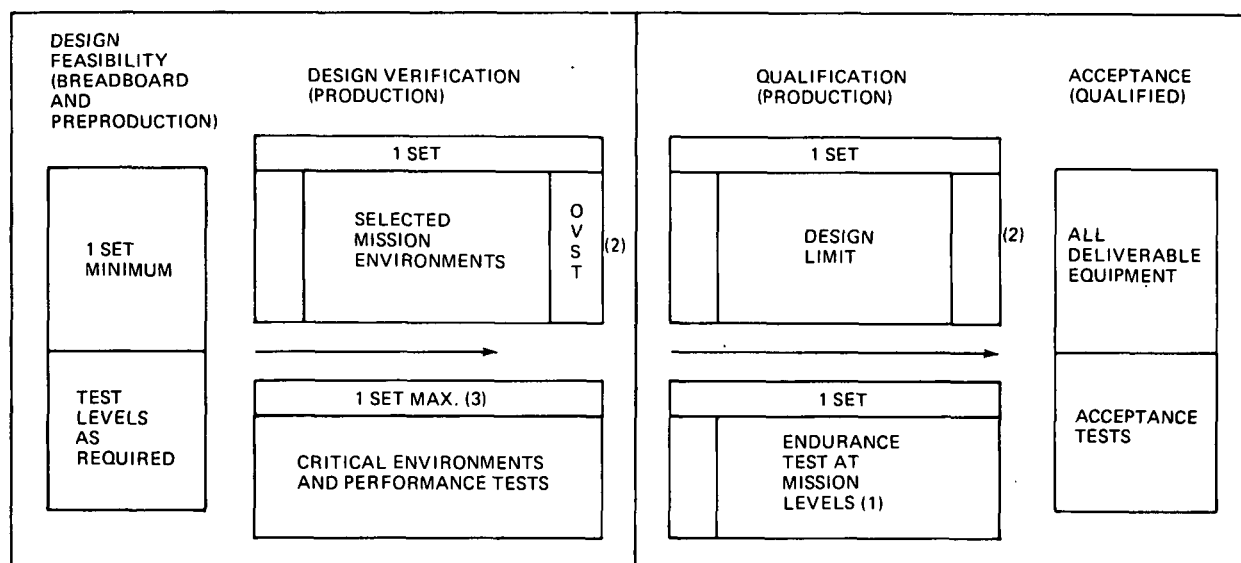
TESTING CONCEPT

The LM test program was broken down into several phases. Developmental testing was divided into two categories: design feasibility tests and design verification tests. (Refer to Figure 7.)

DESIGN FEASIBILITY TESTS

Design feasibility tests were performed for the purpose of verifying component and part selection, verifying the selection of materials, investigating the performance of breadboard models, components and subassemblies under selected environmental conditions. They were also used as a substantiation of the safety margins and analytical assumptions such as material allowables, bonding concepts, temperature response to circuitry and so forth.

Electrical parts and components were evaluated using design feasibility tests and in some cases as a result of these evaluations, components were placed on the LM acceptable parts lists. Promising parts, for which back-up data was either incomplete or not necessarily related closely enough to permit approval, were generally subjected to special tests under the design feasibility test program in order to verify that they could indeed meet the requirements for inclusion on the acceptable parts lists.



1. MINIMUM OF TWO MISSIONS
2. OVST - OVERSTRESS TEST
3. WHERE PRACTICAL ALL OBJECTIVES OF DVT ARE ACCOMPLISHED ON ONE TEST ARTICLE.
 WHERE PRACTICAL THE MALFUNCTION, ENVIRONMENTAL, PERFORMANCE TESTS WILL BE INTEGRATED WITH,
 OR THE HARDWARE REFURBISHED FOR THE STRESS-TO-FAILURE TESTS

Fig. 7 LM Subsystem Test Cycle

Materials for which there was no prior documentation or testing also established a suitability for use on LM during the design feasibility tests. For structural materials, strength and fatigue properties were established for selected materials or processes in order to evaluate allowable stresses for LM application. Welded connections, rivets, bolt patterns, honeycomb structures and special fabrication techniques were tested using LM use-type environments. Where applicable, structural materials and processes were investigated as to their dimensional stability and susceptibility to thermal gradience, thermal conductivity, thermal shock and mechanically induced shock.

All materials were evaluated and/or tested to establish their flammability characteristics in an oxygen environment. In addition, all potential sources of ignition were evaluated.

Mechanisms, bearings and mating surfaces were tested under ultra high vacuum in order to establish their capability of operating in the outer space vacuum. Problems of cold welding and interfaces such as those between the ascent and descent stages were thoroughly investigated. Sublimation studies and off-gasing tests of thermal protection coatings, lubrication materials and bearing surfaces were also conducted. All non-metallic materials, potting compounds and coatings were probed for toxicity properties.

Sealing materials and concepts were also tested for off-gasing characteristics, contamination affects on fluids, leakage and permeation. Adhesive allowables were established for static loading and fatigue properties. Structural configurations which were novel or difficult to analyze were thoroughly tested under static load and vibration or any other environment which was necessary in order to verify strength and stability and to support existing stress analyses.

DESIGN VERIFICATION TESTS

Design verification tests were performed at advanced stages of development and were performed on components, assemblies and sections for the purpose of substantiating the correctness of the design for its intended mission. These tests were conducted generally under simulated mission environments and off-design conditions. Successful completion of design verification tests provided needed assurance that a design freeze decision could be made. Design verification tests were conducted on hardware which was in its production configuration. Off-design tests were conducted to determine the limit of performance capability. For example, malfunction tests were conducted on propulsion hardware and in hot firing tests of engines. These tests simulated upstream malfunctions of the feed and pressurization systems resulting in such parameter verifications as excessive propellant temperatures.

Design verification tests were also conducted to determine the readiness of the hardware to pass qualification tests. In addition, electromagnetic interference and other interface problems were thoroughly investigated and eliminated prior to the qualification test phases.

Overstress tests were incorporated as an integral part of the design verification phase, in order to increase the engineering confidence in the LM equipment by providing vital and timely information about the design and quality of the hardware. The overstress tests fulfilled a twofold role in supporting the design effort and enhancing the engineering confidence in the reliability of flight hardware. Overstress testing verified equipment strength margins. It identified weak links and failure modes and verified assumptions made during the reliability analyses. Overstress tests probed in the direction of least knowledge. The environmental test levels and the overstress tests were varied beyond the range of stress levels which were categorized as mission design and qualification test levels. Knowledge of equipment failure modes was gained as a product of all LM tests; however, the overstress tests were used extensively to evaluate failure modes that were produced directly as a result of the test program. Failure modes which occurred at levels close to mission level environments or failures which were catastrophic in nature were identified and often eliminated by strengthening the design and increasing design safety margins.

QUALIFICATION TESTS

Qualification tests were, in general, conducted on at least two production units of each equipment. These tests were designed to demonstrate the complete suitability of the hardware for the LM mission. In general, the tests were run on the highest level of assembly which was deliverable to Grumman. One of the qualification units was normally subjected to the critical environments of an operating cycle and tested at the design limit levels, while the second unit was subjected to a complete operational cycle plus one additional flight simulation which was an endurance test at mission levels. Prior to any qualification test, the equipment was subjected to an acceptance test in accordance with the applicable detail specifications. Following a successful completion of a qualification test, the test units were subjected to additional tests in order to increase confidence and provide additional information on design life and strength margins. The design limit test unit was subjected to overstress test in the same mode or condition as selected for the design verification overstress test unless the results of subsequent testing indicated otherwise or unless it was so dictated by a design change. Equipment failures which were experienced during post-qualification testing did not necessarily invalidate qualification test results but were always brought to the attention of program management for evaluation of their impact on the flight worthiness of the hardware. Post-qualification tests were not performed on all hardware, only those considered critical.

ACCEPTANCE TESTS

Acceptance tests were performed on all deliverable items in order to verify that the equipment met the design and quality standards prescribed in the detail specifications. Acceptance tests conditions were never more severe than the expected flight conditions and included factors of safety and margins of life and eliminated environmental stresses where applicable.

INTEGRATED SYSTEM TESTS

An integrated system test article was developed and test run on a LM type vehicle assembly verifying the degree of completeness to develop particular subsystem interactions under environmental conditions such as temperature, vacuum, vibration and so forth. The purpose of the integrated system test was to evaluate the system performance under space environments to be experienced by LM. The tests also evaluated off-design and alternate mode capability of the system. Where so designated, the system development test plans were written in such a way that the test assumed the qualification-like rigor in order to provide certification. Items evaluated during integration tests included electronic integration, landing stability, structural strength, thermal vacuum balance, vibration stability, propulsion integration, and manned LM environment integration. The data generated from integrated system tests were used to verify the performance and the environmental assumptions that were made during the reliability analysis. Failure data was used to verify failure mode predictions and analyses and failure mode effect analyses. Failure data from system tests was also correlated with overstress tests to evaluate stress levels and margins of strength and safety.

CERTIFICATION TESTS

As previously discussed, the overall LM test program concept was broken down into several phases: design feasibility tests, design verification tests and certification tests (considered for production hardware). At the beginning of the Apollo program,⁽⁴⁾ three test concepts were studied to determine the optimum method for certification testing. The first concept considered a statistical demonstration type program that would provide a rigorous treatment with statistically demonstrated reliability quantities for all hardware. This would also produce a significant amount of test data and test experience on production hardware. It was determined that this approach required an impractical amount of test hardware with associated large test costs and serious schedule implications.

The second type of certification test considered was a non-time oriented design limit test in which production hardware would be used to demonstrate the capability of the hardware to withstand the severity

of the flight environments increased by some factor of safety. A limited amount of test data would be obtained rapidly with this type of testing and their tests would require a limited amount of test hardware. This type of testing, however, would produce no statistical confidence in the reliability of the hardware. Also, the time oriented sequential exposure of the hardware to the levels in durations of the environments expected in flight would have to be omitted.

The third certification test concept which was considered was an integrated test and analysis program in which two production units of hardware would be used. One unit for design limit testing and the second unit for mission life testing. This approach did not require an excessive amount of hardware and would demonstrate the capability of the hardware to withstand the spectrum of environmental magnitudes and durations with adequate margins of safety greater than those expected in flight. More test articles were required during the testing of certain critical items such as some of those associated with propulsion systems and some of the high usage items such as switches and relays. Although a statistical demonstration of the reliability of hardware was not obtained with this type of testing, this approach would provide a significant degree of confidence in the design. The acceptance test then could provide the necessary confidence in the quality of the flight hardware.

This third test technique was selected for the Apollo program and used extensively on LM. Testing was performed at the replaceable level of assembly and at selected higher levels of assembly to insure equivalent certification testing of the entire spacecraft. Testing was performed on hardware ranging from switches, dials and meters upwards through gyros, computers, valves, tanks and in some cases complete engines. A total of 505 certification tests were performed on Lunar Module hardware. Completion of these tests were required before flight. The complete subsystem level and vehicle level test were also included in the program to demonstrate the design capability of the interfaces between various hardware elements. One hundred seventy-five such subsystem or vehicle level tests were performed on LM.

The establishment of certification test requirements to which LM hardware was to be exposed was a rather lengthy one and in some cases an iterative process. The design environments were known but some of the level and duration requirements were developed over a long period of time. The determination of the items to be exposed to a particular environment at a particular level and duration was performed on an item-by-item basis. This determination was made by an assessment of the type of hardware construction, the location of the hardware on the spacecraft, the expected duration of exposure of the hardware to environment whether the hardware was operational during, before or after exposure. Conservative levels of environmental testing were selected to provide an adequate margin of safety greater than the severity of the environments expected during flight. At the same time, care was taken to prevent the use of unrealistically severe environmental levels. The sequence in which the environments were applied to the test articles roughly approximated the sequence in which the flight article would be subjected to these particular environments during the ground and flight life of the article.

FLIGHT TESTS

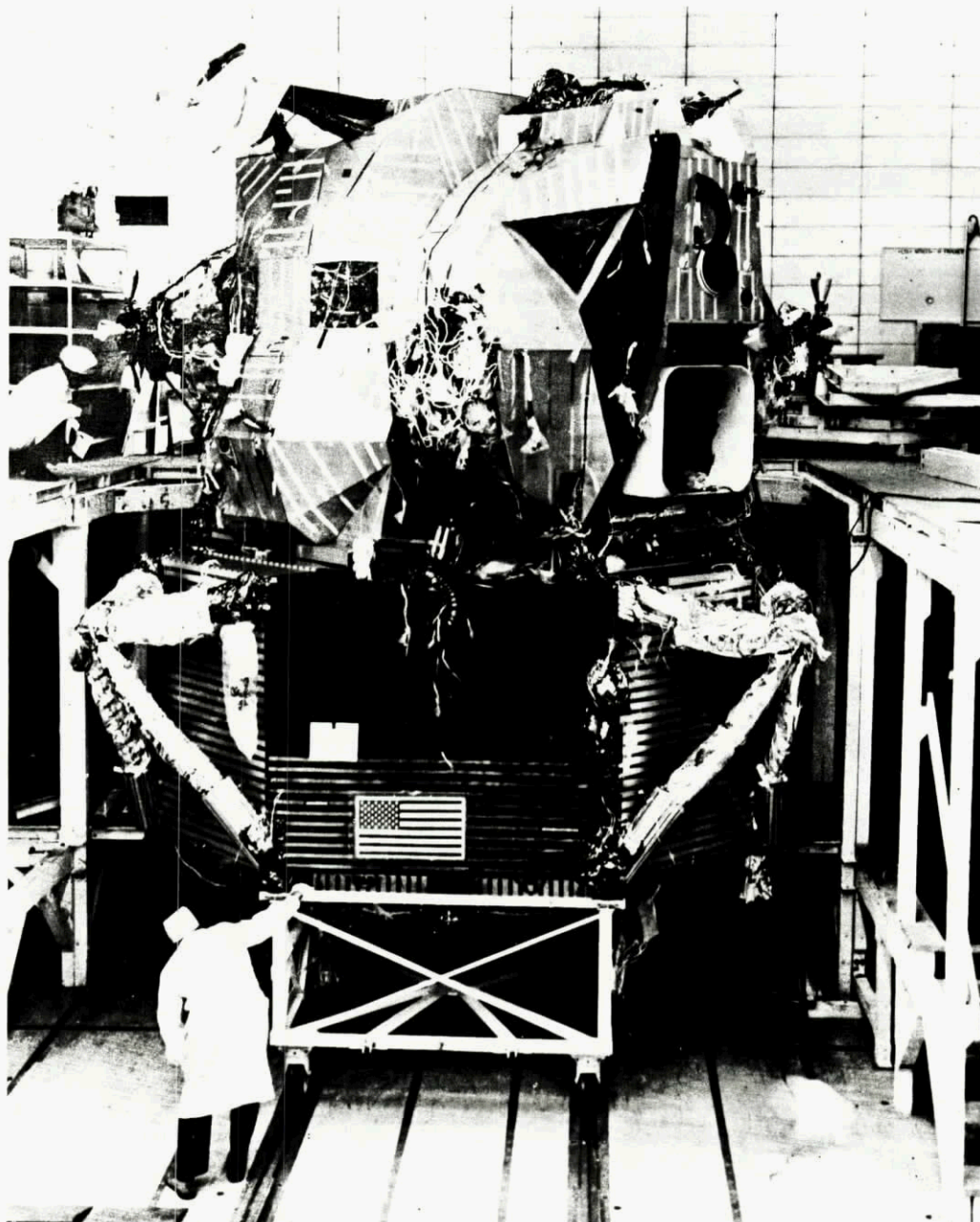
The LM flight test vehicles were subjected to two basic test phases--pre-flight and flight tests. Pre-flight tests were run to verify the flight readiness of the LM vehicle. Portions of these tests were run under environments when it was required for subsystem performance evaluation. The data resulting from the extensive checkout and operational tests verified in many cases design assumptions and provided additional confidence in the reliability analyses.

Flight tests were run to verify the performance capability of the LM system by a step-by-step advancement through actual mission environments and maneuvers. The flight tests provided data of greater significance to corroborate the reliability estimates of LM's lunar mission capability. Subsystem performance parameters were recorded by a data link. This data was analyzed to evaluate subsystem reliability and document any equipment failures or any performance degradations. This data was also correlated with failure mode prediction and failure effect analyses results.

CONTROL OF CHANGES

We would like to assume that once a design has been verified and a thorough test program has been completed that it should not be necessary to make any additional design changes. On a program such as LM, however, this is not possible and it is certainly nothing more than an idealized situation. In this case where the design, test and flight operation phases in some cases overlap or were carried out at the same time, changes were quite often required as a result of certain types of test failures or perhaps a new look at the design or perhaps even a feedback of flight anomaly information. In some cases a redefinition of the flight profiles or mission criteria or changes in the operational use of the hardware itself led to the necessity for a design change. The assumption made on the LM program and, as a matter of fact, throughout the Apollo program was that any change was an undesirable one. Since a design change tends to void all previous test or flight experience, a change no matter how simple could have serious implications and had to be carefully analyzed.

Because of the nature of the LM program, design changes had to be made on repeated instances. When these changes were made, it was considered of ultimate importance to understand the changes and to provide necessary controls no matter how large or small a design change was involved. All changes



LTA-8, a complete LM spacecraft, was designed for thermal vacuum environmental testing in the large environmental test chamber at the Manned Spacecraft Center. The vehicle is shown in preparation for delivery. Visible are the special heater skins containing electrical heater strips which are externally controlled to provide skin heat inputs simulating the solar inputs to the spacecraft during space flight.

were handled through a series of configuration control panels and a configuration control board. The panels considered the minor hardware changes that took place early in the development cycle as well as the crew procedures and all computer programs. The configuration control board considered the more significant hardware changes. Also included under their purview were all hardware changes after spacecraft delivery as well as procedures or software changes that could have a schedule or a mission impact.

An example⁽⁵⁾ of the activity and depth of review by these panels and boards is illustrated by the fact that the configuration control board on the Apollo program met 90 times between June 1967 and July 1969. During this time interval, 1697 changes were evaluated. Of these, 1341 were approved and 356 rejected. The low rejection rate was attributed to the fact that all proposed changes were carefully reviewed by several levels of contract and NASA management before they came to the configuration control board and only those that were considered absolutely mandatory for flight safety were actually brought before the

board. The board consisted of the NASA Program Manager who was considered the chairman who also ruled on most final decisions on all changes. The board also consisted of the Directors of all major technical elements of the NASA Manned Spacecraft Center. The contractor's Program Managers also served as board members.

RELIABILITY DESIGN FEATURES

The LM is a two-stage vehicle comprised of a descent or lunar landing stage beneath an ascent or lunar lift-off stage. The descent stage contains the descent propulsion systems, landing gear, expendable fluid and batteries and the Apollo Lunar Scientific Experiment Package (ALSEP). The ascent stage, the inhabited portion of the spacecraft, contains two astronaut crew stations with cockpit display and controls, environmental control and crew provisions within a pressurized crew compartment. The ascent stage also contains the flight control system, guidance and navigation, ascent propulsion, and all other electrical/electronic systems such as electrical power, communications and instrumentation.

Referring to Figure 8, prominent features include the rectangular front hatch, from which the astronauts egress to the lunar surface, and the triangular front windows. The reaction control jet clusters

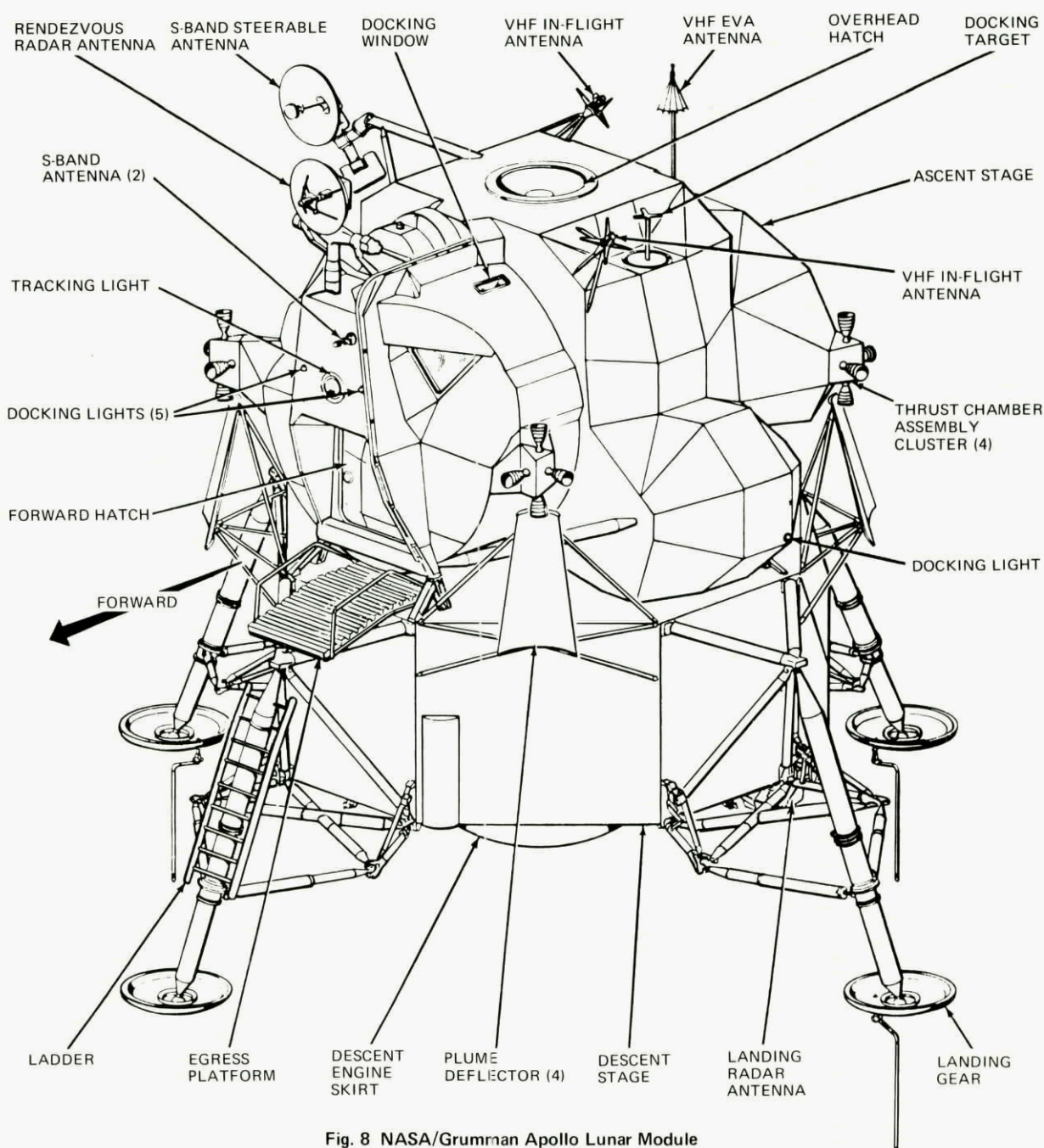


Fig. 8 NASA/Gumman Apollo Lunar Module

are also visible; four 100-lb. thrust jets in each of four clusters provide two fully redundant reaction control systems. The rendezvous radar antenna is mounted atop the cabin front face; it is connected to the navigation base structure for accurate alignment with the primary and the abort guidance systems inertial sensors. The S-band steerable communications antenna is mounted on the starboard side midship; it is the primary communications and ranging link with earth at lunar distances. Other ascent stage antennae are the bedspring-shaped VHF omni used for LM-CSM-astronaut communication, the small cone-shaped S-band omnis, and the C-band scimitar, which is used for beacon tracking on earth orbital flights only.

Principal external features of the descent stage include the outrigger struts, to which the landing gear attaches, and by which the LM is attached to the Spacecraft/LM Adapter, or SLA, in which it is mounted when stacked on the Saturn launch vehicle. The landing gear consists of four retractable legs with aluminum alloy honeycomb foot pads and crushable honeycomb energy-absorbing struts. The nozzle extension of the throttleable descent rocket engine can be seen beneath the base of the descent stage. It is made of thin columbium sheet, and is designed to crush upon impact with the lunar surface.

Much of the electronic equipment is mounted on an equipment rack aft of the crew compartment, where it is readily accessible while on earth. The equipment is attached by heat-conductive flanges to extruded aluminum cold rails, through which chilled water-glycol is circulated.

The entire spacecraft is isolated from the thermal extremes of space with super-insulation blankets of multiple layers of extremely thin 1/8 mil aluminized mylar. Outer coverings of 1/2 mil aluminized H-film provide toughness and fire resistance to the blankets. The insulation blankets are supported from the vehicle structure by low-conductivity fiberglass stand-offs and are covered by a 4 mil thick aluminum alloy skin, which functions as a meteoroid bumper in space. The thermal radiation properties of the skins are carefully controlled to provide the required equilibrium temperatures in sunlight or shadow. Various skin coatings are used in different areas of the spacecraft to satisfy the temperature requirements of different equipment or fluids. In some areas, high-temperature resistant nickel foil is used as an outer layer over the aluminum skin to protect against reaction control jet plume impingement, or thermal radiation from the engines.

The crew compartment interior is shown in Figure 9. A significant weight saving was achieved by

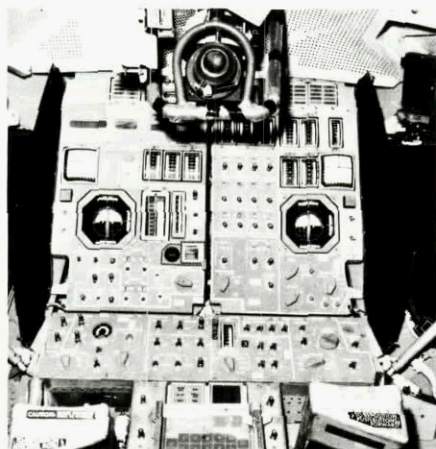


Fig. 9 LM Crew Compartment Interior

dispensing with conventional seats or couches and adopting a stand-up crew position. Flight control is maintained by a pair of hand controllers at each crew station. The primary flight instruments are duplicated to make it possible to fly the spacecraft from either crew station, and other controls and displays are either shared or operated from a single station. A small window above the Commander's head is used to observe the Command and Service Modules (CSM) during the docking maneuver. Stowage for crew equipment, and for the two portable life support systems (PLSS) are provided in the cabin areas behind the crew station, and under the side display consoles. The environmental control systems manual controls are located behind the LM pilot, and the electronics equipment for the primary guidance, navigation, and control system is located on the aft bulkhead of the crew compartment.

SUBSYSTEM DESCRIPTION

A brief description of key LM subsystems is included to illustrate the level of technology and design approach used throughout the spacecraft.

Ascent Propulsion - Emphasis has been placed on assuring reliability of the key subsystem by design simplicity (see Figure 10). The system is pressure-fed by stored gaseous helium, uses earth-storable hypergolic propellants (50/50 hydrazine/UDMH fuel; nitrogen tetroxide oxidizer, the same propellants as LM descent propulsion and RCS, and the Service Module propulsion system), and has a single fixed-thrust engine with ablative nozzle and combustion chamber. The trunnion-mounted titanium propellant tanks have been extensively analyzed and tested to provide a light-weight design with adequate safety factors.

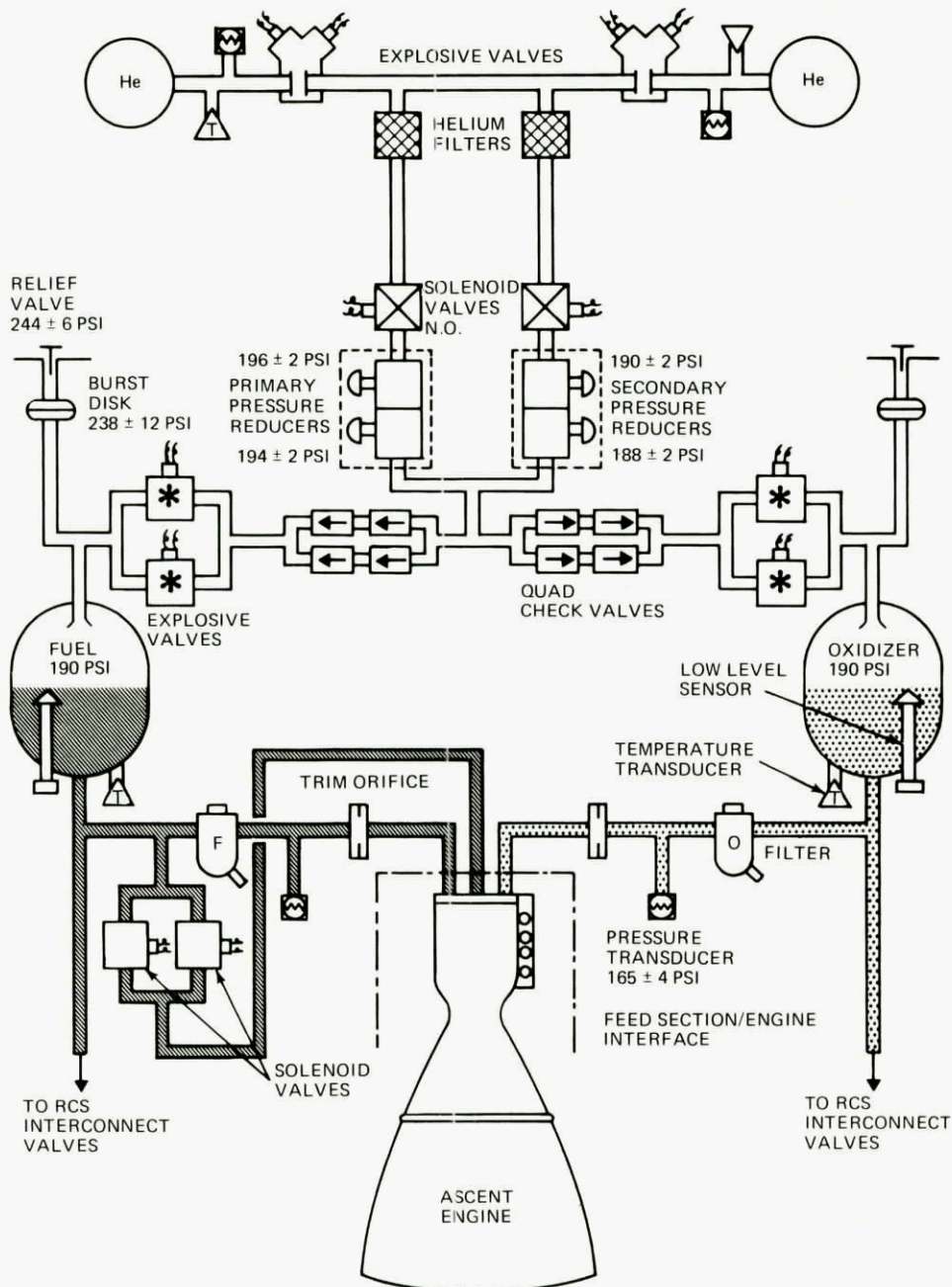


Fig. 10 Ascent Propulsion Subsystem

ENVIRONMENTAL CONTROL

Life support for the crew, including cabin re-pressurization and provision for recharging the primary life support system during lunar exploration, is provided by the Environmental Control System. The ECS also cools the electronic equipment through a heat transport loop, and provides water for cooling and for astronaut use. The ECS interfaces with the spacesuit and primary life support system and has numerous redundancies and emergency provisions. Of interest, are porous plate sublimators, in which water absorbs heat from the heat transport and cabin/suit loops, and sublimates into the vacuum of space and the centrifugal water separators, driven by the oxygen flowing in the cabin/suit loops. The ECS oxygen system provides a nominal 5 PSIA pure oxygen environment, and is demonstrated to a maximum of 5.8 PSIA in ground tests.

ELECTRICAL POWER

The electrical power subsystem also emphasizes simplicity and redundancy. The basic power sources are silver-zinc primary batteries, four in the descent stage and two in the ascent stage. Independent power distribution and control is provided to the Commander's and LM Pilot's busses with provisions for cross-tying the busses and isolating any failed battery. Battery circuit protection and switching is provided by two electrical control assemblies in each stage. Basic buss voltage is 28 volts DC with 120 vs. 400 cycle AC supplied to certain equipment by a pair of redundant solid state inverters. An entirely separate redundant power system supplies ignition power for explosive devices from small silver-zinc primary batteries located one in each stage.

SPACECRAFT WEIGHT

LM weight is an ultimate premium, since LM is the payload to which the efforts of the entire six million pound launch vehicle/spacecraft combination are directed. Within LM itself, a major weight growth factor is built into the mission requirements. Each pound of inert weight that is lowered to the lunar surface and then returned to CSM requires an additional 3-1/4 pounds of propellant to carry it down and back. Thus, a pound of inert weight adds a total of 4-1/4 pounds to the separation weight of the LM spacecraft. The criticality of weight was recognized at the onset of the LM program and substantial efforts were directed to its proper accounting and control. However, initial weight growth was alarmingly rapid. In July 1965, the spacecraft had already reached its control weight limit of 32,500 pounds at earth launch, and the weight was still climbing. At this point, an intensive redesign and weight reduction program was initiated. This program was designated SWIP for Super Weight Improvement Program. As part of the SWIP, every aspect of the spacecraft and equipment design was reviewed and analyzed for potential weight-saving. Redesigns were then accomplished wherever they were within pre-determined guidelines with respect to cost and schedule effects. In the course of the SWIP, the structure of the spacecraft was completely reviewed, and many detailed changes involving additional chemical milling, routing, or changes in basic materials were made. The spacecraft equipment was similarly reviewed and wherever the SWIP guideline showed that an acceptable saving in terms of dollars per pound weight reduction could be achieved by equipment redesign, the redesign was accomplished. Functional requirements of all equipments to support the mission were also examined with the result that some operational modes and features which were not absolutely essential for mission performance were eliminated in the interest of weight-saving.

COMMUNICATIONS

Principal design feature of the communications subsystem is the large variety of operational modes which are provided. A high degree of system redundancy is thus obtained, together with flexibility for handling the unique communications requirements of various mission phases.

During LM flight phases, voice communications, ranging, and data transfer with earth over the S-band system, and voice communications with the CSM over VHF are primary mission requirements. While on the lunar surface, the power must be conserved, requiring the deployment by the astronaut of an umbrella-like high gain antenna which he manually aims towards earth. Scientific data transmissions from the ALSEP are beamed out over a separate antenna. When the astronauts are exploring the lunar surface together, communication between them, the CSM, and earth is routed through the LM from the PLSS which the astronauts carry on their backs. A whip antenna atop the LM is manually deployed after landing to maintain the link to the extra-vehicular astronauts.

FLIGHT CONTROLS

A high degree of redundancy and operational flexibility is provided in this subsystem also. The "brains" of the system is the primary guidance, navigation, and control system (PGNCS) which is backed up by an independent abort guidance system (AGS). The PGNCS contains a 4-gimbal platform and general purpose digital computer, and is programmed to provide control as a digital autopilot, as well as guidance functions. Redundant control capability is provided by an analog autopilot, called the attitude and translation control assembly (ATCA) which also interfaces the pilots' controller inputs into the system. The AGS has a strapped-down inertial sensor package, and a smaller computer capable of abort guidance functions only.

Multiple flight control modes are available: For attitude control; automatic, attitude hold, or direct manual control, in normal or pulsed operations; for RCS translation; 2- or 4- jet select and x-axis translation; for ascent and descent engines; automatic or manual control including manual throttling of descent engine; and PGNCS/AGS selection. All these multiple modes result from mission requirements based on the ground rule that no single system failure shall impair crew safety.

The "muscle" of the flight controls, the reaction control subsystem, is also fully redundant, and until the descent propellant is consumed, both descent and ascent engines are available should it be necessary to abort the mission and return to the CSM.

FLIGHT PROBLEM RESOLUTION

Early detection and resolution of flight problems was considered⁽⁶⁾ important both to allow for modification of crew procedures, as necessary during the flight, and to define the required corrective action for subsequent vehicles as early as possible in the testing or manufacturing flow. In order to affect timely resolution of flight problems, early recognition was essential. During each mission a member of the Flight Evaluation Team was responsible for logging any potential problems and assembling all available information necessary to determine if in fact a problem did exist. The sources of this information included Grumman personnel at the Manned Spacecraft Center, with access to CRT data, and evaluation team and system/subsystem personnel within the Grumman mission control room. Crew reports and flight controller reports from the Flight Director's Network were also used for problem identification. Those items considered problems were placed on a preliminary list for discussion at the first post flight problem meeting.

As soon as is practical after the LM active portion of a mission, a Grumman-NASA meeting was convened to discuss the LM flight problems. The attendees included NASA/MSC Test Division and Grumman mission support personnel in Houston and Flight Evaluation Team and system/subsystem engineers at Bethpage. At this time the combined list of LM problems was reviewed. Those items which were readily explained and required no corrective action were eliminated. Problems requiring extensive testing or analysis were classified as anomalies and verbal authorization was given to Grumman to proceed with the Flight Anomaly Investigation (FAI). LM related items which involved Government Furnished Equipment (GFE) were resolved by NASA with Grumman support as required. The remaining items were classified as discrepancies and were resolved by Grumman personnel during the vehicle flight performance analyses. Problems discovered after the first meeting, through data analysis or crew debriefing were classified at subsequent meetings and added to the flight problem list.

Flight problem investigations were directed by the individual cognizant engineers assigned by the engineering manager. For those items classified as flight anomalies, a close-out plan was prepared by the cognizant engineer. The purpose of this plan was to control and sequence the various system/subsystem, vendor and NASA activities required for resolution of the flight anomalies. These plans were updated weekly for review at project meetings.

Problem resolution procedures were followed for all LM mission activities. The attention to detail here, as in all other data-producing phases of the LM program, contributed significantly to the success of the program. Major LM program activities that provided the primary source of test and mission data are shown in Figure 11.

1964	OCTOBER	M-5 - FORMAL MOCK-UP REVIEW
1966	JANUARY	CRITICAL DESIGN REVIEW
	NOVEMBER	FACI/DEI (FIRST ARTICLE CONF INSP/DESIGN ENG INSP)
1967	JANUARY	C/SM FIRE
	NOVEMBER	APOLLO 4 - SATURN V TEST
1968	JANUARY	APOLLO 5 - LM-1 - UNMANNED EARTH ORBIT
	APRIL	APOLLO 6 - CSM UNMANNED EARTH ORBIT
	OCTOBER	APOLLO 7 - CSM MANNED EARTH ORBIT
	DECEMBER	APOLLO 8 - CSM MANNED LUNAR ORBIT
1969	MARCH	APOLLO 9 - LM-3 - MANNED EARTH ORBIT
	MAY	APOLLO 10 - LM-4 - MANNED LUNAR ORBIT
	JULY	APOLLO 11 - LM-5 - MANNED LUNAR LANDING
	NOVEMBER	APOLLO 12 - LM-6 - MANNED LUNAR LANDING
1970	APRIL	APOLLO 13 - LM-7 - MANNED RESCUE MISSION
1971	JANUARY	APOLLO 14 - LM-8 - MANNED LUNAR LANDING

Fig. 11 Major LM Program Activities

The integrity of the LM design was verified by the very few flight anomalies that occurred during mission phases of the program. There were many more incidents that were classified as discrepancies. Flight anomalies were defined as those problems which were considered significant enough to warrant testing and/or analyses since they might impact future flights. Flight discrepancies were considered of lesser importance with resolution generally accomplished as part of the vehicle flight performance evaluation effort. A summary of the LM mission anomalies and discrepancies by mission is illustrated in Figure 12 below.

LM VEHICLE	FLIGHT ANOMALIES	DISCREPANCIES
LM-1	5	
LM-3	9	6
LM-4	5	32
LM-5	2	27
LM-6	2	9
LM-7	1	9

Fig. 12 LM Mission Anomalies and Discrepancies

Typical of the type of flight anomalies evidenced are those discussed in the following paragraphs:

On the LM-3 manned earth, orbit intermittent operation of the Data Entry & Display Ass'y. (DEDA) CLEAR pushbutton resulted in illumination of the DEDA Operator Error light several times during the mission. Micro-switches internal to the DEDA pushbuttons transferred the signal when the button was depressed. In the case of the CLEAR pushbutton, one microswitch transmitted the CLEAR signal to the AGS computer and one transmitted the signal to the DEDA logic. The set of contacts which transmitted the signal to the computer operated intermittently. Investigation isolated the most probable cause of failure to a contaminated microswitch. Corrective action for LM-4 and subsequent vehicles consisted

of a six-position, vibration screening test of the pushbuttons and a wiring modification providing redundant operation of the microswitches.

Also on LM-3 the Exterior Tracking Light (ETL) failed shortly after staging. Tests indicated that the power supply was good and that the failure could have occurred in the pulse forming network, hi-voltage cable or flashhead. The LM-4 ETL had a transient suppression capacitor added. Design improvements effective on LM-5 and subsequent vehicles included: Controlled pressure N₂ bubble, encapsulated inductor assembly, higher reliability terminals, electron beam welded case, improved assembly techniques, improved hi-voltage cable and improved potting and assembly of flashhead.

On the LM-4 manned lunar orbit mission during a 40-second period prior to staging, the yaw gyro in the Rate Gyro Assembly exhibited erratic behavior. Based upon analysis of RGA data, vehicle body rates and AGS downlink data, it was concluded that the yaw rate gyro experienced intermittent "stiction" probably due to the presence of some form of contaminant. An extensive investigation confirmed the fact that contamination was the most probable cause of failure. Corrective action included intensified inspection and testing at the gyro manufacturer, assurance that defective magnets (which led to contamination) were not used in other flight RGA's, and institution of a "stiction" screening test at Grumman. As a direct outgrowth of this corrective action, a re-build program was initiated in order to provide clean rate gyros for future flights.

On the LM-5 lunar landing mission, the LM Mission Timer stopped operating at lunar touchdown. Prior to ascent, the Timer was reset and operated properly. The Timer had a history of failures caused by intermittent solder connections. The failures were due to a combination of the following:

- Weak joints due to MSFC 158A soldering requirements
- Thermal stresses on the cordwood modules
- The high density packaging which made rework difficult

Prior corrective action had consisted of reworking solder connections using convex soldering, a thermal cycle screening test and a burn-in prior to installation of the Timer into LM Display Panel #1. Since additional corrective action on previously built clocks was not feasible, the decision was made to obtain a redesigned Timer from an alternate vendor.

Also on LM-5, the CO₂ Sensor output became erratic during the ascent phase of the mission. Investigation and tests performed by GAC and the Manufacturer resulted in the conclusion that a small quantity of water from the Water Separator Surge Tank migrated to the inlet line of the CO₂ Sensor and was carried by the air flow into the sensor. Droplets of water on the optics of the sensor caused erratic readings and subsequent triggering of the LM Caution and Warning System. As corrective action, a system design change was implemented whereby the vent line from the Surge Tank was relocated to avoid the CO₂ Sensor inlet.

On the second lunar landing (LM-6) the Exterior Tracking Light (ETL) failed during the ascent phase of the mission. The symptoms indicated that the failure was in the high voltage section of the ETL. An investigation of the test and failure history of the subassemblies and components involved failed to isolate any single specific probable cause.

CHANGES RESULTING FROM APOLLO ACCIDENT

The tragic accident in Apollo-204 in January 1967 resulted in a comprehensive review of all potential crew safety hazards in the Apollo program. Numerous changes were incorporated into manned LM design as a result of the accident to eliminate or minimize potential crew safety problem areas. A major re-evaluation of cabin material specifications was also performed. The flammability test for cabin materials have been made more stringent as a result of better understanding of the correlation between flammability behavior of material test specimens and fire behavior in an actual cabin. A basic requirement was established that all cabin materials must be self-extinguishing when ignited by a hot wire in a 6.2 PSIA oxygen environment. Close attention was also paid to reducing flame propagation paths in the cabin layout. In addition, the need for a simple "water-pistol" type fire extinguisher for onboard cabin use were recognized, to prevent small ignition sources from spreading into major blazes.

CONCLUSIONS

The excellent performance of the Lunar Module on all of the manned flights accomplished to date is attributable to reliable hardware, thoroughly planned and executed flight operations, and skilled superbly trained crews. Major factors that have contributed to LM success and reliability are simplicity and redundancy in design, major emphasis on testing, a comprehensive reliability contract plan, a disciplined system of change control and attention to detail and closeout of all discrepancies. Also important was the emphasis placed on the elimination of complex interfaces between major hardware elements.

The use of man in flying and operating the spacecraft evolved during the development of the system with a tendency to place reliance on automatic systems with the capability for monitoring and manual takeover.

The LM design was generally based on the concepts of simplicity and proven design techniques, which in most cases ruled out large scale use of state-of-the-art design advances unless proven conclusively by extensive testing. The success of the LM program cannot be attributed to any single program element, but the proper combination of all elements from the earliest analytical studies, to the comprehensive parts control program through developmental and qualification testing, certification and acceptance testing and careful attention to flight discrepancies and anomalies, as few as they were, resulting from man's most ambitious and successful space ventures.

REFERENCES

1. G. H. Sandler, System Effectiveness Models in Space Systems, 6th N.Y. Conference on Electronic Reliability, IEEE, May 1965
2. T. J. Kelly, Apollo Lunar Module Mission and Development Status, AIAA 4th Annual Meeting, Anaheim, California, October 1967
3. LM Reliability Program Plan - LPL-550-1"C" - Grumman Aerospace Corporation, December 1967
4. J. H. Levine and P. E. Fitzgerald, Apollo Spacecraft Certification Test Program, AIAA Test Effectiveness Conference, Palo Alto, California, April 1970
5. G. M. Low, What Made Apollo, Aeronautics and Astronautics, March 1970
6. T. J. Kelly, Flight Experience With the Apollo Lunar Module, AIAA 5th Annual Meeting, Philadelphia, Pa., October 1968

HIGH RELIABILITY DESIGN TECHNIQUES APPLIED TO LM

Figure No.	Caption
-	(LM landing)
-	(Saturn Liftoff)
1	Differences in Reliability Requirements Associated with Different Use Applications
2	Differences in Demonstration Associated with Different Use Application
3	Some Early LM Program Uncertainties
-	(LM on Moon)
-	(Ascent Stage in Flight)
-	(LM Footpad)
4	Failure Analysis Determination and Sequential Activities
5	Vendor Failure Reporting Data Flow Vendor Acceptance and Qualification Test Failure
6	LM Parts Control Program Flow
7	LM Subsystem Test Cycle
-	(LM in Test Chamber)
8	NASA/Grumman Apollo Lunar Module
9	LM Crew Compartment Interior
10	Ascent Propulsion Subsystem
11	Major LM Program Activities
12	LM Mission Anomalies and Discrepancies

TESTING THE RELIABILITY OF AVIONIC EQUIPMENT FOR SPACECRAFT APPLICATIONS

by

Dipl.-Ing. Guenter Vollhardt
SIEMENS AG
8000 Munich 25
Hofmannstrasse 51
West Germany

SUMMARY

"Reliability" is the supreme demand in space application. Evaluation under well-defined environmental conditions, in particular of equipment employed in space projects, is therefore an absolute requisite. The demands here placed on the individual units of equipment result from the environmental conditions to which these units are exposed during the launch phase and orbit. In order to prove that during launching of the spacecraft the equipment units are not stressed to the limit of destruction, several test models are constructed and tested under different stresses. These tests must be so composed that the various types of failure can be discovered. Basically, failure can occur on equipment units due to the following causes:

- errors in the electrical or mechanical design;
- drift of electrical parameters caused by changes in the material of electrical and mechanical parts.

To assess the different types of faults, circuit analyses as well as long-time tests must be carried out, besides mechanical and climatic tests. The paper describes the provisions, which have to be carried out in the individual phases of a project in order to reveal failures in due time without delaying the project. The considerations are explained, which lead to the circuit optimization. In long-time performance tests, equipment units are in continuous electrical operation with monitoring of the various parameters. The acquisition of the so gained measurement data is described and the problems outlined, which appear in their evaluation.

LIST OF SYMBOLS

a_i	coefficients of function $f(t)$
$f(t)$	time-dependent function giving the real values
g	gain of an amplifier
N	number of the measured values
s	standard deviation
s^2	variance
T	temperature
t	time
V	max. chi-squared value
y_i	measured value
$\bar{y}$	mean value
α	confidence level
σ_0	dispersion
χ^2	chi-squared distribution.

INTRODUCTION

The reliability factor in space projects plays a very important part since the failure of a single equipment unit often causes the failure of an entire subsystem and repair possibilities after the launching of the satellite are eliminated.

Endeavours must be made to recognize and remedy all possibly occurring faults before the launch. Since a detected fault often results in a mechanical modification of the equipment, relevant considerations and tests on individual subsystems must be commenced at an earliest possible development phase, because later mechanical modifications of prototypes or even flight models demand not only high costs but often also

lead to a delay in the launching date.

The demands thus made on the individual subassemblies result from the environmental conditions which the subassemblies are exposed to during the launch phase and orbit.

The environmental conditions include thermal stresses, i.e. high and low temperatures in the vacuum, damp heat and mechanical stresses, e.g. sinusoidal and random vibrations, shock, linear accelerations as well as solar radiation and particle radiation, especially in the case of orbits in the Van Allen belt. In addition, there are other requirements: electromagnetic compatibility between the subassemblies must be guaranteed; a high degree of magnetic purity is required, particularly for research satellites owing to the experiments to be carried out.

1. PROOF OF RELIABILITY OF FLIGHT MODELS

Before delivery, acceptance tests are carried out on the flight models which simulate the mechanical and thermal stresses occurring during launch and orbit. The purpose of these tests is to prove that the subassemblies can stand up to the expected environmental conditions. In contrast, more stringent demands are placed on the qualification models, which are identical to the flight models, so that it can be proved that sufficient mechanical and thermal margins have been allowed for in designing the subassembly. The mechanical stresses, e.g. shock and vibration, are generally made 50 % greater than during the acceptance test. The thermal stress is selected approx. 10 to 20 K lower or higher, i.e. the temperature range in which a subassembly must remain completely operational is about 20 to 40 K wider than during the acceptance test.

During the development the subassemblies are stressed almost up to the destruction limit. This is to determine the maximum mechanical and thermal load capability in order to establish whether the required margins are sufficient for operating in orbit, whether they must be widened or whether they can be reduced to save weight.

2. BASIC TYPES OF FAILURE AND THEIR ASSESSMENT

The tests on the development models are also intended to determine whether a module exhibits various aging characteristics.

The causes of this are:

- a) Electrical or mechanical design errors, e.g. overloading of the components and mechanical parts due to inadequate size.
- b) Drifting of electrical parameters caused by changes in the material of electrical and mechanical components, e.g. changes in the crystal structure.

The results of the two causes of failure are considered below and measures are described for tracing and preventing them.

2a) Failures caused by wrong electrical and mechanical design:

Such potential failure sources must be investigated and eliminated as early as possible during the development of the equipment. For this reason circuit analyses are made where the components in the circuit are analyzed according to the following two aspects:

- regarding their applicability with respect to the environmental conditions of the units;
- regarding the respective stress in the individual application.

In the first case it has to be checked that the components used are fully covered by corresponding standards or suitable specifications. It must be ensured that the stresses on the unit are not such that the component may be impaired in its function.

In the second case the application of particular parts in the respective circuit must be analyzed. Thus it is examined whether the component is overloaded by the mode of application or how large the provided safety margins are from the limit data, which are normally fixed by the manufacturer. At the same time the individual parameters which influence the reliability of a part are to be compared with the permissible values as in specification sheets. Further there are design factors to be considered, such as the mode of application, the electrochemical compatibility, the possibility of mixing up components or contact connections by inadequate lettering.

2b) Failures caused by the drifting of the electrical parameter:

This type of defect occurs when the specified parameters of an equipment unit exceed the permissible limits after a short or long period of time. Therefore, when considering the reliability, it is necessary to examine the influence of tolerance limits and of the drift of the individual parts on the function of the circuit. These examinations will be much more important and give stronger evidence than a statement of the total failure possibility of an equipment unit on the basis of the failure rates of the individual parts. The tolerance limit of a part is understood as the admissible limits for the deviation from a certain nominal value

in the condition as supplied. Drift variations may be due to environmental influences as well as electrical stresses and aging effects. These influences can have an individual or combined effect on the parts data. These values are spread within a certain range, the mean value, distribution pattern and the limits of which change as a function of environmental stress, load, and aging.

3. CIRCUIT ANALYSES

The drift of the output of a module is related to the drift of its parts by means of its transfer function.

It is the purpose of a tolerance and drift analysis within the scope of reliability analyses to check the influence of the parts drift distribution on the output parameter of the module. If the output parameter is not within tolerance, the parts parameters have to be changed.

Experimental procedures by inserting so called "limit-value components" with transistors whose current amplification is at the limit, and resistors with the maximal allowed deviation, are very restricted in their range of application and can be used only for very simple circuits. Moreover, only a "worst-case analysis" can be so attained.

With the "worst-case analysis" the two values of the quantity of interest, e.g. the transfer function, applied with the greatest possible margin from the nominal value, are determined. In doing so, in each case the lowest and the highest values or the individual component parameters are entered in the transfer equation.

If, however, one assumes that the component fluctuations follow a Gaussian distribution and bases the calculation on the σ -values depending on the required confidence level, then it is evident that the probability of the "worst-case values" exceeding the given limits of the individual parts is very small. The probability that all the components simultaneously reach their "limit values" becomes smaller with increasing number of components in a circuit.

Therefore, information is required on the spread of the output parameters of the module depending on the spread of the parts parameters.

These calculations can be made on a computer using such programs as STAEN Net-1, IMAG or others. It would be beyond the scope of this paper, however, to describe in detail the individual calculation procedures.

The tolerance and drift analyses must, of course, be based on the drift values of the individual parameters. At the same time it must be considered that the drift characteristics are strongly influenced by the operating stress. Some information on the drift characteristics can be obtained from the RADC-Reliability Notebook and the MIL Specifications. Further information can be obtained from publications of the respective part manufacturers as well as from those of the governmental and industrial laboratories.

At the present state, these theoretical circuit analyses cannot yet be applied to complex RF circuitry with many active parts. Since very few transistors are contained in the programs, equivalent circuits must be worked out for the majority of solid-state devices. The equivalent circuits of the RF solid-state devices are extremely complicated and demand a large section of the program. Besides, the different influences such as stray capacitances of the RF circuits, which affect the functioning of the circuit, cannot be covered accurately enough.

In order to examine the aging characteristics of these circuits, one depends exclusively on the durability tests described below.

4. DURABILITY TESTS

The tests can only be carried out effectively when several subassemblies are available and are electrically operated during the tests and their transfer functions are constantly monitored. In doing so the same measurements must always be repeated on the different modules at regular intervals.

A continuous oscillographic recording system makes the evaluation difficult, since the individual parameters are interdependent. A computer will not constantly be available.

For this reason an automatic mode of measurement has been developed, where the individual measured values are stored on perforated tape for subsequent evaluation by a computer. This leads to possibilities which would otherwise be very difficult to realize, such as accurate information on the variation in time of the various parameters. Also, this method permits obtaining an increased accuracy of the final result by using a larger number of measured values which are recorded. It is here assumed that the individual measured values follow a normal distribution about a mean value.

4.1. Description of the Measuring Set-up

The block diagram for the automatic coverage of the different parameters of a module is illustrated in Fig. 1.

All measured values must be applied as dc voltages at the input of the metering-point selector. Physical measurements must previously have been converted into dc voltage. At this stage a total of 60 input points are available at the metering-point selector switch. Before commencing with the measurement one must select the points where an "interrogation" is to be made. After a start pulse, which is given by a timer, the voltages which are present at these points are then "interrogated" successively. The output of the metering-point selector switch is read and converted to digital form.

The control system of the perforator regulates the recording of the information.

If modules with frequency-dependent transfer functions are being tested, e.g. amplifiers, then not only the time-dependent variation of the gain at a given frequency is of interest, but also at various frequencies. In doing so, it can be determined whether the gain slope is time-dependent or remains constant. Therefore, the frequency is automatically adjusted step by step before each measurement. If modules are being tested with temperature cycling, then a new temperature is set with a control circuit after every measuring cycle.

4.2. Carrying out the Measurement

In the case of a long-time test, a measuring operation is initiated at predetermined times by a start pulse from the timer. In order to restrict the data quantity, depending on the type of module, a distinction is made between frequency-dependent and frequency-independent parameters. Here an interrogation is first made concerning the frequency-independent parameters, such as supply voltage, temperature, etc. Subsequently the remaining parameters, such as gain or input and output level, are measured at the set frequencies.

The most important subassemblies being tested at present are UHF wide-band amplifiers, frequency converters and SHF tunnel diode amplifiers. Owing to the large number of specified parameters of a subassembly, all the parameters cannot be constantly supervised during the tests. On the contrary one should restrict the tests to such parameters where variations are most likely. For the TDA and wideband amplifier this is the gain and for the frequency converter it is the conversion loss. Since measurements are carried out at several frequencies, the frequency response can also be found at the same time.

4.3. Processing the Measured Data

A program was prepared for the evaluation of the measured data. The program is laid out in such a manner that it can be used for any type of module. This means that the data of the measurements of the various modules can be stored randomly on the perforated tape. First the individual data is assigned to the corresponding modules and then analyzed. The measured results of a module at one frequency and two temperatures are plotted in Fig. 2 for illustration.

Since all physical quantities under test, such as current and temperature, are present as dc voltages at the input of the metering-point selector switch, these voltages are initially converted to their physical quantities. When this has been done, the measured values are printed out. These values are automatically assigned to the corresponding test modules. If the durability test was carried out at different frequencies then the printed data for the test module is assigned to the individual frequencies. Subsequently the data of each module is processed successively and separately in the program.

If the measurements were carried out at different temperatures then the data measured at the same temperatures are picked out and combined in groups. If, for example, measurements are taken at (8) frequencies and (3) temperatures then one has $(8) \times (3) = (24)$ new groups. Each group is examined for changes.

During the measurement it is attempted to keep the system parameters, such as supply voltage and temperature as stable as possible. In spite of these efforts minor deviations from the nominal value occur, especially in the case of the temperatures. Since only measurements carried out at the same system parameters can be inter-compared, these deviations must be corrected accordingly.

In order to be able to calculate the deviation, e.g. of the gain of an amplifier, from the temperature difference ΔT , the relation between the output power and the temperature, at constant operating conditions, such as supply voltage and frequency, must be determined first. In the same way the relation between the parameter to be measured and the other operating conditions must be determined, whereby only one parameter at a time is varied and the others are left constant. Thus different calibration curves are obtained. A number of fixed points from these calibration curves are fed to the program. A linear interpolation is carried out between these points.

After correcting the individual measured values and thus eliminating the external influences of the operating conditions, the modified data can be intercompared and evaluated.

So far it has been assumed that the measured values are quantities having a normal distribution about a mean value $\bar{y}$. For an accurate analysis it is necessary to examine how the measured values behave as a function of time.

As an approximation, an attempt is made to run a curve as a function of time through the measured values by applying a polynomial and expanding it until the functional relationship of the measured values is described accurately enough.

$$f(t) = a_0 + a_1 t + a_2 t^2 \dots a_n t^n$$

With the first approximation there is $n = 1$,

with the second approximation $n = 2$, etc.

Then the coefficients a_i are calculated. The different terms of the polynomial represent here the time-dependence of the parameter variations.

If the polynomial is differentiated with respect to the time, then a measure is obtained of the rate of change of the parameter as a function of time.

In order to examine the distribution of the measured values about the real values some of the characteristics of the χ^2 distribution are used. The variance is calculated according to the formula

$$s^2 = \frac{\sum_{j=1}^N (y_j - f(t_j))^2}{N - 1}$$

where N is the number of the measured values and $f(t_j)$ the real value of all the measured values y_j .

Furthermore, an empirically determined spread σ_0 for the measurement device is accepted. It can be proved that the quotient

$$V = \frac{(N - 1)s^2}{\sigma_0^2}$$

has a χ^2 distribution with $(N - 1)$ degrees of freedom. The measured values correspond to a normal distribution if

$$V \leq \chi_{\text{crit}}^2 (N - 1, \alpha),$$

where α presents a previously fixed confidence limit of the χ^2 distribution. If

$$V > \chi_{\text{crit}}^2 (N - 1, \alpha),$$

then it is assumed that there is no normal distribution of the measured values. A sudden variation of the measured values can be the cause of a distortion of the frequency distribution. In this case the data measured before and after the sudden change is evaluated separately. Thus both measured series are considered as undistorted. This, however, leads to a result only when the sudden change is larger than the time-dependent variation.

The total parameter degradation can be determined only by adding the degradation in the two intervals as well as the degradation due to the sudden change.

The spread of the measured values determined during the calculations is a measure of the accuracy of the durability tests.

4.4. Test Results

Finally some test results shall be given. Several identically designed subassemblies were subjected to the following test cycles:

a) High temperature storage at 100°C for about 1000 h;

b) Temperature cycling with 24 cycles:

- i. Test every 3 h; +20°C; +40°C; +20°C; 0°C;
- ii. Test every 3 h; +20°C; +90°C; +20°C; -30°C;
- iii. Test every 3 h; +20°C; +40°C; +20°C; 0°C.

It was the purpose of the test to ascertain which parameter variations are presented by these subassemblies after an operating time of 40000 h, the operating temperature range being between 0°C and 40°C.

After 1000 h of storage at 100°C the subassemblies show no evident parameter variations.

The results of the temperature change tests, which were carried out in a vacuum chamber at low pressure for different frequencies are shown in Fig. 5.

At 20°C after the first and third 24-cycle test (temperature range $0^{\circ}\text{C} < T < 40^{\circ}\text{C}$) the parameter variation after 200 h was 0.03 dB for the third frequency, and after a second 24-cycle test (temperature range $-30^{\circ}\text{C} < T < 90^{\circ}\text{C}$) it was 0.13 dB at the same frequency.

It is important to know that in this case there was a variation of gain with frequency.

The effect on the degradation due to the wider temperature range can be seen in Fig. 5.

Tests were performed to investigate the correlation between the accelerated degradation of a module and the type and duration of the temperature cycle.

Further work will be done to improve measurement methods, to reduce the spread in the measured data, and to improve the computer program for evaluating the data.

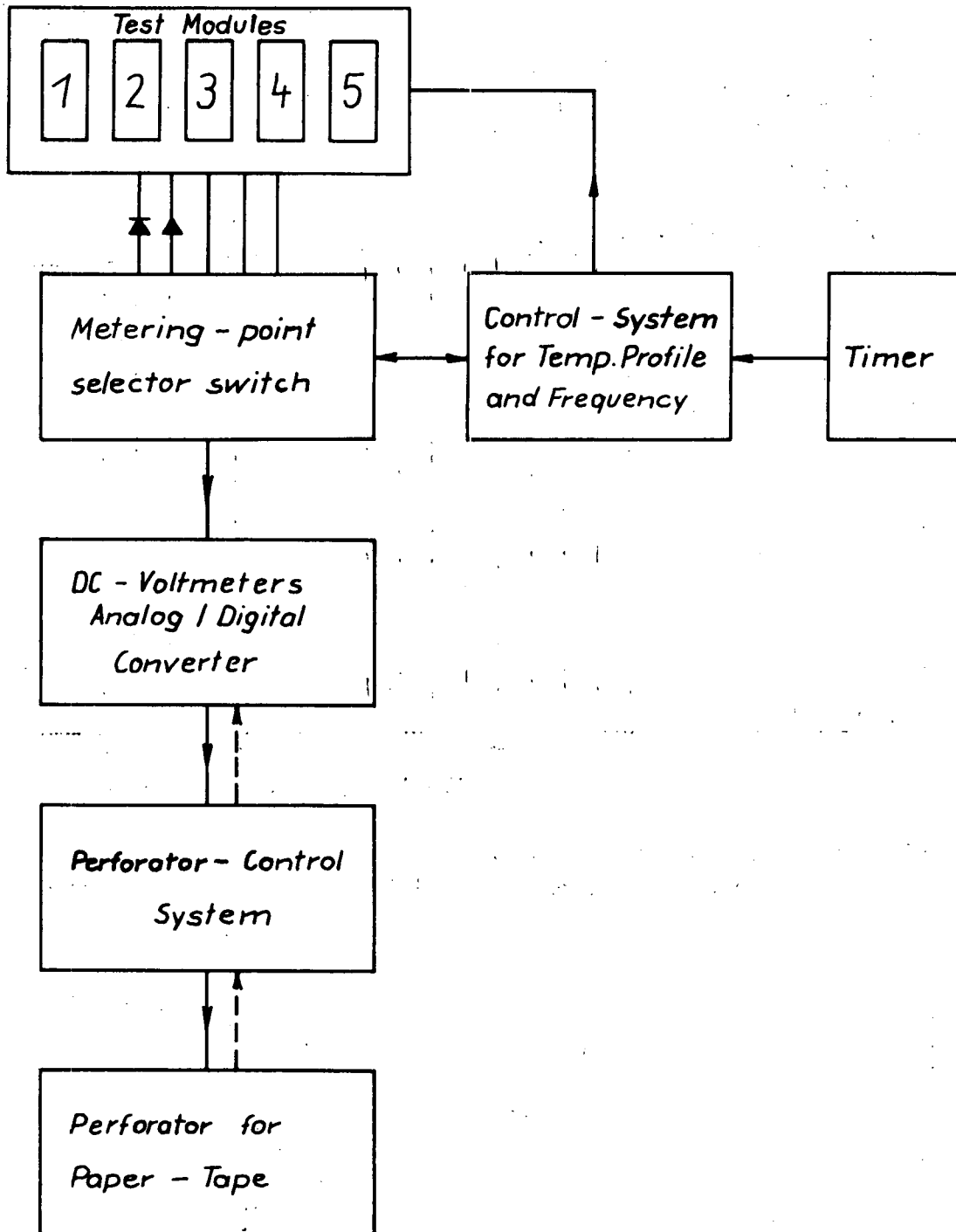


fig 1 Block Diagram of Measurement System

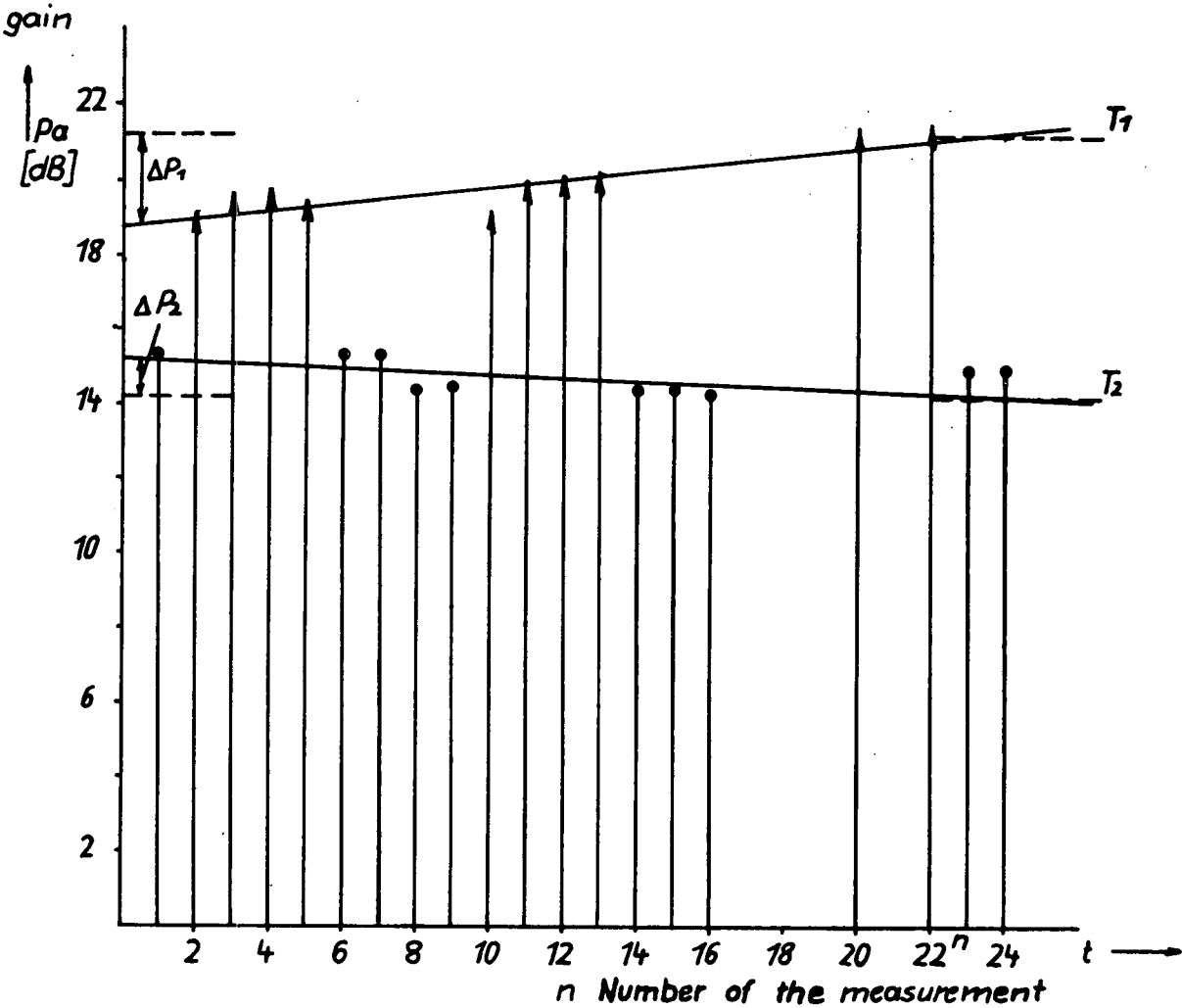


fig 2 Evaluation of the measured values for one frequency and two temperatures of the gain of an JF-Amplifier

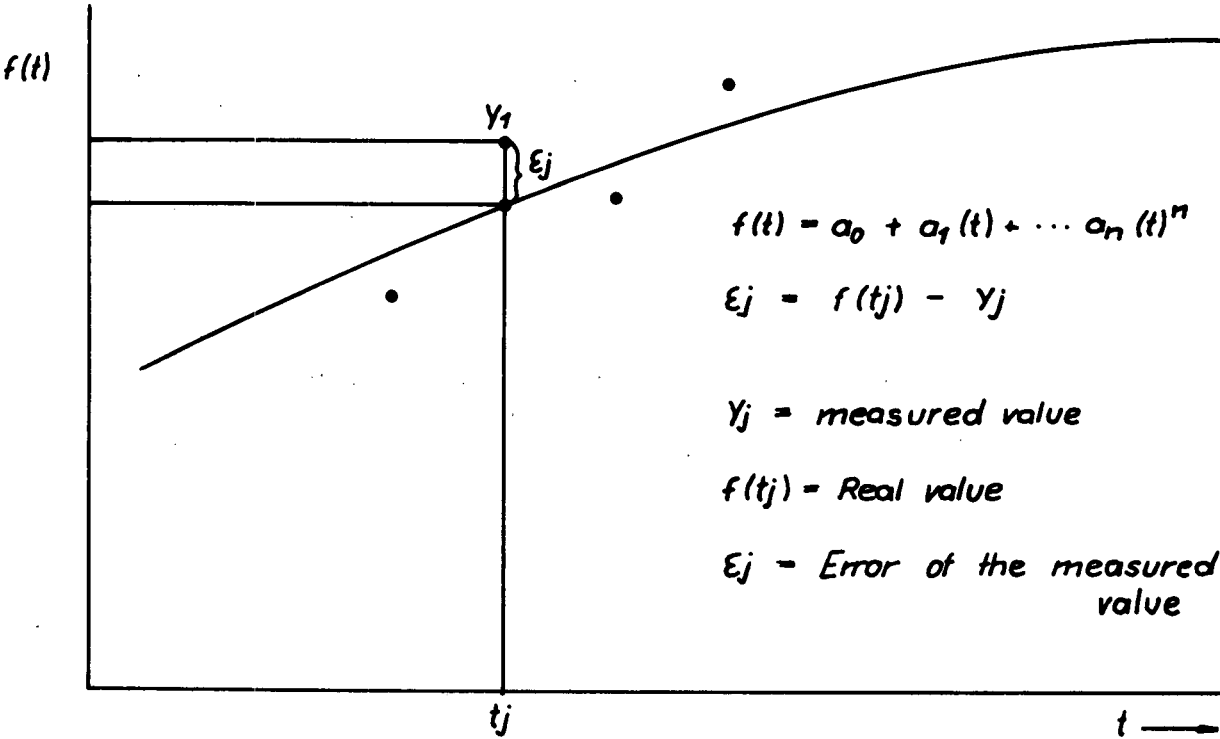


fig 3 Schematic of mathematical model

KORRIGIERTE MESSDATEN PA/PE TEMPERATUR=-35 GRC

FREQUENZ		NU 1	NU 2	NU 3	NU 4	NU 5
N=	2	0.12	0.34	0.36	0.32	0.33
N=	6	0.15	0.36	0.38	0.33	0.34
N=	10	0.13	0.35	0.37	0.32	0.33
N=	14	0.15	0.35	0.37	0.32	0.33

TEMPERATUR=23 GRC

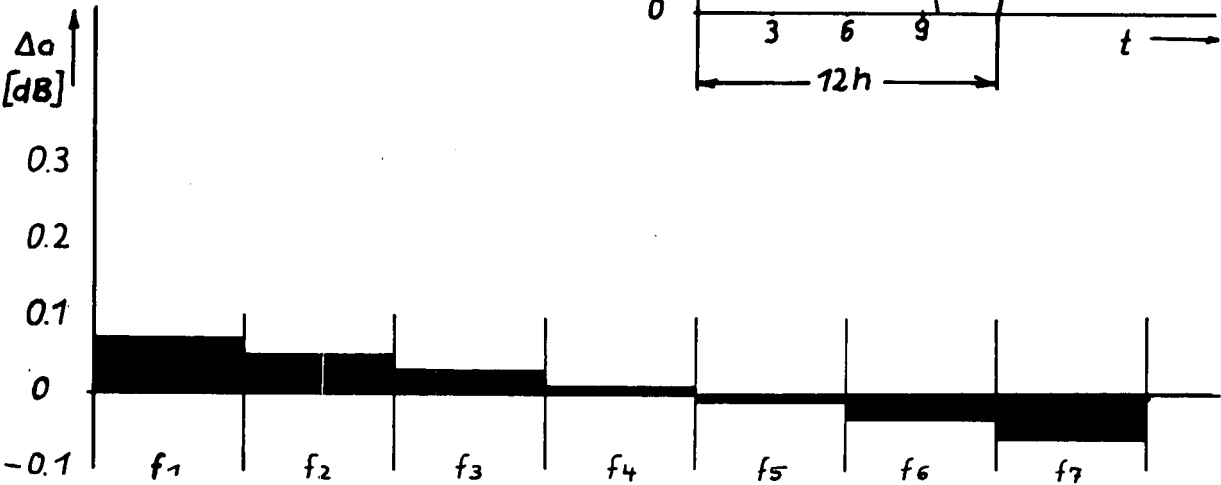
FREQUENZ		NU 1	NU 2	NU 3	NU 4	NU 5
N=	1	0.98	0.38	0.56	0.52	0.54
N=	3	1.05	0.37	0.55	0.52	0.54
N=	5	1.04	0.37	0.55	0.52	0.54
N=	7	1.09	0.37	0.55	0.52	0.53

TEMPERATUR=90 GRC

FREQUENZ		NU 1	NU 2	NU 3	NU 4	NU 5
N=	4	0.60	0.28	0.48	0.48	0.50
N=	8	0.62	0.26	0.48	0.48	0.50
N=	12	0.60	0.28	0.48	0.48	0.50
N=	17	0.59	0.28	0.49	0.48	0.51

fig 4 Evaluation of the Measured Data

Gain - Variation at 20°C
Test conditions :
24 cycles between +40°u. 0°C



Gain - Variation at 20°C
Test conditions :
24 cycles between +90°C u. -30°C

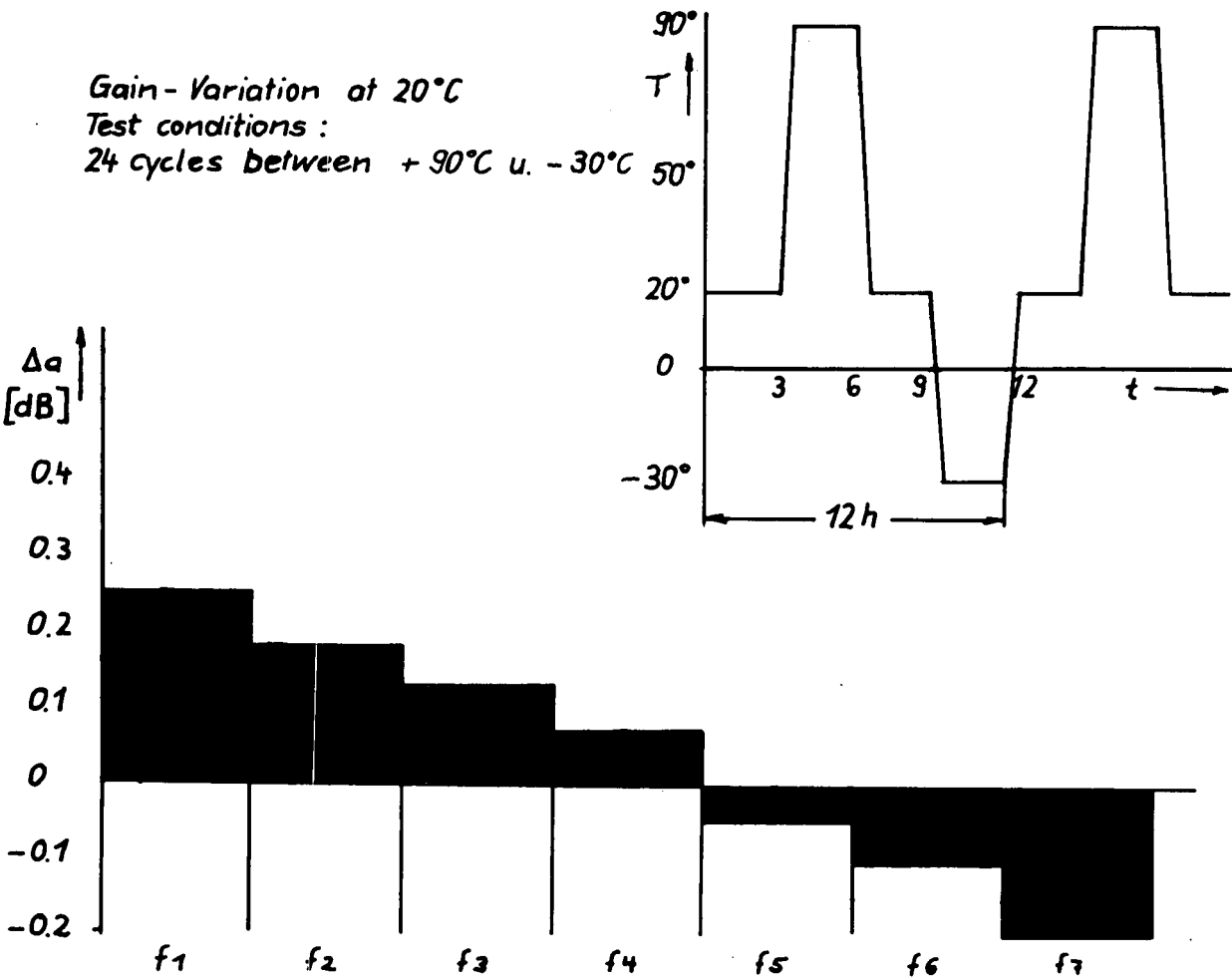


fig 5 Test Results : Gain Variation of an JF-Amplifier

METHODS OF SPECIFYING AND CONTROLLING DESIGN RELIABILITY

by

J. J. Bussolini
Director of Engineering Operations and Administration
Grumman Aerospace Corporation
Bethpage, New York

SUMMARY

The process of integrating reliability into product design rather than permitting some external application of techniques to "fix" product performance is a critical element of the developmental cycle. History has proven that proper specification of reliability requirements and the imposition of certain key reliability program elements is the corner stone of a successful program. This paper examines some examples of techniques used to accomplish early determination of system and equipment reliability requirements, the methods used to specify these requirements and the contractual techniques used to test and demonstrate compliance to specification requirements. Incentive-penalty contracting for reliability is discussed including recommendations for relating these incentives and penalties to conventional and modified demonstration test techniques.

INTRODUCTION

It has been only thirteen years since the Advisory Group on Reliability of Electronic Equipment (AGREE) published its first report. This report is generally credited with causing the birth of the reliability engineering technology. During the years since this report was released, industry has seen the birth, growth, maturity and sophistication of this new engineering technology. Reliability Engineering has perhaps been subjected to the most extensive criticism of any comparable engineering technology and has survived well as can be evidenced by the volumes of documentation authored by notable specialists in the field which occupy sizeable segments of every corporate technical library.

A significant portion of the new learning in this 13 year era relates directly to the development of electronic hardware, since electronic design has also shown its most significant growth during this time period and reliability became an inseparable part of the design process.

Today, although in an environment of declining "technology spending" especially related to defense and aerospace, emphasis is still focused on operational effectiveness, life cycle costing, maintenance free utilization and reliability for all electronic hardware. Austerity in spending, coupled with the need for more sophisticated electronic equipment, focuses an even more important light on the need for a new and more practical reliability engineering technology. The continued criticality of effective equipment performance in sophisticated systems creates a changing emphasis on reliability and requires much more careful control of the design process.

RELIABILITY PROGRAM CONTROL

During development, reliability management and control includes, but is not limited to, tasks for:

- Program Planning and Control
- Seller Control
- Parts Control
- Design Reviews
- Failure Reporting, Analysis, and Close-Out
- Status Reports

Because a reliability program usually incurs its major costs early in a system development program, there is a natural tendency to place restrictive management curbs on reliability at this time. Yet, it is in the early design and development stage when a reliability program is most effective and should be emphasized accordingly. The reliability program, usually defined in detail in the Reliability Program Plan, must include iterative and detailed analyses to give needed technical visibility. These analyses include:

- Reliability Mathematical Models
- Apportionment (Continually updated)
- Predictions (Continually updated)
- Configuration Analysis
- Weak Link Analysis
- Failure Modes and Effects Analysis (Iterative--each more detailed)
- Circuit Analysis
- Environmental Effects Analysis

While each of the above analyses contributes to, and is necessary for attainment and control of hardware reliability, the impact of each is not equal, and its degree of application must be modified for the specific program being considered. Timeliness, rather than formality, is important in the accomplishment of these analyses.

A test program should be coupled with the analyses tasks and adjusted to the specific program and hardware. In general, the test program includes:

- Development Tests
- Qualification Tests
- Acceptance Tests

A strong test program can somewhat compensate for a weak analysis effort, when a rigid failure close-out procedure is added. Development testing, including step-stress testing, has proved its value time and again. Unless a strong test program is included in product development, the qualification test of the production configured equipment becomes an exorbitantly expensive design screen.

In production, continued program surveillance is necessary to control design changes, acceptance tests, and the subcontractor's participation in the failure reporting and close-out procedures.

RELIABILITY CONTROL OVERVIEW

The challenge of establishing the requirements for a design approach which will most effectively satisfy the needs of the customer at the least risk to the contractor, and within cost restraints, is significant during the time leading up to a proposal. Unless each system under consideration is analyzed from a reliability aspect before a selection decision is made, there is a strong possibility that the contractor could encounter a program in which the system could not possibly achieve the necessary reliability goals. Early analysis requirements include:

- Evaluation of the customer's reliability requirements. All parametric trade-offs and analyses associated with reliability and maintainability parameters should be performed to determine the validity of the requirements and the risks associated with contractor compliance.
- Definition of subordinate equipment reliability requirements and risks. The system requirements must be apportioned to the subsystem and equipment levels.
- Identification of critical system functional trade-offs, and if applicable, incentive strategy. Mission success criteria rationale are to be developed and analyses approaches defined.
- Structuring of systems requirement specification to identify complete system prospectus for compliance to the customer.
- Performance of system level failure mode effects analysis to determine critical areas in the functional design.

A program plan tailored to the customer's requirements and objectives should also be prepared at this time.

Reliability oriented program management directs the tasks which control both contractor and subcontractor efforts that govern the achievement of reliability in the systems, subsystems, and equipment. The tasks are interrelated, but are categorized into the following disciplines:

- In-House Contractor Controls
- Subcontractor Controls
- Parts Control
- Design Reviews
- Failure Reporting and Close-Out

Contracts, to have meaning, should call for incremental subcontract payments tied to timely report submittals and approval of these reports by the contractor. A prime concern is timeliness of document submittal. Although formal subcontractor reports are generally not needed to perform contractor reliability functions, it has been found that these requirements do provide assurance that the required reliability functions have been performed in accordance with specification requirements, have been thorough, have been accomplished on schedule, and that outputs have been applied to the program.

A sound parts control effort has proven to be one of the most successful elements of recent reliability programs. Major elements of an effective parts control program include:

- Weapon System Coordination for Parts Standardization
- Control of Parts Application
- Maximum Use of Proven Parts
- Maximum Use of Screened Devices
- Enforcement of the Program in the Early Design Stage

The design review is an excellent control for the assurance that the designer is achieving the desired performance and reliability requirements on schedule and is accomplishing the necessary follow-up from previous reviews. These reviews include consideration and discussion of:

- Design Features
- Estimates of Current Reliability
- Potential Design or Production Problem Areas
- Failure Modes and Effects Analyses
- Parts Program and Problems
- Significant Program Achievements
- Effects of Engineering Trade-Offs

One of the most important aspects of a reliability control program is the problem reporting and corrective action close-out system. Every failure should be documented and investigated and the corrective action approved before proceeding further. One of the most serious problems experienced on many programs is that failures go unreported or are ignored on the assumption that they are inconsequential. Then the failed item is repaired without determining the cause of the failure. Fast reporting, investigation, and follow-up is essential for a well-planned, effective reliability program.

The prime purpose of reliability analysis is to impact the design--from system level through part application--to enhance the features which provide reliability. A secondary purpose is to determine whether the design will meet its quantitative requirements. The analyses vary in scope according to program needs, and include:

- Math Model - provides method for analyzing system reliability.
- Configuration Analyses - compare alternate configurations/methods for achieving system requirements.

- Reliability Prediction - computes inherent reliability from bottom up under expected conditions.
- Apportionment - allocates reliability requirements to system subtiers.
- Failure Modes and Effects Analysis - determines consequences and criticality of failures.
- Weak Link Analysis - identifies failure prone items.
- Circuit Analysis - assures proper part application and electrical stresses.
- Environmental Effects Analysis - examines peripheral effects-handling, storage, transportation, etc.

The timeliness of the analyses rather than their formality must receive priority. Only on-schedule results can have an effective impact on the system or equipment development of reliability and safety.

A point not commonly recognized is that many of the analyses are iterative--the predictions must be recalculated whenever changes are made, the failure modes and effects analyses must be performed at each lower level of design as it appears, and the circuit and parts applications analyses must be repeated whenever changes occur in circuitry or new parts are applied.

During development a series of tests must be conducted to evaluate the basic design, ensure that any design weaknesses are eliminated, and establish reasonable environmental and functional margins of safety. The importance of a strong development test effort which includes both design assurance and step-stress tests cannot be over-emphasized. It is only during development phases that testing can truly impact and benefit a design and corrective action can be implemented in a timely, cost effective manner.

Since a test program can only be effective if properly implemented, it is vital that all tests be carefully monitored by knowledgeable personnel who are fully cognizant of the test requirements imposed and also understand the equipment functions. The qualifying phase confirms the ability of the equipment to function satisfactorily in all expected service environments and also determines whether an equipment has met the specified reliability requirements. Tests to be performed during the final (production acceptance) phase must be designed at this time to eliminate workmanship problems and must be capable of continuously reaffirming the inherent reliability integrity of production equipment.

When a design has been frozen and the product qualified and in production, all changes must be closely controlled. At this stage, too many actions and too many dollars have been committed to permit any change unless authorized by the customer through a formal change control process. The manner in which internal control is established and maintained may vary, but reliability engineers should be a formal part of the design change authorization group. Many of the analyses and tests performed during development may have to be repeated to verify that reliability will not be degraded by the proposed change. Any proposed change should include the impact as related to the equipment and system as well as other parameters.

Acceptance tests are usually performed on deliverable equipment to assure retention of inherent reliability. Poor workmanship methods, manufacturing defects and quality and inspection shortcomings all degrade the potential reliability of well-designed equipment. Hence, the test program must be capable of a dual function. First, latent quality type problems must be removed before final acceptance. Second, a continual assessment of reliability must be made to assure compliance with originally demonstrated reliability requirements.

Two specific test techniques have proven effective and should be applied to all deliverable hardware, as well as to the qualification and reliability demonstration samples prior to those tests; they are: Burn-In (Environmental), and Reliability Acceptance Tests.

While burn-in answers a definite need (the elimination of infant mortality), it is not capable of (or intended to act as) a control of subcontractor's product reliability. Consequently, a reliability acceptance test should be performed which serves a dual function:

- Provided a continual assessment of equipment reliability during production.
- Establish tight control of equipment quality by forcing subcontractors to take positive corrective action.

SPECIFICATION TRENDS

One usually reliable indicator of industry and customer trends is the myriad of specifications that formulate policy and procedure governing the application of a particular discipline or technology. Reliability has certainly not been exempt from this rule. MIL-STD-441 which was released in 1958 put forth some very basic procedures and concepts for achieving design reliability. MIL-R-27542 which was issued in 1961 described some minimal developmental test requirements and left the option for reliability demonstration in accordance with another specification MIL-R-26667. With the release of MIL-STD-785 in 1965, the military insisted upon a comprehensive reliability test program including developmental, demonstration, and acceptance testing and included the provisions for step-stress testing where applicable. More recent release of MIL-STD-785A solidified the requirements for sound reliability test programs. The specification transitions that have occurred over the years certainly indicates a movement towards solidification of the procedures involved in reliability engineering. MIL-R-26667A which was issued in 1959, MIL-R-23094A issued in 1963, MIL-STD-781A released in 1965 and MIL-STD-781B issued in 1967 have all offered refinements to the procedures for performing reliability demonstrations. Reliability testing alone is represented by a sizeable number of available specifications which can be used in part or in whole to govern procedures used on test programs.

RELIABILITY PROGRAM SPECIFICATION AND APPLICATION

Controls during the design phase are certainly the keystone of a reliability control system. A long accepted theory states that reliability must be an inherent part of the design process if the basic design is to be sound and reliable. If some subsequent phase of the execution or operation is faulty, something can usually be done to salvage the project. This action usually takes the form of improving procedures or establishing more rigid control over detailed characteristics of the hardware. If, however, the basic system or hardware design is deficient from the start, no amount of reliability control in any area can ever correct or make up for the basic design deficiencies without exhausting tremendous financial resources. The most economical solution in cases such as this, either when the project is large or the design quite advanced, is to scrap the project and start from the beginning.

Considering all this when examining history,⁽¹⁾ we find that reliability control during the design phase has quite often been the weakest point of many reliability programs. This situation correlates itself to the general lack of emphasis on excellence of design in many developmental programs. Only in recent years has this trend been reversed. In general, our science has proven to be far ahead of our design capability. It is worthwhile, however, to attempt to understand why this is so.

The design function is not a straight forward handbook process--it is an art which is based on the application of science and technology. Analytical methods will, therefore, go so far. From that point on the process of cut and try takes over. Design also requires ingenuity and creativeness. Individuals who have neither design experience nor design responsibility often find it difficult to comprehend the design process and intuitively reject the design concept. In designing a reliability program and subsequent generation of a reliability specification, one must take a fresh look at the reasons for unreliability of current major systems. We must start with fundamentals and embrace new concepts to develop a control program which offers reasonable promise of accomplishing the desired results within known available resources and developmental schedules.

Some product characteristics such as weight and size are easy to measure and there is usually little disagreement on whether or not these items satisfy the stated requirements related to these characteristics. These have been called "hard product characteristics." With single source items that must be delivered on a given schedule, non-conformance with the hard requirements can often be overlooked if safety is not involved. In order to minimize this possibility, most companies when embarking upon development programs require that contractor's conduct one or another type of control program for significant hard product characteristics. System weight goals for example are apportioned to all components of the systems. Estimates are then prepared as soon as the first design sketches or layouts are made. Thereafter, periodic weight estimates are prepared and whenever the estimates exceed the goals or requirements some action is taken and very often this action is effective. After the product is built, it is always weighed to confirm the analytic procedures and assumptions.

Reliability is considered a "soft product characteristic" which cannot always be defined and measured without a great deal of discussion, if at all. In any case, it is a much softer characteristic than weight. Control and product acceptance procedures, if they are to be effective, must therefore be much more rigorous than those for items such as weight. As a minimum, system reliability goals or requirements must be apportioned to all components of the system and periodic estimates prepared as the design progresses. Each of these estimates must be compared with the corresponding goal or requirement. Similar to the hard item, if the estimate does not equal or exceed the goal or requirement, the item must be redesigned until it does. Reliability assurance tests similarly must confirm the analytical results.

The complex nature of a reliability program and the implications that result when considering the many tiers of contractors, subcontractors, associate contractors, hardware, component and parts suppliers dictates the need for effective specification contract definition and reliability program control.

The design of a reliability program that considers all aspects of the design process can be sacrificed quite readily if the program elements are not adequately specified and funded with acceptable test and demonstration techniques adequately defined in contract terms. The generation of reliability program plans and the ultimate conversion of these program elements for inclusion in detail vendor control specifications is a starting point for a well-implemented reliability program. The specification process begins at the earliest product development phases, even as early as the establishment of the preliminary system operational requirements. System effectiveness studies and mission effectiveness studies depending upon product utilization must result in a development of total system reliability requirements and both customer and contractor management personnel must be aware of the severity of the required reliability levels and the cost and schedule implications resulting from their achievement. Utilizing system requirements as a base, the reliability program can be properly designed and planned and the proper set of control specifications and contract procedures established. As any other control technique, the effectiveness of specification and contract control is directly related to the point in time of the product development cycle where the concepts are first formulated. The effectiveness of the specification and contract program is also a function of the acceptance by management of these concepts and their willingness to implement them considering the cost and schedule implications. Most unsuccessful reliability programs have failed as a result of the lack of continuity between program requirements, part proposals, system and equipment specifications and the ultimate conversion of these requirements to contract terms measurable in terms of performance, incentives, and penalties. A well-controlled specification program requires that each phase of product development be carefully evaluated and appropriate contract terms tied to each of these phases.

The relationships between system, subsystem reliability and detail requirements specifications and the various levels of contracting are very important to a well coordinated program. It is possible to visualize the interrelationship between each of these elements and the total flow of information as a closed loop system where the absence of any individual relationship will render the system inoperable. Refer to Figure 1.

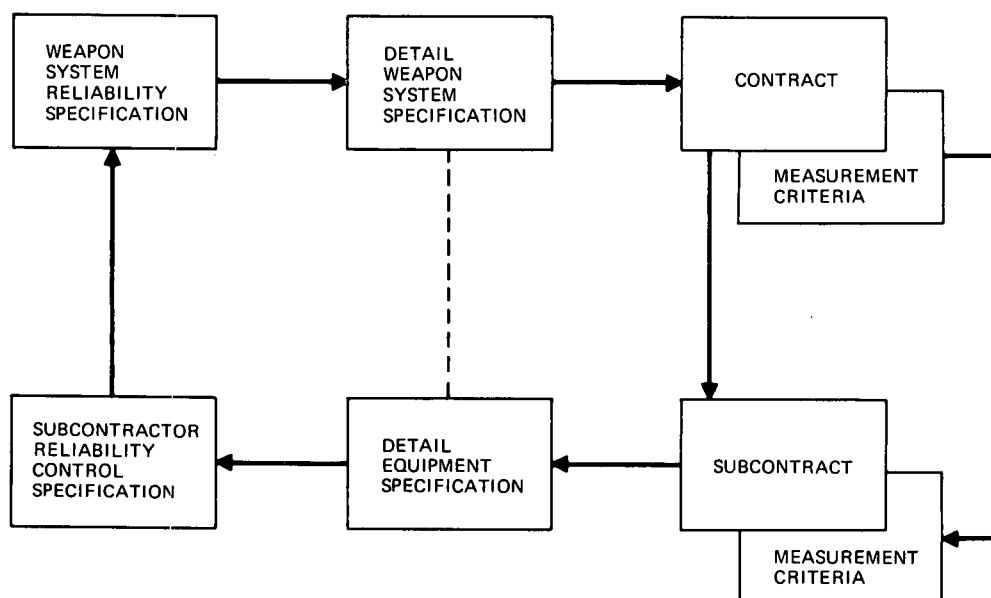


Fig. 1 Closed Loop Specification and Contract System

On a major weapon system procurement, the Weapon System Reliability specification contains the in-depth detail defining the system contractor's reliability program requirements. Reference to this specification is made in the Detail Weapon System specification which defines all system performance requirements including reliability. Those performance parameters considered most significant are then translated into contract form with appropriate measurement criteria listed, including incentives or penalties where appropriate. An effective and well defined weapon system reliability specification will prevent overcomplicating either the detail system specification or the contract with program control information.

The second segment of the closed loop is, of course, the subcontract elements of the system. System contract requirements and measurements criteria must be carefully passed down to the subcontract network. Each subcontract, in turn, must reference performance data from individual equipment specifications. Again, these equipment specifications contain only quantitative reliability requirements and

refer to appropriate subcontractor reliability control specification for reliability program definition. Subcontractor reliability control programs then must reflect the program committal contained in the weapon system reliability specification.

A more detailed examination of these relationships is shown in Figure 2.

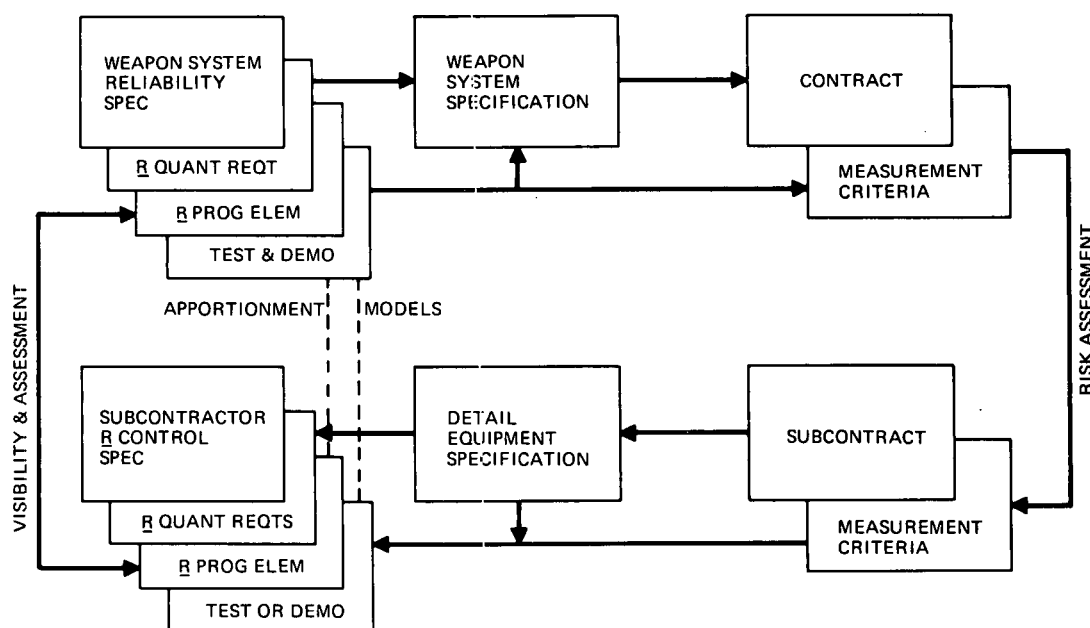


Fig. 2 Related Elements of Reliability Specifications and Contracts

The standard format for the reliability specification usually divides the document into three distinct segments: quantitative reliability requirements, reliability program elements and test and demonstration requirements. The requirements segment of the weapon system reliability specification relates to the detail weapon system specification. The test and demonstration information relates to both the detail specification and the measurement criteria portion of the contract or subcontract. The reliability program segment relates primarily to the comparable portion of the subcontractor control specification.

Conversion of contract to subcontract measurement criteria requires a risk assessment discussed later in this paper. Test and demonstration relationships between the system and subcontractor reliability control specifications are based largely on reliability models. Quantitative reliability requirements are based on apportionments and the program controls achieve management visibility and provide needed assurance of program success. These illustrations become extremely complicated when considering the large number of subcontractors involved with a major system procurement. It is for this reason that all of this effort must be achieved during early definition phases of the program life cycle to assure cohesion between the system requirements and guarantees and those requirements and guarantees passed down through the subcontract network.

UNDERSTANDING PROGRAM TIMELINESS

The evolution to prominence of reliability demonstration during the last several years has certainly not been an accident. The trend towards more precise contract definition, fixed price contracting, the need for a success index to measure contractual compliance, and the use of demonstrations as a management tool to insure supplier's sincerity are only a few of the forcing functions that have driven this approach to prominence. These same factors make it imperative that a systematic approach be taken to evaluation of requirements, assessment of the economic risks, proper allocation of sub-level requirements, inclusion of these requirements in specifications, and the eventual implementation of a comprehensive program of demonstration. Regardless of the level of contractual interests, whether it be system, subsystem or component, the same sequence of considerations must occur. The systems approach to reliability demonstration reflected in firm specification and contract practices when properly planned can form a reference against which nearly every element of a reliability program can be compared. A typical reliability program flow illustrated in Figure 3 provides a time sequenced series of events that illustrates the inter-relationships of many (certainly not all) of the program elements extending from the customer's initial system requirements through final measurement of contract success.

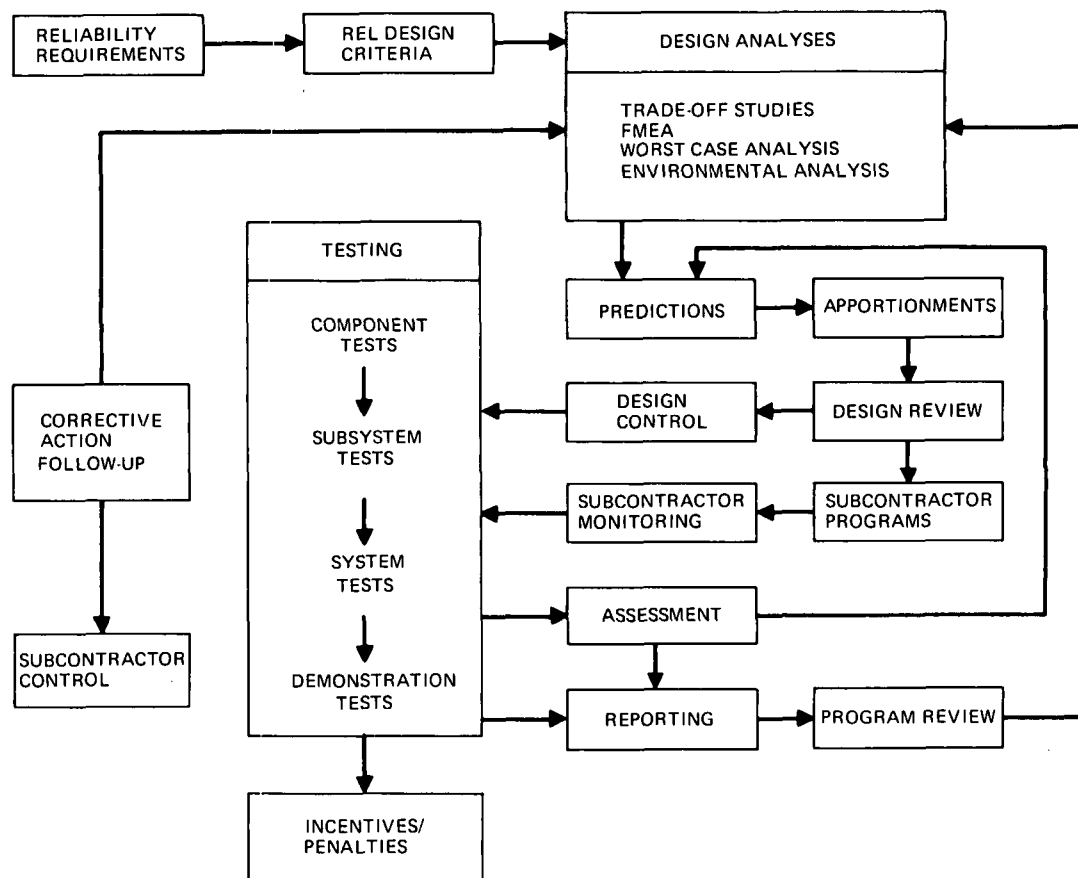


Fig. 3 Typical Reliability Program Flow

Relating these program elements in terms of demonstration milestones offers the advantage of identifying the elements of a reliability program against a meaningful end-item that is profit or loss expressed in terms of incentive or penalty based on the outcome of a demonstration. The ability to relate various program elements and their associated cost to product reliability and its associated incentive now allows the base for intelligent trade-offs to be made related to reliability parameters. These trade-offs can be made on an equal basis with trade-offs of other parameters.

An equally important consideration influencing the total demonstration program tied to a contract is the need to visualize total program implications at every tier of contracting. This becomes more important if the contract is of significant size such as a major space or weapon system where many tiers of contracting and subcontracting exist. Each participant in the program whether a major equipment supplier, system supplier or part manufacturer, must be made to recognize through stringent contract and specification controls, the affect of his performance on the ability of the system contractor to meet his program contract commitments. A clear understanding in this area tends to simplify the specification and negotiation process. This process is, however, the point where many effective reliability programs have historically been ruined due to lack of understanding of program elements and, therefore, unrealistic cost associations.

Perhaps the most key element of the reliability program as it relates the contractual commitments, incentives and/or penalties is the reliability demonstration program.⁽³⁾ When a demonstration is part of the contract, it becomes extremely important that the reliability design requirement be specified in terms of a well-defined mission, sets of missions or mission criteria. Missions must be considered because of the differing functional requirements and time mission profiles where the reliability objectives for each mission or mission profile could differ. When specifying the design and test requirements, it should be made clear which mission or mission profile is the basis for the requirement or if requirements for each mission are desired they should not be conflicting. There are several alternative approaches to the problem of demonstrating when several design requirements exist. The simplest of these, but usually not economically sound, is to demonstrate each requirement in a separate series of tests. Another is to demonstrate the mission with the most stringent reliability requirement; the one which generally appears to be the most difficult to achieve. A third approach is to specify the total number of demonstration missions and simulate each of the design missions in proportion to their expected operational utilization. The total number of successes that would be required to pass the test would be a weighted function of the individual mission requirements. This last approach is based on defining a composite type mission which could be used to demonstrate but might not be an exact replica of an operationally feasible mission. This composite mission might exercise all of the functions and time profiles of all the missions and would be given a reliability requirement on this basis. A major problem in system demonstration relates to the retest criteria or what happens when a test has failed. Passing a test

implies that the design requirements have been satisfied and, if everything else is satisfactory, the program normally continues. In the event that the reliability test has failed, certainly corrective action must be taken to remove the uncovered failure modes. But how will the system be retested? Who will pay and what will be the penalties? These questions should be clarified in the contract if the test is to have any reasonable meaning from a legal or contractual point of view. Establishing demonstration test and contract requirements requires that careful evaluation be made of the system mathematical models where the potential design can be evaluated to determine both customer and contractor risks associated with the design requirements and possible demonstration criteria. To illustrate this, we can take a typical example to show the process involved for the customer and the contractor.

Take as an example the case of an Aircraft Weapon System where the customer desires and the contract is to specify a Weapon System reliability of approximately .90. Based on normal economic and schedule constraints the customer might have to limit the number of demonstration flights, since on a major system level these flights are relatively expensive. Assume that the maximum number of flights desired is 50, and again assume that the customer is willing to take no more than a 20% risk that he will accept a system that is less than the requirement of .90. The contractor can and should develop a series of charts similar to the one shown in Figure 4.

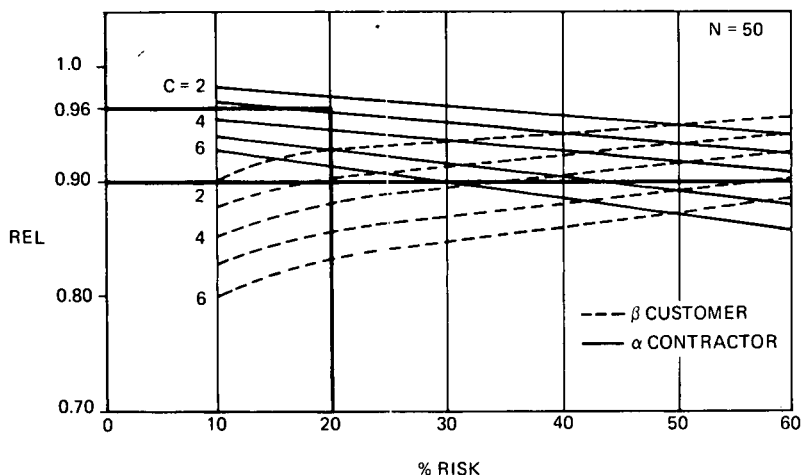


Fig. 4 Typical Flight Demonstration

To compare various combinations of the number of tests and number of successes required to achieve reliability and desired risk, the particular chart shown in Figure 4 represents a 50 flight system ($n = 50$) and is plotted for the allowable number of failures ($c = 2, 3, 4, 5 \text{ \& } 6$). The customer risk (β) is given by the dotted lines for the various desired reliability levels and the required number of successes.

If the demonstration is to be based on the outcome of 50 flights, the customer can allow in this case at most three failures. This will limit his risk to 20% that he will accept the system with less than a .90 reliability. However, if the contractor actually achieves no more than a .90 reliability he, the contractor, will have a risk of greater than 80% of failing this test. In order that the contractor limit his risks, for example, to a minimum of 20%, he must impose upon his system a design goal of .96 and he must then achieve that goal.

If the incentives and/or penalties associated with the demonstration are substantial compared to those associated with other program elements then the contractor should be inclined to design a system to a .96 goal based on the demonstration requirement rather than the specified design requirement of .90. If this high value isn't feasible, then the contractor must attempt to negotiate an alternative demonstration test if he didn't already commit himself to this test in his attempt to get the contract. It should be noted that a reasonable design requirement should be over-shadowed by an unreasonable test requirement which could lead to an over-designed or over-priced system. Therefore, it becomes painfully clear that the risk margin between the system design requirement and the self-imposed design requirement is really an economic factor rather than a technical luxury. This example points up the need for consideration of the demonstration requirements as imposed by contract at the earliest possible program phases even as early as the response to the initial customer RFP, so that system design requirements can be established and subsequently apportioned to lower levels which are sufficiently high to assure acceptable degrees of risk on the part of both contractor and customer. Once overall system requirements have been negotiated in contract, it is most difficult to select a test process that will produce satisfaction on the part of both customer and contractor.

SPECIFICATION AND CONTRACT RELATIONSHIPS

Industry has over the years gradually seen a more sophisticated approach to reliability contracting especially on major aircraft systems procurements. In one of the more recent U. S. Navy Weapon System procurements, the request for quote actually contained the outline format that was desired by the customer for the Weapon System reliability specification. Each competing systems contractor was required to include in his proposal a complete version of the Weapon System reliability specification with all associated quantitative requirements. The concept here, of course, was that the winning contractor would, during the negotiation, simply negotiate a demonstration guarantee and incentive/penalty program associated with this Weapon System specification.

It becomes imperative in this type of a process that the contractor carefully work out his Weapon System requirements; that he weigh his risks; that he evaluate his reliability models; that he define the financial risks that he is willing to take to design his Weapon System demonstration and then, after considering all this, to prepare the details of his Weapon System specification. Using this approach to reliability contracting makes the process somewhat simpler. All the quantitative requirements, definitions, groundrules and reliability program elements are spelled out in detail in the Weapon System reliability specification. When the contract is written, therefore, it is necessary only to reference the requirements of the Weapon System specification and spell out in contract language those financial incentives, penalties and guarantees, if required, that are associated with reliability demonstration; such as was the case in one Weapon System contract illustrated here for purposes of examination. The Weapon System reliability specification was a 25 page document which spelled out in reasonable detail every element of the required reliability program including critical math models, definition of success criteria, demonstration parameters and the details of the reliability program.

The contents of this Weapon System reliability specification are summarized in Figure 5.

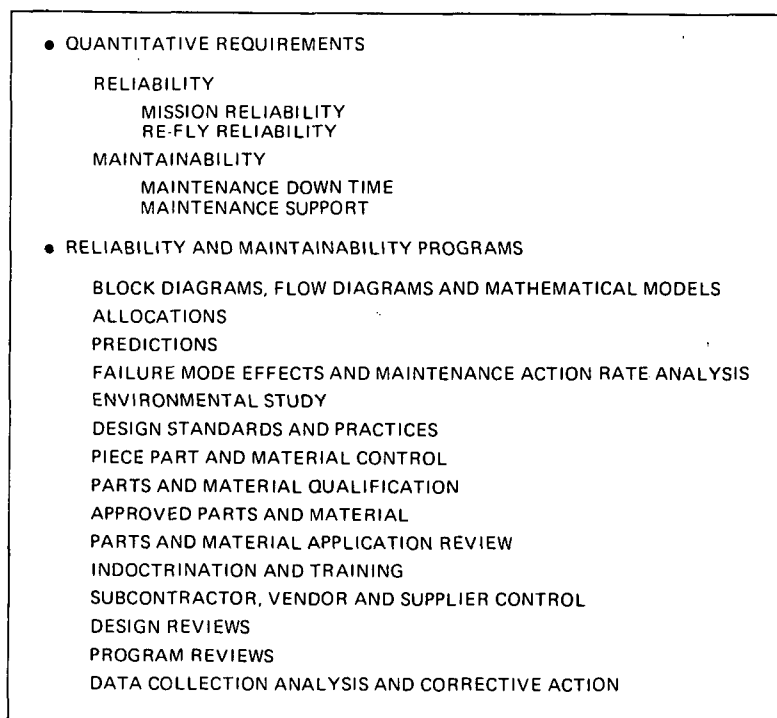


Fig. 5 System Reliability Specification Contents

As in most major contracts, the Weapon System reliability specification also contains quality assurance provisions which associate themselves with the process of inspection, test and demonstration. An outline of the quality assurance provisions of a typical Weapon System reliability specification are outlined in Figure 6.

- RESPONSIBILITY FOR INSPECTION
- CLASSIFICATION OF TESTS
- PREPRODUCTION TESTS
 - PREPRODUCTION SAMPLE
 - SCOPE OF PREPRODUCTION TESTS
 - PREPRODUCTION ACCEPTANCE CRITERIA
- QUALITY CONFORMANCE TESTS
 - SCOPE OF QUALITY CONFORMANCE TESTS
 - QUALITY CONFORMANCE ACCEPTANCE CRITERIA
- TEST METHODS
 - MISSION PROFILES
 - TEST MISSIONS
 - TEST MISSION DURATION
 - MISSION SUCCESS CRITERIA
 - AIRPLANE WEAPON SYSTEM FUNCTIONS
 - SUBSYSTEM FUNCTION SUCCESS CRITERIA

Fig. 6 Quality Assurance Provisions of a Weapon System Specification

It is obvious from the examination of the detailed contents of this typical Weapon System specification that literally all of the minute details of the reliability program - the predictions, estimates, allocations, assessment of risks, etc. have to be worked out prior to the contractor's submittal of a Weapon System proposal. Without this evaluation completed, it would be impossible for a contractor to evaluate the likelihood of his attaining the required levels of system reliability. Without this assessment, it would also be impossible for him to evaluate his financial risks or to establish a competitive position in terms of incentive contracting and its associated negotiation problems.

RELIABILITY INCENTIVE CONTRACTING

The concept of fixed price incentive contracting has gradually found its way to prominence in the Aircraft Weapon Systems business. One problem that has been related to the association of incentives to reliability parameters in the past involved the various weighting factors that were assigned to reliability incentives. One concept of an incentive is, of course, to make the monetary value associated with this incentive significant enough so as to attract management attention to the financial rewards realizable if incentive levels of reliability are achieved or the financial penalties incurred if the demonstrated reliability levels are unacceptable. On one fairly current Aircraft Weapon System contract, which was written under a fixed price incentive contract, overall incentives were divided into three major categories. Minimum incentives were realized by the contractor for attainments of the minimum design and performance parameters and the incentive point total here was based on a 400 point system. The achievement of target values or specification values were incentivized to an 800 point total and the achievement of maximum or ceiling performance parameters were based on a 1000 point incentive system. An examination of the target performance criteria established for this contract illustrated that the reliability and maintainability incentives assigned under this system represented a total of 100 points out of the 800 possible. When scaled to actual dollar incentives this could amount, of course, to a sizeable source of added revenue for the contractor. The reliability and maintainability incentives in this case as compared to other program incentives are as shown in Figure 7.

	INCENTIVE POINTS
WEIGHT	120
PERFORMANCE (CATEGORY A)	48
(CATEGORY B)	20
(CATEGORY C)	40
RELIABILITY MISSION SUCCESS	40
RELIABILITY RE-FLY CAPABILITY	10
MAINTAINABILITY - DIRECT MAINTENANCE	50
MAN-HOURS PER FLIGHT HOURS	
PROGRAM SCHEDULE	72
PROGRAM COST	400
TOTAL INCENTIVE POINTS	800

Fig. 7 Incentive Parameter Relationships

In contracting for Aircraft Weapon Systems, the customer has become more attentive not only to the reliability parameters but the more all-encompassing parameter of maintainability as expressed in terms of direct maintenance man-hours per flight hour. If on one hand, maintenance characteristics of the system are extremely well defined and reliability levels are unacceptable, demonstrations would never be passed. Similarly, if reliability levels of the system were high but maintainability characteristics were less than desirable, the demonstration would likely also be failed. This is true since the direct maintenance man-hours per flight hour concept entails both the frequency of failure directly related to reliability and the elapsed time for repair which is related to the ease of maintenance characteristics of the particular system design. Using the maintainability parameters for purposes of Weapon System demonstration also provides a smooth transition, if required, into future concepts of life cycle costing and the ultimate establishment of long duration program incentives associated with life cycle contracting.

INCENTIVE TECHNIQUES

In the mid-1950's industry saw the development of part failure prediction methodology.⁽⁴⁾ This quickly gave way to reliability program requirements, hi-rel programs, part improvement techniques and countless other reliability controls. It was only a matter of time before all of these appeared in the design requirements and test requirements of design detail specifications. In most recent years, reliability testing became quite common and these reliability test ventures have been adopted to the incentive features of all military contracts. One reason being that it is quite simple to equate MTBF to dollars gained or lost.

One recent publication presented some rather interesting alternate techniques for reliability incentive contracting. The author in presenting his conclusions summarized that:

- The worth of a reliability incentive is dependent upon the size, the program and its associated incentive fee.
- Reliability demonstration tests without previous reliability qualification tests are tremendously risky.
- Reliability incentive formulas where the fee increases at a greater rate as the MTBF improves is a real incentive to the contractor. (This is generally a non-linear incentive curve.)
- Reliability demonstration tests and incentives are of great value when it is desired to keep proven hardware from degrading.

The incentive programs defined in this reference were categorized in three ways:

- MTBF versus incentive dollars on a linear scale
- MTBF versus incentive dollars on a non-linear scale
- Negative MTBF versus penalty dollars

The first two of these plans are considered bona fide incentive plans while the third is construed as a reliability penalty and not an incentive. For a comparison of the first two incentive plans refer to Figures 8 and 9.

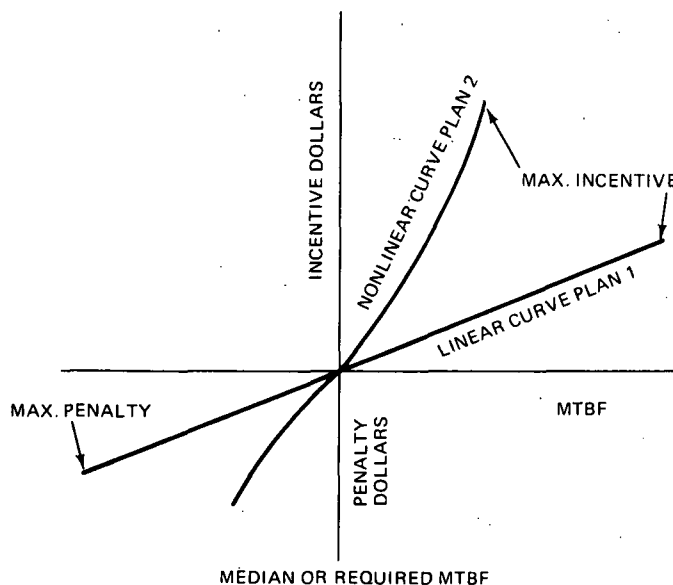


Fig. 8 Example of Linear and Nonlinear Incentive Curves

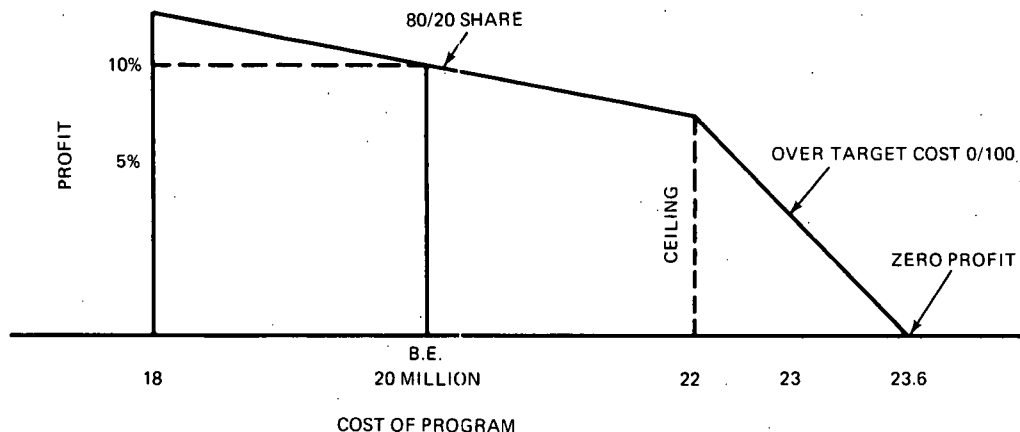


Fig. 9 FPI Profit/Cost Curve

DESCRIPTION OF AN INCENTIVE CONTRACT

It is in order here to describe the basic features of the popular concept of fixed price incentive contracting referred to as FPI. In this type of financial arrangement a target cost is established along with a ceiling cost. All expenditures above this ceiling are assumed by the contractor. Between the target cost and the ceiling cost there is a sharing arrangement normally made with the customer. This sharing arrangement implies that the customer is willing to share in the overrun. If the sharing arrangement, as an example, is 80/20 it implies that the customer will pay 80 percent of the overrun and the contractor only 20 percent. This type of cost sharing is normally illustrated as shown in Figure 2. This arrangement only holds until the ceiling cost is reached. At this point the contractor pays the full share of the overrun which, of course, results in a direct reduction of profits until at some point the profit is reduced to zero which, of course, economically is unacceptable to any profit-making corporation.

Fixed price incentive (FPI) programs are getting more popular for many procurements. This type of contracting, however, does present some real problems when tied directly to reliability incentives. Two of the more subtle considerations that should be taken for FPI contracting are:

1. How much overrun should be planned into the program in order to improve reliability? In other words, what is the actual profit desired from the program?
2. How much of the hoped for incentives should be traded off to counter the increased cost of improving reliability? This can be the greater risk especially if there are other factors which could increase the cost.

In conjunction with the dollar risks, probably of a greater importance is the risk involved in making failure rate predictions. Unfortunately, the whole quantitative reliability game centers around the present methods of making failure rate predictions which are in themselves questionable to say the least.

One proposed system of reliability incentives is the MTBF versus incentive dollars linear curve concept illustrated in Figure 10.

For some median MTBF value (A) no incentive is gained. However, as the MTBF increases or decreases around point (A) the incentive or penalty is assessed. From the incentive point of view, this is a poor plan for a contractor. Normal sampling variations could allow the MTBF to move, as an example, between points (A) and (B). The lucky contractor might get to the (B) incentive. Now this case, it might be desired to spend some money on component part improvement, corrective action or the like in order to gain some incentive. For a very little expenditure, we might guarantee point (B) or point (B¹). However, to get to point (C) or perhaps even point (D) could be exceptionally difficult.

It is easily understandable that a linear increase in expenditure does not necessarily give a linear increase in reliability. That's the reason why this incentive plan does not normally favor the contractor. On the other hand, if for some reason the equipment median MTBF is not achieved, the penalty may not be too severe as the penalty is also linear with respect to MTBF.

The second proposed plan, MTBF versus incentive non-linear curve, is probably the fairest method of incentive contracting. This non-linear plan puts the contractor at a real advantage--see Figure 11 below.

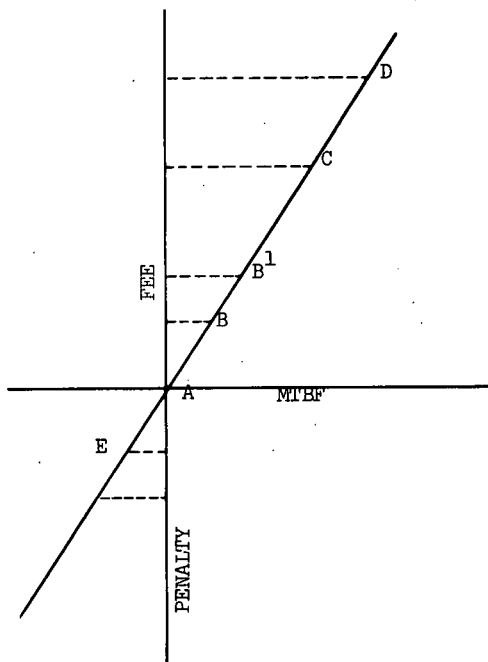


Fig. 10 Plan 1 – Typical Linear Curve

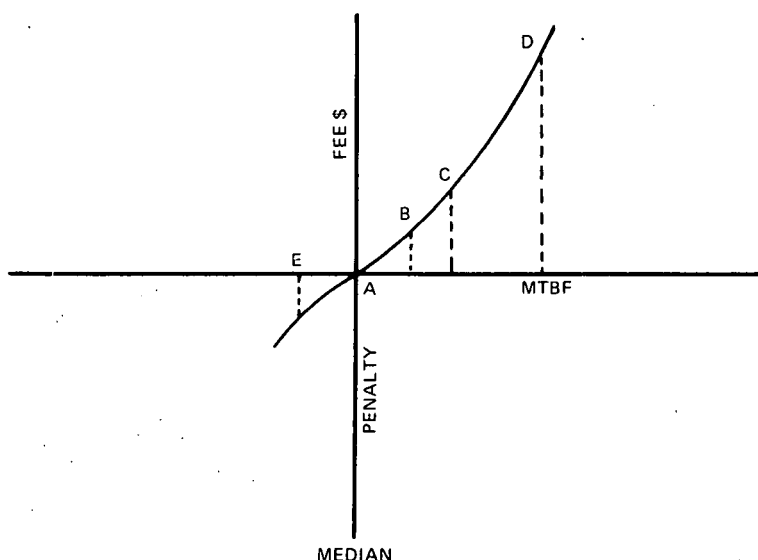


Fig. 11 Plan 2 – Typical Nonlinear Curve

The contractor knows that if he expends a good deal of effort the rewards could be quite attractive. He also knows that if he fails badly the penalty will be more severe than it would have been in the linear plan previously discussed. Examination of Figure 11 shows that the normal variability might still fall between points (A) and (B), but it is evident that the increase in MTBF does not result in the same proportionate increase in fee. For more dollars expended for effort where the risk is greater, the reward is also potentially much greater.

The third plan proposed is the MTBF versus penalty plan. This plan certainly cannot be considered as an incentive program in the truest sense but rather a negative incentive or penalty program. If the median MTBF is not achieved, the contractor is most definitely penalized. A contractor that accepts this type of arrangement during a research and development contract is not making a wise decision. It is true that the contractor has the obligation to meet the requirements but additional severe penalties are not normally justified.

SUBCONTRACTOR RELIABILITY CONTROL THROUGH CONTRACTS

One major aerospace contractor instituted rather severe withholding clauses in its purchase contracts in the early 1960's. All contractor purchase orders for hardware items requiring qualification and/or reliability testing by the supplier included the requirements for contractor engineering approval of all such testing. The following conditions were included:

"Until the contractor has received and approved all qualification and/or reliability test reports required hereunder, the contractor will withhold 20 percent of payments otherwise due Seller. The contractor will either approve or disapprove such reports within no more than 30 days after receipt. The contractor will make final payment of the amounts withheld immediately after approval of such test reports. Pending Seller's submission of, and approval by, the contractor of such test reports, Seller will proceed with manufacture and delivery of articles to the contractor-required delivery schedule specified herein. Successful completion of qualification and/or reliability tests is to be accomplished and acceptable test reports are to be furnished the contractor before (dated included)."

The above clause in this case was used in all purchase orders for parts, equipment, subsystem and systems procured against the contractor specification control drawings or other forms of procurement specs. The clause was initially communicated to all bidders in the contractor's request for quote package and was included within the "special purchase order condition" section of contracts with the suppliers. The clause was handled as a contract condition and not as a technical specification parameter. As such, no wording relative to the withholding was included in any of the contractor's engineering specifications.

The same contractor also took safeguards in instances of development programs where required delivery schedules were such that hardware deliveries had to occur prior to the satisfactory completion of testing by the seller. In these cases the following statement was included also as a purchase order condition to supplement the basic clause listed above.

"Rework or replacement or to be delivered equipment required as a result of failures in qualification and/or reliability testing will be accomplished by the Seller at no increase in contract price."

This method of handling the contractual aspects of the reliability program appeared to touch most of the basic problems normally encountered. First, it made clearly evident to all suppliers the contractor's definite interest in timely test completion and more important perhaps, it also established a financial lever in the contract to ensure appropriate management attention by the suppliers to their reliability test commitments. Secondly, it established limiting criteria for contractor action towards approving or disapproving test reports. Thirdly, it established a specific schedule requirement for test completion. Fourthly, it provided for continuity in supplier's actions as to manufacturing and delivering hardware in parallel with their conduct of required testing. In those instances where schedules dictate or where test failure experience delays the completion of specific tests and also where hardware must be delivered prior to test completion, it establishes the retrofit responsibility and clearly defines that this responsibility resides with the supplier.

This contractor negotiated this type of condition in a number of different ways with various suppliers on various types of procurements. These negotiations at times resulted in reducing the percentage withheld and in other cases, it established a specific dollar amount limitation for the withholding or applied a percentage withholding only against funding that was applicable to an initial procurement under a design and development purchase order but not against subsequent production orders. Aside from the expected deviations resulting from bargaining negotiations, the contractor implemented the clause "as is" in a good number of instances. Many of these instances involved large quantity buys of rather sophisticated hardware. In many cases the money withheld exceeded six figures. However, in some cases where significant quantities of sophisticated hardware were required with accelerated delivery schedule, the contractor quite regularly negotiated a fixed dollar ceiling for the withholding in order not to provide an unrealistic financial burden on the supplier. The contractor here recommended no specific formula for determining the appropriate fixed dollar ceiling. The amount was generally in the neighborhood of approximately one-half million dollars or more.

It should be noted that the clauses as stated read that the percentage withholding is applied against the "payments otherwise due the seller." In instances of major procurements where progress payments by the contractor were involved, the contractor generally followed the Government's pattern of making progress payments at 70 percent of costs actually incurred up to the progress point. In this manner when the 20 percent withholding was applied against the payments otherwise due, the actual payment made shrinks to 56 percent of the incurred costs. This is certainly further reason for negotiating trends towards a fixed dollar amount in the withholding of major procurements. It would otherwise become burdensome to the seller.

Another example⁽⁵⁾ describes attempts to impose incentive contracting techniques to an after-the-fact reliability improvement program during the early 1960's. The goal of this proposal was twofold:

- To form the basis for engineering change proposals for supplier package improvements.
- To emphasize to the customer the intended financial benefits of such a program.

In this case as a result of the difficulty of defining a reliability program on the complete Weapon System due to the constraints of available customer funding, it was determined that in order to satisfy customer requirements, reliability programs should be developed on the most critical subsystems of the Weapon System. Critical subsystems were defined here as systems in which improvements in reliability would result in the maximum benefit to overall Weapon System performance. They selected four such subsystems, all of which were under the contractor's jurisdiction as CFE equipment and they proposed to establish a guaranteed mean time between failure and then sample test each production lot to assure that this MTBF was being achieved or exceeded. Their proposed plan included an incentive/penalty approach in which incentives took the form of added profits that would be obtained if the MTBF values above the certain value were achieved. Penalties were assessed if the MTBF values fell below an established minimum. They ran into considerable difficulty in the early stages of negotiation. Difficulties encountered included:

- How to ascertain the true MTBF value from which the program groundrules could be established?
- How to ascertain the form of incentive--its amount and the scale on which it should be based?
- How to ascertain the form of penalty--its amount and the scale on which it should be based?
- The environmental conditions and methods of testing
- Sample size and lot sizes
- How to accommodate such a program in the middle of a relatively high production program?
- How to control reliability test items?
- How to apply these programs down the line to subcontractors, making them consistent with overall objectives?
- Methods of analyzing failures and the procedures for obtaining corrective action?
- The degree of risk to be assessed to the contractor and to the customer

This contractor did manage to solve most of these concerns to the mutual satisfaction of the customer and himself.

The results reported indicate a very rewarding experience. The customer, as was his initial intent, did obtain an improved system. The manufacturers involved in the production lot testing realized increased profits as a result of increased performance above the value established as the base for incentives. Although actual quantitative improvement factors were not made available, it was stated that almost every system showed a significant reliability improvement. The levels of improvement reported in both subsystem and mission reliability are as shown in Figure 12.

	% OF SUBSYSTEM IMPROVEMENT	% OF MISSION RELIABILITY IMPROVEMENT
COMPUTER	53%	18%
DISPLAY SYSTEM	31%	53%
RADAR	55%	20%
WEAPONS CONTROL	30%	13%

Fig. 12 Reliability Improvements with Incentive Contracting Techniques

This contractor does not profess that all of the above listed reliability improvements were solely a function of the fact that contractual incentives were made available, and he acknowledges that certain design improvements were made but the report lends a great deal of importance to the fact that increased management emphasis on behalf of suppliers resulted from the opportunity to gain more profit on behalf of the suppliers. The same reference reports estimated savings resulting from the reported reliability improvements. Although there were many parameters included in the calculation of these savings, it is interesting to note the comparison of the first year cost savings resulting from the reliability improvements as a result of the program costs. Figure 13 depicts the estimated savings accrued to the customer as a result of this reliability incentive program. These savings considered removal and repair costs only. The reduction of these costs due to the increased MTBF was compared to total program cost. Methods of calculating these costs are listed in the reference. Part of the savings accrued to the contractor were onetime savings. The reason for this saving lies in the fact that the systems delivered to the contractor after the incentive program was initiated experienced far less failures, lowering the cost of the factory and flight acceptance tests. This saving is, of course, a onetime saving. On the other hand, the saving

to the customer would be repeated each year until the retirement of the Weapon System. He projected that the total customer savings on a contract lot covering approximately 300 aircraft would be an excess of \$8M. It should be noted that the amount of money indicated to be saved considered only the improvement in reliability of the systems indicated. There were also additional savings resulting from other system improvements.

	PROGRAM COST	FIRST YEAR SAVINGS
COMPUTER	941,500	301,500
DISPLAY	941,500	174,000
RADAR	1,774,850	785,000
TOTAL	\$3,657,850	\$1,260,500

Fig. 13 Estimated Customer Savings Resulting from Incentive Contracting

The contractor also calculated the total savings projected over a normal 10 year life cycle of the 294 aircraft in question. He projected these total savings at \$8,947,150. He also estimated savings that would have resulted if the incentive plan were imposed at the beginning of the total production lot which involved over 750 aircraft. This calculated program saving in his estimate amounted to \$22,950,660.

Some of the interesting conclusions and recommendations that this contractor put forth as a result of his experience with incentive contracting included the following:

- Do not use canned environmental cycle testing. The environmental cycle should be designed to be representative of how the equipment is going to be used and serviced. This, of course, has some constraints involved with the capability of available environmental test equipment.
- The test specification has to be very detailed. They recommended spelling out in great detail how each failure would be analyzed, what would constitute a failure in terms of definition, the test procedure used and so forth.
- More equitable relation of incentive-to-penalty should be utilized. This particular contract involved the penalty which was not on the basis of reduction of fee but included a rework requirement. They recommended very strongly that industry should generally not accept this type of program because of the difficulty or impossibility of assessing the dollar risks on rework type programs in case reliability improvements are not realized. In addition to the rework clause, the customer requested that industry take contracts in which there was an obligation to retrofit, in the field, the complete fleet. This, of course, brings the contractor to a point where the financial risk is completely unreasonable regardless of the value of statistical risk. Moreover, an incentive could never be offered to balance this potential loss. Since rework or retrofit requirements are impossible to assess, the customer here puts the contractor in a position of being a speculator. They recommended that a worthwhile program be designed in which incentive and penalty are truly on a fee basis, realizing that the customer indeed does not want to reduce contractor's profit. He is more interested in getting a good product which, if it does not operate properly, should be fixed. When dealing with state-of-the-art development, however, and when ultimate field operation cannot be predicated, it is not logical to require the contractor to assume such indeterminable financial risks. Another conclusion offered, related to why it is important not to accept a penalty on a rework basis, is the difficulty for the prime contractor to evaluate the vendor problem in this area. Although rework consideration can be passed on to the vendor, the contractor has to estimate how much cost he may incur if the vendor fails to meet his requirements--the cost that is going to be incurred from the aircraft removals, the re-shipment to the vendor's plants for rework, production delays, etc. To some extent these difficulties can be overcome by having a relatively large bank of parts so that the use of a lot is never begun until the vendor has passed the test on a particular lot. This is sometimes easier said than done since production lines generally have a way of requiring equipment almost on the day it comes out the door.

In still another major Aircraft Weapon System procurement,⁽⁶⁾ the original customer system specification issued in 1960 included the following provision. "The contractor shall plan and conduct a comprehensive reliability program in accordance with the requirements of Weapon Systems specification MIL-R-26674 Reliability Requirements for Weapons Systems."

MIL-R-26674 referenced in the above specification abstract had been released in 1959 and represented the first complete reliability program specification for Air Force systems and the referenced program was the first actual implementation of this specification on a new aircraft. The program proposed by the contractor in response to this requirement was incorporated into the contract and for perhaps the

first time in aircraft history, a large scale reliability engineering effort was initiated simultaneous with the design program. Two years subsequent to contract award these requirements were extended under the more stringent provisions of MIL-R-27542.

Contractor recommendations put forth, as a result of the application of this concept of reliability to early Air Force design, contained some observations including:

- For more equitable competitive pricing, the customer should include in the RFP required MTBF values for the specific functions as well as system MTBF to be demonstrated. In addition, the failure criteria should be included in the RFP. Likewise, the prime systems contractor should clearly specify requirements in failure criteria in his supplier specification documents.
- The dividends from a reliability program investment are directly related to the understanding and active support by contractor management.
- Substantial reliability improvement can be attained without guarantees. It is interesting to note that in this particular recommendation, the contractor here felt that there is a much higher probability of high reliability attainment with a guarantee than without for the following reasons:
 - Management is more attentive to reliability engineering recommendations when there are specific contractual obligations.
 - Factors such as weight no longer dominate the designer's decision-making process.
 - Price of purchase parts is no longer an overriding factor independent of life expectancy.
 - If the supplier is required to guarantee his product to meet a specified numerical performance level, the quality producer is in a favorable position compared to the low quality producer.
 - Timely effective corrective action is more likely to be taken once the problem is identified as a result of failures in demonstration testing.
- Stringent reliability guarantees dictate aggressive reliability emphasis during design, manufacturing, test and early operational phases. The absence of reliability emphasis during any one of these phases normally has a serious affect on product reliability.

It is interesting to note from the above recommendations put forth as a result of early 1960 program experience that the contractor rather quickly concluded the overriding benefits of a well contracted and well specified and perhaps guaranteed reliability program.

CONCLUSIONS

The sophistication of current techniques of contracting, coupled with more challenging technological design goals, requires that all elements of a successful reliability program be carefully pre-planned. Improper emphasis on the establishment of meaningful and yet reasonable reliability objectives can have a disastrous outcome if these objectives become an integral part of an incentivized contract. Every element of reliability program must be geared to the attainment of reliability goals sufficient to satisfy customer requirements. Conversion of system to subsystem requirements and the generation of sub-level specifications and contracts requires careful attention to the evaluation of risks at each step in the process. Once initial requirements are established, a program of analysis and design control must be implemented to provide the needed assurance of goal attainment. Program visibility is provided by a well established reliability program plan, coupled with minimum but meaningful reporting requirements and a controlled system of design reviews.

A well planned program of reliability testing and demonstration that is carefully but effectively tied to contractual incentives and/or penalties will provide the needed tools for assisting in the achievement of design reliability, the measurement of contractual compliance, and for focusing of management attention on the financial advantages of a proper investment in reliability.

Timeliness of reliability program elements is critical. Many preliminary analyses must be performed long before design decisions are firm so that unrealistic reliability commitments can be avoided. Properly weighted subcontractor incentives and penalties must be related to their reliability requirements to insure that, at times when pressing delivery schedule make sacrifices attractive, trade-off decisions will be influenced greatly by potential financial consequences.

Reliability specification demonstrations and guarantees will not in themselves assure the success of a program. History has proven, however, that once these elements are defined, proper management attention on design reliability is usually a natural outcome and with this added stimulus, the attainment of a reliable product becomes far more feasible.

REFERENCES

1. J. S. Coutinho, The Reproduction Process, 5th Pacific Area National Meeting, American Society for Testing, Phoenix, Arizona, 1965
2. C. V. Overton, Reliability Testing Requirement, Management and Test Plans, 15th Annual Technical Meeting, IES, Anaheim, California, 1969
3. J. J. Bussolini and S. A. Weisberg, The Systems Approach to Reliability Demonstration, Annals of Assurance Sciences, Denver, Colorado, 8th R & M Conference, July 1969
4. M. Raphelsen, Reliability Incentives - A New Dimension, Institute of Environmental Sciences, Annual Meeting, Anaheim, California, 1968
5. C. W. Russell, Report on Incentive/Penalty Reliability Programs, ASME, SAE Reliability Symposium, San Francisco, California, 1964
6. J. T. Hinely and F. A. Slovall, C-141A Reliability Program, Annual Reliability Symposium, IEEE, Washington, D. C., January 1968

RELATIONSHIPS BETWEEN PROGRAM TEST AND USER SUPPORT COSTS

M. M. Tall

RCA

The discussions during this lecture series have been primarily directed toward the improvement in system effectiveness as a result of reliability improvement and toward the various techniques available to achieve that improvement. The value of an extensive AGREE-type test program has been discussed as providing the focal point for assessing reliability effort during the RDT&E and production phases and for directing future effort. Depending on the system requirements, the reliability effort, including the test program, can be quite costly. From an economic point of view, however, the reductions in maintenance and support costs resulting from improved reliability can lead to substantial savings in the total cost of ownership. It would appear, therefore, that an investment in improved reliability is always cost effective. However, there are several militating factors which may make a reliability investment less attractive than it may initially appear to be.

An analysis, including all appropriate factors, is required to properly assess what the optimum values of acquisition cost and operational reliability should be if the total cost of ownership is to be minimized. In the event a higher order of reliability than indicated as optimum by the analysis is required by operational considerations, the analysis should estimate the acquisition cost increase required.

This paper will address itself to several significant factors that should be included in a cost ownership analysis of avionic equipments. The value of reliability improvement efforts, including AGREE-type test programs, will be assessed.

Cost of ownership considerations are usually divided into three major categories:

- (1) Research, Development, Test and Evaluation (RDT&E) Costs.
- (2) Initial Investment Costs.
- (3) Operating and Maintenance Costs (on annual or life cycle basis).

RDT&E costs are non-recurring and include all costs necessary to achieve an acceptable equipment design. Initial investment costs include the cost of the prime equipment, initial spares and specialized test equipment. Operating and maintenance costs include the cost of flight line, base and depot personnel, spares replenishment and replenishment of specialized test equipment. A more extensive breakdown of these cost categories may be found in Appendix A.

Many analyses have shown that operating and maintenance costs are highly sensitive to improvements in reliability. However, if we refer to the very familiar qualitative relationship in Figure 1, it is evident that the cost of obtaining a reliability improvement increases with the existing level of reliability.

Also evident from these curves is the existence of an optimum value of reliability which minimizes the overall cost of ownership.

There are several significant factors which contribute to the simple relationships shown in Figure 1. These include: changes in RDT&E costs with changes in reliability; changes in initial investment costs with changes in reliability; changes in O&M costs with changes in reliability.

It has been estimated by Hevish⁽¹⁾ that RDT&E costs increase 5 percent for each 10 percent improvement in MTBF (mean time between failure). This approximation appears to hold true for incremental changes to the normal range of MTBFs encountered today. Colandene⁽²⁾, however, in considering the difficulties in achieving the higher levels of reliability has classified reliability into three categories, normal, high and ultra-high. Utilizing his basic data, the RDT&E cost increases have been calculated as follows: RDT&E costs increase 4.3 percent for each 10 percent improvement in MTBF in the reliability range from "normal" to "high". Thus, the average percent increase of 5 percent per 10 percent improvement discussed by Hevish is a reasonably good figure for discussion purposes.

Initial investment costs also show a marked increase with reliability improvements. Again utilizing Colandene's data, production costs increased 4.2 percent for each 10 percent improvement in MTBF in the reliability range from "normal" to "high" and 4.9 percent in the range from "high" to "ultra-high". An average figure of 4.5 percent

will be employed during this discussion. With these estimates, doubling the projected MTBF of an avionic equipment would increase RDT&E costs by 50 percent and production costs by 45 percent. Production costs, of course, are more significant since RDT&E costs are written off against all production equipment. If production is substantial, then the incremental RDT&E cost increase per equipment may be quite small. In addition, some savings may be evident as a result of larger material orders and the feasibility of specialized automation in large production runs.

The increase in production costs may be attributed to:

- (1) Premium costs for high reliability parts and materials. These costs can add about 50 percent to the cost of materials. Part burn-in can add another 25 percent to their cost.
- (2) Increased in-process testing and improved process controls during fabrication and assembly can add 10 percent to these costs.
- (3) Increased inspection can add 25 percent and equipment burn-in another 60 percent to inspection and test costs.
- (4) Reliability support costs can grow 150 percent when production sampling tests are involved.
- (5) Quality Engineering costs can increase 35 percent to cover the increased attention to problem areas.

These are a few indications of how high reliability requirements can affect production cost. There are many others such as the cost of training operator personnel, longer production cycle time as a result of extra care, production delays while problems are being solved, retrofit of built equipment to remove a problem and material losses when improved versions are employed as a result of a problem.

However, if the reliability improvement is substantial, it may result in a reduction in the number of prime equipments required for standby and in the support pipe line. This reduction may well counterbalance the increased acquisition cost associated with each equipment. Although it is not the intent of this paper to discuss weapon system effectiveness analyses, the results of such an analysis may have a significant effect on reliability versus cost considerations. The required number of aircraft necessary to carry out a mission or set of missions is a function of the capability, reliability, survivability, availability, etc. of the aircraft as well as the subsystems. Analyses can indicate the average force size requirements for all projected missions. The increase in force size resulting from estimated aborts due to avionic failures may have significant impact on required subsystem reliability versus the cost of its attainment. In this case, the savings are in number of aircraft required as opposed to the former consideration of savings in prime avionic equipment. Borchers and Churchill⁽³⁾ in describing the procedure employed in an Advanced Manned Strategic Aircraft (AMSA) study illustrates this point in Figure 2. Starting with an assumed avionic MTBF requirement of 400 hours, the increase in force requirements are shown for smaller MTBF values. The cost of 5 or 10 percent additional aircraft may well make a cost of ownership analysis of avionic equipment academic.

The use of redundancy or back-up modes as a means of improving reliability should be briefly discussed. Redundancy may not have a significant effect on RDT&E costs but does reflect in increased production costs for the redundant equipment or elements. The effect of increased weight and volume on aircraft cost or mission capability should be considered. O&M costs will increase since additional equipment must be maintained. Thus, redundancy is a useful technique when operational requirements can be met more economically in this manner than by increasing prime equipment reliability or if the required reliability is beyond the current state-of-the-art. Selective redundancy has proved to be cost effective in many instances where higher orders of reliability are required.

The reduction in operating and maintenance costs as a result of improved reliability may be substantial. However, it should be recognized that a 50 percent improvement in reliability does not reflect in a 50 percent saving in support costs. The number of support personnel may not be affected unless the reliability improvement is substantial, although they may be more lightly loaded. Depending on the avionics support required, there may be a minimum number of personnel required regardless of the reliability improvement involved. In addition, the cost of spares may be higher, even though the quantity is reduced. Further, there are a number of failures that are due to accidents, good parts are replaced because of improper maintenance, and material shrinkage occurs because of loss or damage. The number of these replacements are not

affected by the reliability level, but the material costs of these replacements are.

The decrease in operating and maintenance costs, in spite of these factors, may still make the initial expenditure worthwhile. However, these savings are generally available in the latter portions of an equipment's life. As a result, there are several factors which may reduce the value of such savings. Expenditures in the latter portion of an equipment's life may be less of a budget burden than earlier expenditures, reducing the value of future savings. Technical obsolescence and/or program cancellation may prevent realization of these future savings. Further, aircraft attrition, as a result of combat or accidents, may require replacement at higher cost without realization of later savings. These factors may have a significant effect on the desirability of a reliability investment.

In determining the relative ability to fund a program during the early or latter phases of its life, two considerations are involved:

- (1) The economic growth of the nation.
- (2) Inflationary effects.

Sobin⁽⁴⁾ discusses the growth of a nation in terms of per capita income growth. If the per capita growth is positive, then later expenditures assume a smaller portion of the national income and are less of a budget burden. Supplementing this thesis is the potential value of later funds if invested today. A private investor, comparing alternative opportunities, examines the potential payoff and risks in relation to a low risk interest bearing investment, such as a bank. That is, funds invested today are expected to have a greater value later. Conversely, a saving at a later time has a smaller value today. That is, the saving must be discounted to its present value. For example, one million dollars invested today is worth 1.79 million in 10 years at a 6 percent annual interest rate and 2.594 million at a 10 percent interest rate. Conversely, a one million dollar saving ten years from now is equivalent to (present value) an investment today of \$559,000 at 6 percent and \$385,000 at 10 percent.

A nation, of course, does not have the investment opportunities available to a private investor. National income, if not spent in one area, will generally be spent in another governmental function. However, if the nation is operating on a deficit budget, the cost of borrowing funds affects the value of later savings. Further, if the economy is growing at an annual rate of, say, 3 percent, 5 percent or 8 percent, then an investment (normalized at 1.0) as percentage of national income assumes a smaller percentage of income in 10 years, .745, .614 or .463, respectively.

This discussion, of course, is concerned with real growth and did not consider inflationary effects. It is not realistic to evaluate the effect of inflation on prices alone; the effect of inflation on income must also be considered. If prices are growing faster than income, then this difference should be added to expenditures planned in the future. At the same rate, inflation would have no effect on the ability of the budget to fund a future expenditure. On the other hand, if income is growing at a greater rate than prices, that is, the nation is becoming more affluent, then the difference further discounts the value of future savings.

The risks of technical obsolescence and program cancellation are real and cannot be ignored. Although the risk of technical obsolescence extends throughout the program life, there is a distinct probability of program cancellation during its early life as a result of technical obsolescence, state-of-the-art limitations, or other factors. Technical obsolescence may require equipment replacement earlier than planned in its life cycle. Under these conditions, projected savings may not be realized.

Aircraft attrition may assume major proportions, particularly in combat conditions. If the aircraft is replaced, the higher acquisition costs negate some of the expected savings.

Let's examine the effect of these factors. Five hundred avionic systems are to be procured. The contract calls for an RDT&E phase of two years at a cost of six million dollars. The RDT&E phase is followed by a five year production phase at the rate of one hundred equipment per year. Each system cost \$200,000 for a total production cost of \$100 million for a total contract value of \$106 million. The operational life is planned for 15 years, overlapping all but the first year of production. For convenience, the inherent reliability of the equipment is assumed to be immediately available with initial production.

Several considerations are involved in Tables 1 and 2. Table 1 relates these considerations to a system possessing high reliability and Table 2 to a system of lesser

reliability. The reliability of these systems are expressed as a ratio (M_R) of the annual O&M cost to the production cost of the equipment. Thus, in Table 1, $M_R = .1$, the annual maintenance cost per equipment is \$20,000 ($.1 \times \$200,000$). In Table 2, $M_R = .3$, the annual maintenance cost is \$60,000 ($.3 \times \$200,000$).

In each table, the cost of ownership for the baseline system is shown for each year of its projected life. An incremental improvement of 20 percent is compared to a significant improvement of 50 percent. Further, for each improvement, the effect of not including discounting ($r = 0$) is compared to the effect of a 3 percent discount rate ($r = .03$) - the cost of ownership difference for each condition to the baseline system is shown.

In Table 1, it is evident that an incremental improvement to a high reliability system is generally not cost effective. A 20 percent improvement increases RDT&E costs by 10 percent or \$0.6 million and production costs by 9 percent or \$9 million for a total increase of \$9.6 million in acquisition costs. For $r = 0$, breakeven occurs in the fifteenth year with a net savings of \$3.4 million. For $r = .03$, breakeven occurs in the seventeenth year with a net savings of \$1.5 million.

A more significant 50 percent improvement increases RDT&E costs by 25 percent or \$1.5 million, production costs by 22.5 percent or 22.5 million for an increase in acquisition costs of \$23.7 million. For $r = 0$, breakeven occurs in the eleventh year with a total net savings of \$28 million; $r = .03$ results in a twelfth year breakeven with savings of \$25.1 million. Improvements in high reliability systems should be carefully evaluated as to whether an improvement or a next generation design is more cost effective.

An increase in the initial investment becomes more cost effective at lower levels of reliability as is illustrated in Table 2. A 20 percent improvement reaches breakeven during the ninth year for $r = 0$ and $r = .03$ with savings of \$29.4 and \$28.8 million, respectively. A 50 percent improvement reaches breakeven in the seventh year for $r = 0$ and the eighth year for $r = .03$ with net savings of \$132 and \$131.3 million, respectively. Thus, it is evident that a significant improvement of 50 percent in a relatively low reliability system is cost effective. In general, a significant improvement is easier to obtain in a low reliability system when compared to a higher reliability one.

It should be noted that in calculating O&M costs that a 20 percent improvement was assumed to result in a 10 percent saving in O&M costs and a 50 percent improvement in 40 percent savings. The effect of variations in several key factors should be noted. The higher the projected reliability of the baseline system, the lower the savings and, in fact, additional cost may result. Conversely, the lower the reliability, the greater the effect of an investment. Savings are directly relatable to the improvement programmed except for ultra-high reliability systems where the cost of an incremental improvement can be very large. Utilizing higher discount rates reduce savings and extend the breakeven point further in the program's life.

The effect of aircraft attrition should be noted. Under peacetime considerations, the expected losses due to accidents, while reducing the savings, do not do so significantly. Under combat conditions, losses may negate all projected savings. However, the increase in force size required because of avionics reliability will more than counterbalance this negative factor. In the analysis, it was assumed that the inherent reliability was achieved in initial production. In actual operations, an equipment possessing "normal" reliability may take as long as 4-5 years to attain its inherent reliability. Instituting a rigorous reliability program, including a test program, results in a sharper reliability growth. Thus, the inherent reliability, a higher level, may be attained in 2 years.

The effect is to increase the cost of ownership of both the baseline and improve systems. However, the savings resulting from the improved over the baseline system may be significantly improved.

The value of a more rigorous reliability and test program in terms of cost is highly dependent on the level of reliability projected for the baseline system. For a high reliability system, incremental and even significant reliability improvements may not be cost effective. However, for systems possessing "normal" or lower levels of reliability, an investment in acquisition costs necessary to achieve a significant improvement is highly cost effective.

References:

- (1) A. H. Hevish, "Cost of Reliability Improvement", Proceedings of the Annual Symposium on Reliability, 1967.
- (2) B. T. Colandene, "Program Costs vs. Reliability", Proceedings of the National Symposium on Reliability, 1964.
- (3) C. R. Borchers and R. E. Churchill, "System Design Trade-offs and Economic Planning", Proceedings of the Annual Symposium on Reliability, 1966.
- (4) B. Sobin, "Interest Rates in Weapon System Evaluation", presented to the EIA Requirements Committee, December 1964.

APPENDIX A

COST OF OWNERSHIP FACTORS

- I. Conceptual Phase
- II. Definition Phase
- III. Research, Development, Test and Evaluation
 - A. System Development (including support equipment)
 - 1. Preliminary Study and Design
 - 2. Design
 - 3. Purchased Materials
 - 4. Fabrication and Assembly
 - 5. System Management
 - B. System Test and Evaluation
 - 1. Test Facilities
 - 2. Test Materials
 - 3. Prototype Construction
 - 4. Installation
 - 5. Test Operations
 - 6. Management
 - C. Documentation
- IV. Initial Investment
 - A. Production Facilities
 - B. Tooling and Test Equipment
 - C. Purchases
 - 1. Materials
 - 2. Supplier Controls
 - D. Fabrication and Assembly
 - E. Test
 - 1. Facilities
 - 2. Equipment
 - 3. Materials
 - 4. Installation
 - 5. Test Operation
 - F. Military Facilities
 - 1. Operational
 - 2. Maintenance
 - 3. Training

- 4. Support
 - G. Initial O&M Training
 - H. Spares
 - I. Technical Data
 - J. Engineering Support
 - 1. Modifications and Changes
 - 2. Sustaining Engineering
 - K. Packing and Shipping
 - L. Travel
 - M. Management
- V. Operating and Maintenance Costs
 - A. Installation
 - B. Maintenance
 - 1. Spares
 - 2. Consumables
 - 3. Facilities
 - 4. Tools

FIGURE 1
AGREE REPORT COST MODELS

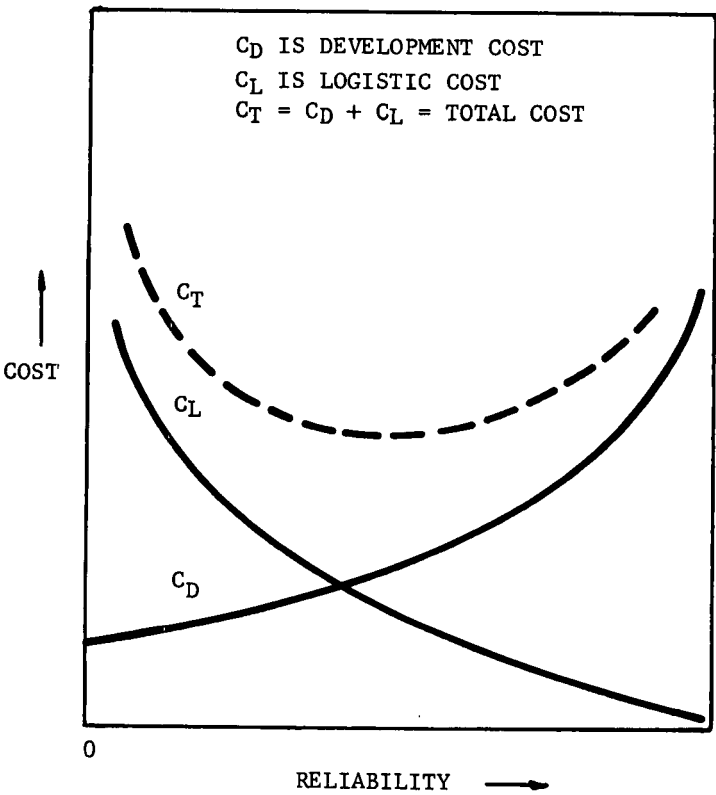


FIGURE 2
INCREASED FORCE REQUIREMENTS DUE
TO DEGRADED SYSTEM RELIABILITY

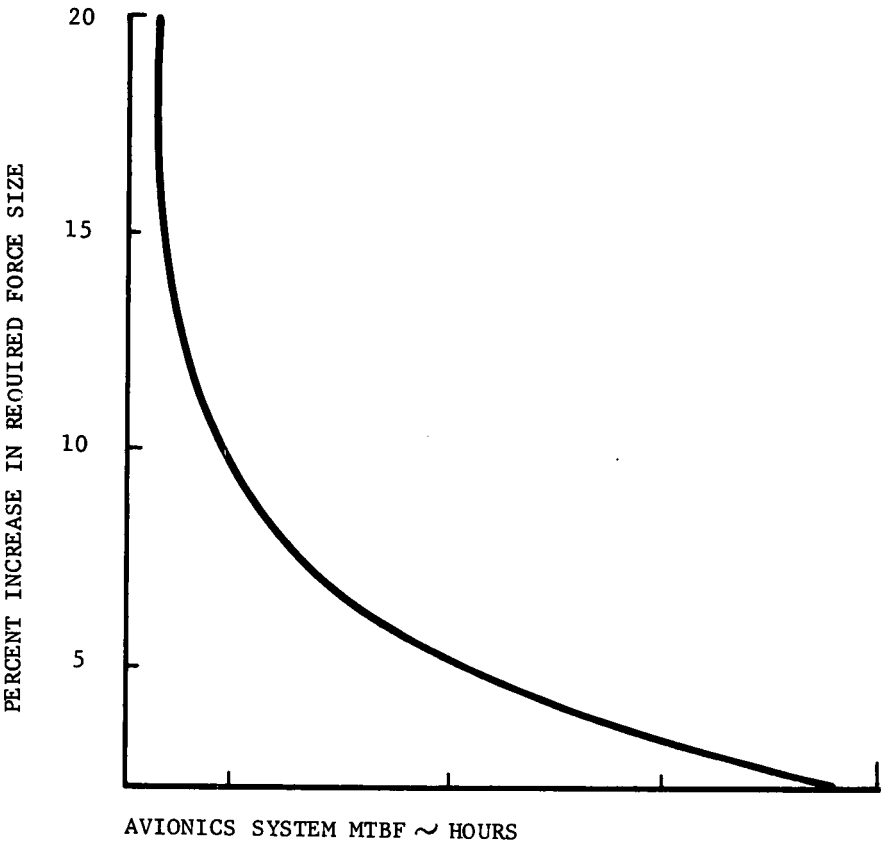


TABLE 1
 COST OF OWNERSHIP COMPARISON
 FOR $M_R = .1$
 (\$10⁶)

Year	Baseline System Cost	20% Improvement				50% Improvement			
		r = 0		r = .03		r = 0		r = .03	
		Cost	Differ- ence	Cost	Differ- ence	Cost	Differ- ence	Cost	Differ- ence
1	3.0	3.3	+0.3	3.3	+0.3	3.8	+0.8	3.8	+0.8
2	6.0	6.7	+0.6	6.6	+0.6	7.5	+1.5	7.5	+1.5
3	26.0	28.4	+2.4	28.4	+2.4	32.0	+6.0	32.1	+6.1
4	48.0	52.0	+4.0	52.0	+4.0	57.7	+9.7	57.7	+9.7
5	70.0	75.4	+5.4	75.5	+5.5	82.6	+12.6	82.7	+12.7
6	92.0	98.6	+6.6	98.7	+6.7	106.7	+14.7	107.0	+15.0
7	114.0	121.6	+7.6	121.8	+7.8	130.0	+16.0	130.7	+16.7
8	124.0	130.6	+6.6	130.9	+6.9	136.0	+12.0	137.1	+13.1
9	134.0	139.6	+5.6	140.1	+6.1	142.0	+8.0	143.5	+9.5
10	144.0	148.6	+4.6	149.2	+5.2	148.0	+4.0	150.0	+6.0
11	154.0	157.6	+3.6	158.4	+4.4	154.0	0	156.5	+2.5
12	164.0	166.6	+2.6	167.8	+3.6	160.0	-4.0	162.9	-1.1
13	174.0	175.6	+1.6	176.7	+2.7	166.0	-8.0	168.9	-5.1
14	184.0	184.6	+0.6	186.0	+2.0	172.0	-12.0	174.9	-9.1
15	194.0	193.6	-0.4	195.2	+1.2	178.0	-16.0	180.9	-13.1
16	204.0	202.6	-1.4	204.4	+0.4	184.0	-20.0	186.9	-17.1
17	214.0	211.6	-2.4	213.5	-0.5	190.0	-24.0	192.9	-21.1
18	224.0	220.6	-3.4	222.5	-1.5	196.0	-28.0	198.9	-25.1

TABLE 2
 COST OF OWNERSHIP COMPARISON
 FOR $M_R = .3$
 (\$10⁶)

Year	Baseline System Cost	20% Improvement				50% Improvement			
		r = 0		r = 0.3		r = 0		r = 0.3	
		Cost	Differ- ence	Cost	Differ- ence	Cost	Differ- ence	Cost	Differ- ence
1	3.0	3.3	+0.3	3.3	+0.3	3.8	+0.8	3.8	+0.8
2	6.0	6.6	+0.6	6.6	+0.6	7.5	+1.5	7.6	+1.5
3	26.0	28.4	+2.4	28.4	+2.4	32.0	+6.0	32.2	+6.1
4	52.0	55.6	+3.6	55.6	+3.6	60.1	+8.1	60.2	+8.2
5	84.0	88.2	+4.2	88.4	+4.4	91.8	+7.8	92.1	+8.1
6	122.0	126.2	+4.2	126.5	+4.5	127.1	+5.1	127.6	+5.6
7	166.0	169.6	+3.6	170.0	+4.0	166.0	0	166.6	+0.6
8	196.0	196.6	+0.6	197.1	+1.1	184.0	-12.0	184.7	-11.3
9	226.0	223.6	-2.4	224.2	-1.8	202.0	-24.0	202.7	-23.3
10	256.0	250.6	-5.4	251.2	-4.8	220.0	-36.0	220.7	-35.3
11	286.0	277.6	-8.4	278.2	-7.8	238.0	-48.0	238.7	-47.3
12	316.0	304.6	-11.4	305.2	-10.8	256.0	-60.0	256.7	-59.3
13	346.0	331.6	-14.4	332.2	-13.8	274.0	-72.0	274.7	-71.3
14	376.0	358.6	-17.4	359.2	-16.8	292.0	-84.0	292.7	-83.3
15	406.0	385.6	-20.4	386.2	-19.8	310.0	-96.0	310.7	-95.3
16	436.0	412.6	-23.4	413.2	-22.8	328.0	-108.0	328.7	-107.3
17	466.0	439.6	-26.4	440.2	-25.8	346.0	-120.0	346.7	-119.3
18	496.0	466.6	-29.4	467.2	-28.8	364.0	-132.0	364.7	-131.3

SYSTEM OPERATIONAL CONSIDERATIONS AND THEIR RELATIONSHIP TO THE TEST PROCESS

W. T. SUMERLIN
Manager, Engineering Reliability
McDonnell Aircraft Company
P.O. Box 516
St. Louis, Missouri 63166, U.S.A.

SUMMARY

Initial decision must be made as to the extent to which test conditions and profiles must simulate operational field use. Frequently the wide variety of expected field utilizations make test standardization more valuable for comparison purposes than accuracy of simulation of field conditions. Then the usual approach is to select standardized test conditions equal to or more than the most severe expected field environment. Important in this process is the choice of cycle timing and thermal extremes for operational cycling. Often it is found that standardized cyclic testing environments lead to the demonstration of a reliability figure considerably worse than will later be observed in typical field use. Thus system procurement is often to a reliability requirement related to test conditions rather than field conditions. Reliability growth, or the extent by which the reliability of a system hardware unit can be raised by burn-in, test, failure analyses, and corrective design change, and the extent by which the average reliability of all hardware units being procured can be raised during the life of the procurement program is difficult to predetermine but some useful indicators do exist. Present procurement practice leads to extensive use of these techniques.

INTRODUCTION

Reliability as a system performance characteristic is usually defined in terms of failure-free performance-as-desired for critical operating periods. The common index of reliability that most of the time suits such a reliability definition is Mean-Time-Between-Failures, sometimes slightly varied in form to Mean-Cycles-Between-Failures, or Mean-Time-Before-Failure. The first and most general variation of this index presupposes an operational system whose continuous satisfactory performance for critical operating periods is of interest. This system from time to time suffers unexpected failure, or cessation of satisfactory performance, whereupon it is returned to operation through repair or other remedy, only to sooner or later suffer another failure. The Mean-Time-Between-Failures is the average operating interval between successive outages, and when only unpredictable failures are considered, this Mean-Time-Between-Failures is most frequently found to be constant for a static system design. It is not the purpose of this paper to expand on the theory of random failures, the exponential theory of reliability or such basics, but rather to take a particularly close look at Mean-Time-Between-Failures, hereafter shortened to MTBF, as an index of reliability for use in describing operational requirements and relating them to test and verification observations. Also to consider MTBF as a quantitative requirement to be specified when defining procurement and operational requirements. With proper understanding of certain limitations MTBF can become the common parameter relating reliability to all conditions of operation, be they field conditions, test conditions, simulated conditions, or otherwise. The problem at hand then is to examine all necessary limitations and constraints that affect the relationship of MTBF to performance and operation criteria.

MTBF IS A VARIABLE EVEN FOR A FIXED DESIGN

The MTBF of a system is determined by the sum of the failure rates of all the individual pieces, parts, and functional items that compose the system, and MTBF is then the reciprocal of this failure rate summation. If we limit failure consideration to unpredictable failures, because when a failure can be predicted, one can replace the soon-to-fail item just prior to its failure and presumably at a moment of convenience which will avoid a system failure, then the unpredictable or random (in time of occurrence) failures will reduce system reliability in proportion to their frequency and prime consideration must go to analyzing and eliminating their cause.

Extensive observation of piece part failure rate variation over the past two decades has identified for the standard piece parts the factors that have major effect on failure rate. For ease of discussion the important factors can be divided into two categories: those that are present as part of the external environment in which the part must operate; and those that exist as a result of the way in which the part is being employed and thus are produced internally in the part. In the former category, the most prevalent and significant factor is temperature. Temperature often accelerates deterioration processes in proportion to the (absolute) temperature level. It can change other characteristics also, for instance through thermal expansion and contraction. There are undoubtedly many more thermal mechanisms to relate temperature to failure rate, but of importance here is only the fact that often a significant relationship exists. Stress and vibration are sometimes related to failure rate through fatigue and similar mechanisms. While humidity and altitude effect (air pressure) can often be eliminated as deterioration factors by hermetic sealing, design oversight sometimes leaves failure rate dependency on these factors. There are some occasions when failure rates are raised by a radiation environment. Thus the failure rate of an item will be determined by some sort of complex summation of the effects of those factors of external environment to which the item is sensitive. Knowledge of the quantitative effect produced by each external environmental factor will enable us to gage relative failure rates in different environments, but environmental complexity and large and varied piece part population often force mathematical treatment beyond tolerable extremes. But then practical examples of such systems can be life tested to demonstrate failure rate, and the environment can be varied and the change in failure rate observed. Thus we do know that failure rate and MTBF will vary with and will be a function of the operating environment.

From the external environment and its effect on failure rate, it is a simple step to consider internal environment and the effect of operating parameters on the failure rate. Most important are electrical stress factors such as wattage dissipation which produces internal heating, in turn accelerating the failure rate in the same manner as external high temperature, and voltage gradient which produces breakdown of insulation,

migration of metals, and other dissipative effects which directly increase failure rate. An often quite severe internal environmental factor which can easily be overlooked is operation cycling. The cyclic stresses produced include cyclic thermal expansion and contraction and resulting mechanical stress with mechanical fatigue, and cyclic electric-field insulation fatigue. Failure rates can climb rapidly from such causes. Again common piece part failure rates can be tabulated as functions of the more common internal factors, and thus MTBF estimates can make some allowances. However, in a large complex system with many varieties of parts, and many varieties of simultaneously imposed environmental factors, the best calibration will be by experiment.

From consideration of internal and external environment, let us turn to the relationship of MTBF and failure rate to the manner in which a system is operated and the definitions which establish satisfactory performance. To begin with, large systems frequently have several operating modes, each of which employs part of but not necessarily all of the total system. Since one can easily imagine a reduction in failure rate if a significant portion of a system need not be operational, it is obvious that MTBF can depend on system operating mode. The second factor, definition of satisfactory operation, brings up a situation which can easily defy quantitative analysis. If system performance requirements relate heavily to quantitative measurement of performance elements, it may be impossible to judge satisfactory system operation without excessive subjective bias unless test equipment is used to measure performance. Thus in field use, system operation by one operator might be judged failure free, and by another operator in identical circumstances as unsatisfactory. Historically, it was found that airborne avionic systems appeared to have notably higher MTBF when used in combat than when used in field exercise. Perhaps the explanation here is that in field exercise, the operator has more concern in careful scrutiny of a system which he wishes would suffer fewer failures. In combat, the operator's attention is turned to other things, and he expects no more from the system than he has been accustomed to getting, hence does not score failures so frequently.

If desired, excellence of system maintenance and its effect on system MTBF can be included in the overall consideration, and since it is importantly dependent on human factors, it can be considered along with system performance factors.

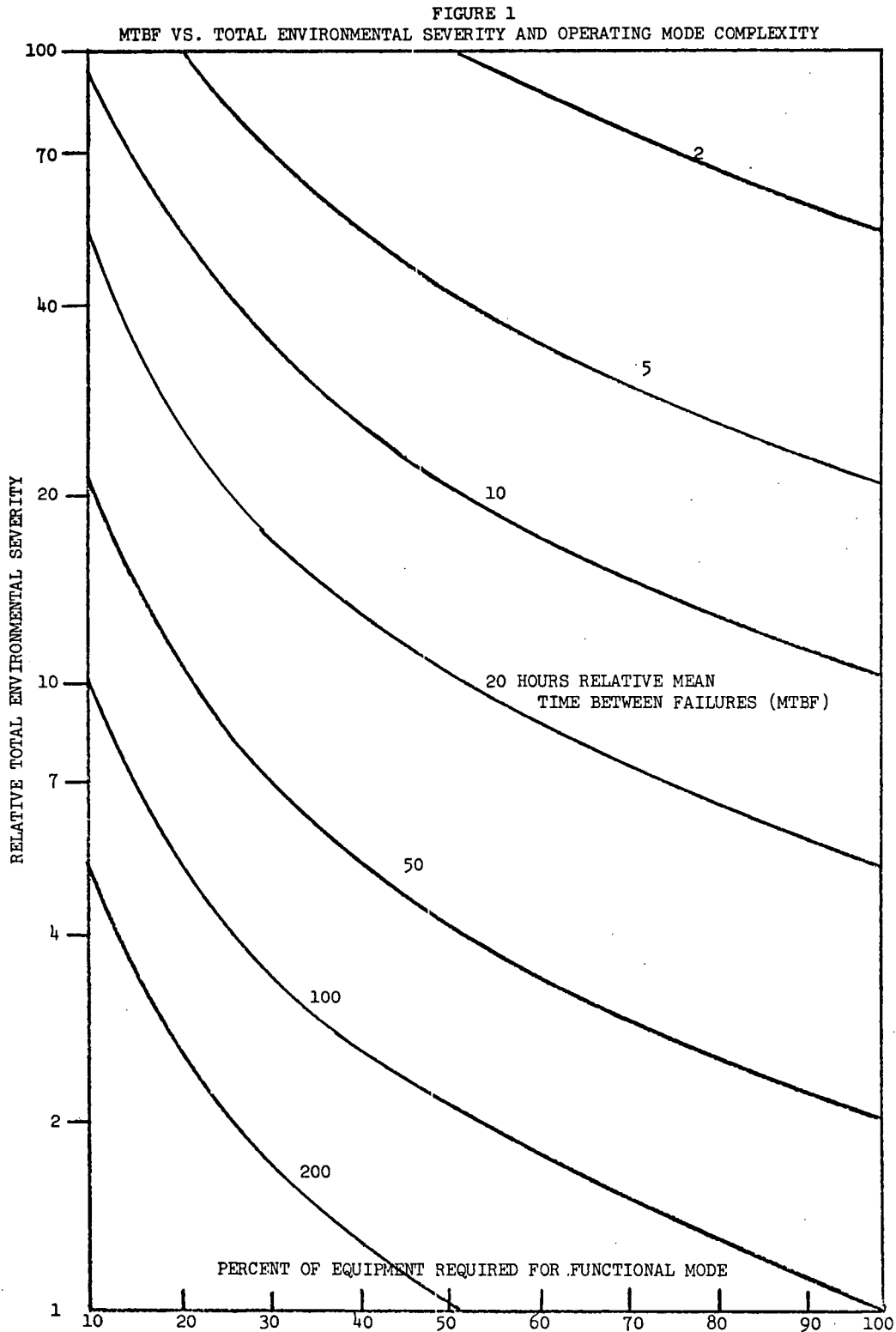
Let us consider making up a chart for an hypothetical system. The abscissa of this chart will indicate performance (and maintenance) modes with increasing severity in terms of increasing failure rate from left to right. The ordinate axis will measure total combined environmental severity, both external and internal, with respect to its effect on increasing failure rate. Hypothetically now, the subject system will have a particular MTBF for every severity level of operation (along the abscissa) and for every severity level of environment. Thus the chart will be a matrix of MTBF's. It will be found that where environmental severity (with no operational severity) produces the same effect on failure rate as operational severity (with no environmental severity) the MTBF will be the same. In fact, contour lines may be drawn on the chart connecting all points of equal MTBF, and one can expect that these contour lines will appear to describe increasing gradient (increasing failure rate, decreasing MTBF) as one progresses from the origin to the upper right hand corner. The shapes of the contours will depend on the relative scales used for the ordinate and abscissa and the linearity of the severities involved. In any case, the conclusion to be drawn is that a given system inherently possesses a broad band of MTBF's depending on operating circumstances, and system MTBF is a combined function of environmental and operational severity. See Figure 1.

SPECIFYING SYSTEM MTBF

If system reliability is an important performance parameter, then it must fall within desired limits if the system is to be effective. Operational planning can identify limiting MTBF minimums for operational conditions of maximum requirement. Other related performance requirements together with the reliability requirement will establish whether needs for reliability push or are within the present state-of-the-art. If they are quite nominal then considerable latitude for setting requirements is permissible. If however, reliability is going to be difficult to attain then the considerations to follow will perhaps be of considerable benefit.

Difficult reliability requirements usually justify means of verification such that development will not be considered complete unless the desired reliability is attained. Because reliability cannot be verified by test or measured until working equipment exists, failure to achieve the reliability requirement usually means design correction and sometimes extensive redesign. If detailed reliability estimates based on a detailed proposed design can be counted upon to be accurate then a useful indication of design adequacy can be based on a reliability estimate without waiting for a working model to be constructed and tested. For this reason, when a development program reaches the point of reliability demonstration test, it is usual to employ the test results to not only verify reliability requirement compliance, but also to verify accuracy of the reliability estimate. To make this latter verification possible, two conditions must prevail. First, a reliability estimate employing the best available technique must have been diligently performed with emphasis on high accuracy. Secondly, the reliability demonstration test parameters must be such as to impose an environment sufficiently standard to permit direct comparison to failure rates employed in the estimate. The benefit the standard test environment provides to estimate verification, plus the benefit of standard test environment to acquiring a fund of useful reliability demonstration testing experience, makes it very beneficial to select standard test environments for reliability demonstration testing. Now since expected field use environments will not likely duplicate the standard test environments, it is usual to select a standard combination of test environments next more severe than the expected use environment. Since MTBF is a variable dependent among other things on operating environment, it becomes desirable once a standard test environment is chosen, to specify the appropriate MTBF requirement for the standard test environment. Then requirement compliance is determined on the basis of the standard reliability demonstration test with the specified standard environment, and not on the basis of field use. The added benefit of verification of reliability estimate then is achieved at no additional effort.

With the bulk of avionic reliability demonstration testing requiring standard test and standard environment, tests have been devised that have maximum efficiency, if at the expense of slightly greater administrative complexity. Test experience with standard tests builds up quickly and slightly more administrative complexity is no handicap because of the rapid acquisition of experience and familiarity. Furthermore, total understanding of the risks and probabilities associated with the standard tests is available. In the U.S.A. practically all reliability demonstration testing for military avionics is in accordance with MIL-STD-781¹



which for most test plans employs a sequential probability ratio test for which exact statistical calculations have been made and are available.^{1,2} Thus, the probability of all possible outcomes for every MTBF is known continuously throughout the test.

MTBF CHANGE

While variation of MTBF with total environment and with operating mode for a given avionic design has already been discussed, MTBF can change during the life of a particular unit of avionic equipment, and for a fixed or constant design, MTBF can change during the life of the production program. Such capability of change establishes a risk that a given design may change sufficiently between reliability demonstration test and field use so that a flunked test might be followed by satisfactory field experience later on, or conversely, a favorable test outcome might be followed by later deficiency. Examination of these MTBF changes will provide sufficient protection to allay concern.

Very frequently inspection processes and manufacturing techniques are such that avionic piece parts have latent defects. The deficiencies are infrequent, and difficult to screen out by customary inspection processes. Their presence in the manufactured product raises the failure rate sufficiently so that initial

MTBF is importantly less than the MTBF observed after a small amount of operating time has accrued and the early deficiencies remedied. Experience with relatively simple avionic communications equipment several years ago indicated that in nearly every case all latent defects had been identified and MTBF had reached its expected value after no more than twenty-five hours of operation of each unit. Because these equipments were being manufactured in large quantity, it was possible to gain enough data to recognize the brevity (25 hours) of this early failure period. It has been claimed that relatively complex avionic equipment has taken as long as one hundred hours of operation to reach its normal MTBF, even after optimizing inspection and manufacturing techniques. On the other hand, it was possible in still another avionic program by tightening inspection techniques to reduce the time for latent defect identification to the one or two hours of operation routinely needed for tune up and check-out of the equipment on the production line, thus eliminating any need for special effort to avoid latent defects. Many manufacturing programs have a burn-in requirement specified which forces anywhere from ten hours to 200 hours operation before acceptance test. Some programs require that the last few (specified) hours of burn-in be failure free.

There has been much talk over the years about equipment wear-out. Implied is a defined operating life after which the equipment is presumed to have such reduced reliability (or increased failure frequency) as to no longer be serviceable. In actual practice, and with avionic equipment, design obsolescence usually occurs before such a wear-out condition can be detected. Those equipment designs so complicated as to encounter frequent failure and repair, often reach an unrepairable condition caused by degradation from many repairs, and this condition occurs before any otherwise identifiable wear-out. Specific items in an equipment design can actually wear-out but as they are known it is usual to replace these items. In this category are cathode ray tubes, magnetrons, bearings, etc.

Development programs often have MTBF (or reliability) growth during the course of development, and even during the course of one or several reprocurments following a presumably complete and adequate development. A relatively common reason for reliability growth is related to the "fail and fix" sequence wherein nearly every failure is sufficiently analyzed to permit some probability of design adjustment to forever preclude possibility of a repeat of this failure. Note that this statement says "some probability," and even a very low probability, if regular, will produce a noticeable effect (reduction) on failure rate quite quickly. If one is disposed to presume that every failure encountered will be so thoroughly analyzed as to permit perfect fix and total elimination of repeats, this difficult and unlikely process must be continued until a large fraction of all failure modes of all failing items have been encountered and remedied if this process is to greatly raise reliability without basic redesign. Thus growth will be frequently noticed but should not significantly be counted upon by this process.

Sometimes equipment is found to have negative growth. Investigation often uncovers relaxation of piece part procurement requirements, relaxation of inspection, abridgement of acceptance tests, poor handling practices, etc. When negative growth is noticed principally in field use, it has been found that field procurement of repair parts and assemblies is not to as rigorous standards as initial procurement, and sometimes field repair manuals are deficient in information provided.

Question is sometimes raised as to the reliability variation from unit to unit in a homogeneous production lot of equipment. If the overall MTBF is heavily dependent upon the particular failure rate of one or two high failure rate items or parts, then unit to unit variation can be as much as part to part variation. Since such situations automatically point to the bad acting parts, they are quickly remedied. In the typically complex equipment, if any one production unit stands out with an MTBF differing by more than ten percent, it can be traced, if with diligence, to unique factors in the fabrication or manufacturing process. Years ago it was customary to always run reliability demonstration tests on more than one equipment simultaneously to guard against the misfortune of testing a single unit which would later be found to be a "lemon." The plurality of units under test permitted comparison of the failure frequency of one unit with that of the other(s). It is this author's opinion that experience has shown so small a likelihood of any significant difference as to justify reliability demonstration tests of a single equipment whenever a desire for reducing overall test time does not justify test of more than one equipment.

TEST PARAMETERS FOR CHOICE

Establishing a reliability demonstration test necessitates decision making in several categories. While not all of the following categories need receive detailed attention, a comprehensive list would look something like the following:

- Total Test Environment
- Test Plan
- Sample Size
- Performance Parameters for Measurement and Frequency
- Failure Definitions and Counting Relevant Failures
- Allowable Preventive Maintenance
- Detailed Test Procedure and Test Report Requirements
- Acceptable Basis for Repeating Test

Several of the above have been chosen as topics for the following paragraphs.

TOTAL TEST ENVIRONMENT

The total test environment must be considered to include not only limiting extremes of temperature, altitude, vibration, and source power (voltage and frequency extremes), but must also include appropriate cyclic variations of these environmental parameters, and cyclic operation between equipment power-on and power-off. Usually simple cycling between specified extremes at a specified frequency is sufficient. However, with simple cycling the cyclic waveform may not necessarily be allowed to assume its most convenient shape. Expediency often dictates that temperature cycling needs be hastened by specifying a minimum rate of temperature change for the test chamber. Fortunately standard test documents such as MIL-STD-781 spell out a number of different environmental test levels in considerable detail, and the benefits of standardization already mentioned motivate most programs to follow the standard test closely.

Limiting criteria used for selecting a standard environmental test level are important, and ideally might consist of the following:

Environmental severity equal to or slightly in excess of the environmental severity expected by the equipment when in field use.

Environmental severity equal to or slightly less than limits specified for the parts from which the equipment will be fabricated.

Sufficient environmental severity to maximize the likelihood of uncovering defective parts and workmanship.

Environmental severity less than that level which will cause significant number of failures from non-relevant failure modes.

Some years ago the rigors of environmental extremes were so feared by equipment designers that many reliability demonstration tests were carried on at laboratory ambient environment because the next more severe standard environment was felt to disastrously exceed the expected field conditions. Conversely today several electronic equipment designers feel that routine equipment can readily be designed to perform as well under a cycling environment varying between -54°C and $+71^{\circ}\text{C}$, with vibration thrown in for good measure, as under laboratory ambient conditions, and at no extra cost or other penalty. There can be no question that equipment satisfactorily passing reliability demonstration test under such a standard extreme environment is unquestionably sturdier than its predecessors.

One is tempted sometimes to overlook the actual temperature extremes that avionic equipment actually encounters in the field. Sealed up equipment resting in the sun in the tropics, even though with power off, can reach very high temperature. The actual thermal transient condition it then goes through when first energized is dependent upon many hard-to-measure factors. The standard environmental level spelled out for standardized testing which is somewhat more severe is often a safer course to follow to establish design adequacy than detailed thermal calculations dependent upon many parameters and some difficult assumptions.

In order to effect appropriate thermal standardization for standardized reliability demonstration testing, it is customary to require an experimental thermal survey of the equipment to be tested such that the equipment's point of greatest internal thermal inertia is located, and thermal cycling is then specified in terms of temperature cycling of this point. The thermal survey required is a very illuminating experience for many designs because it illustrates how long it takes to change the temperature of interior portions of equipment.

Some years ago a reliability field evaluation team found that certain avionic equipment was displaying considerably lower reliability in field use than test results would support. Ultimately the difficulty was tracked down to the on-off cycling the equipment got in aviation service where flight times were short but flights were many. As designed, this avionic equipment would have demonstrated a far better failure history were it to have maintained power on between flights, which tactically was out of the question. The long term result was that avionic designers learned how to design for on-off cycling and the thermal and mechanical cycling it induced. Today, reliability deficiency because of on-off cycling is likely to be considered design error.

Not too long ago hermetic sealing had not reached the perfection of today. At that time thermal and altitude cycling could cause an imperfectly sealed unit to breathe. Then ambient humidity would cause moisture ingestion and later difficulty. Today the importance of sealing and attendant skill has grown for a myriad of reasons and hermetic seals seldom give trouble when fabricated by sound manufacturing methods.

For the designer who lacks experience in facing up to the more difficult environmental extremes of the standardized reliability demonstration test, the design process will be beset with many difficulties. But the quicker he surmounts all the difficulties and learns the technique, the more successful his designs will be.

TEST PLAN SELECTION

Reliability testing is based on the observation over a known period of operating time of a counted number of relevant failures (the failed equipment under test being returned to proper performing condition immediately on the occasion of failure so that it can continue test). The assumption is then made that the average rate of failure observed during test is indicative of this equipment's average rate of failure to be encountered in the future if operated in similar manner under similar conditions. It is customary with complex avionics to assume that reliability is exponentially distributed which is synonymous with assuming the mean-time-between-failures to be constant and independent of the avionic's age. It is also customary to assume that the MTBF demonstrated by an equipment to be tested will be the same as the MTBF for every other equipment of identical design and manufacture operated in the same manner under the same conditions, and to assume MTBF is independent of equipment age. History has shown such assumptions to be quite practical in nearly all instances.

Prearranged rules for acceptability are established with statistical care to predetermine the number of relevant failures to be allowed per defined operating interval for these reliability demonstration tests. Accordingly, for any set of such rules that defines acceptance (and defines rejection) an operating characteristic is automatically defined relating probability of acceptance to true MTBF. Because decisions can only be made on the basis of mean (average) time between failures, it takes many observed failures (e.g. a long test) to closely discriminate between an acceptable MTBF and an unacceptable MTBF if these two MTBF values are close together. Such characteristics are inherent in all statistical sampling tests. In practice, it is common to define an acceptable MTBF as θ_0 and assign a probability of test acceptance to θ_0 of something slightly less than certainty, say 0.90, in which case there is a risk α of 0.10 that an equipment with MTBF exactly equal to θ_0 would not be accepted (would be rejected). The test operating characteristic will tell us that a true MTBF of specific value and much higher than θ_0 will have a specific and much greater

probability of acceptance (typically 0.99 or 0.999 with corresponding lower α risks of 0.01 or 0.001). Alpha is identified as the producer's risk of failing to accept an acceptable unit.

At the lower end of the test's operating characteristic a second MTBF is identified as θ_1 and we choose θ_1 , the probability of acceptance, low, say 0.10 so that we may say the user's risk β of accepting an unacceptable MTBF (θ_1) is 0.10. Test plans are predesigned to provide θ_0/θ_1 , the discrimination ratio, with values such as 1.5, 2, 3, 5, etc., and risks are usually chosen so that $\alpha = \beta = 0.10$ or $\alpha = \beta = 0.20$, but α need not be identical to β .

The philosophy for selecting a test plan on the basis of MTBF requirements varies. If a large production quantity of equipment will be required and the test will be repeated many times during the production run, then a manufacturer could hardly tolerate having his product, were it to have a true MTBF of θ_0 , to have a 0.10 risk of flunking the test, especially if production deliveries were jeopardized following a test rejection. Hence he would bend every effort to deliver equipment with an MTBF equal to something better than θ_0 .

On the other hand, if the manufacturer had only a small order, was newly developing the avionics, and lacked experience to know just how low the MTBF might turn out, then the user perhaps should be capable of tolerating an MTBF as low as θ_1 . To provide a test with $\theta_0/\theta_1 = 1.5$ requires three times as much testing as if $\theta_0/\theta_1 = 2$ and twenty-five times as much testing as when $\theta_0/\theta_1 = 5$.

For these reasons the following factors are often judged relevant in deciding on a test plan and the magnitude of testing it imposes on a development program:

- Importance of Reliability to Equipment Use
- Funding Available to Development Program
- Procurement Schedule
- Availability of Test Facilities

For a production program, the program magnitude and prior experience are the principal factors in judging the hazard in ignoring θ_1 and concentrating only on θ_0 and a short test.

PERFORMANCE PARAMETERS FOR MEASUREMENT

A reliability demonstration test can be conducted on a single avionic equipment or on several simultaneously, and since the duration of test is measured in total equipment operating hours (or total relevant failures) doubling the number of equipments on test will double the operating hours, the relevant failures, and halve the time it takes to gain test acceptance or rejection. The practical limitation is the space available in the test chamber (or number of chambers) for simultaneously testing several equipments, or sometimes more limiting, the magnitude of test equipment on hand to permit rapid but comprehensive measurement of satisfactory performance.

To reach a decision on just what performance parameters to measure (and the frequency of measurement) in order to quickly recognize the occasion of a failure during the test, several factors must be considered. First, the test procedure must be sufficiently comprehensive to identify all the principal modes of relevant failure. If such a procedure is impossibly long and therefore cumbersome to repeat frequently, a streamlined procedure must be developed to quickly identify the more prevalent modes of failure so that this shorter procedure can be cycled more frequently, with the longer procedure less frequently.

On the occasion of identified relevant failure, it is customary to count as valid operating time only that operating time up to the moment when last that (now failing) performance element was tested and found satisfactory. This penalty on the less frequently measured performance modes (less valid operating time allowed on the occasion of failure) is offset by the lower likelihood of these modes of failure.

Because with temperature cycling it is difficult to make the equipment linger at the lowest temperature once its power is applied, fast performance verification routines should be developed for as much of the performance as possible for the low temperature performance measurement. Much more time can be taken for measurement at high temperature since operation is stabilized here for a reasonable interval.

Automatic performance testing via built-in-test (BIT) circuitry can be an asset to reliability demonstration test, but it is necessary to have prior agreement as to whether failure of the BIT is easily determinable, will not abridge veracity of test, and is to be counted against allowable relevant failures (it usually is).

With the prevalency of temperature cycling during reliability demonstration test, it becomes necessary to satisfactorily perform needed testing on equipment within a test chamber by remote-control from outside the chamber. When such is not possible, considerably more planning and analyses of consequences are advisable.

RELEVANT FAILURES

Common sorting of failures into relevant and non-relevant categories usually places failures induced by circumstances foreign to proper equipment use and failures that occur secondarily as the result of a separate inducing relevant failure in the non-relevant category. However, experience has shown that other ground rules are important also:

- (a) Failure can only occur following proper operation; otherwise there is strong likelihood of material discrepancy rather than failure.
- (b) An equipment's performance failure must be counted as a relevant failure even though no out-of-specification elemental portion of the equipment can be identified in order to permit replacement or repair.

- (c) Out-of-specification conditions must be identified in every item to be replaced or repaired during the course of the reliability demonstration test. Specific policy is needed on the acceptable magnitude of readjustment of adjustable features without counting a relevant failure.
- (d) Secondary failure and non-relevancy cannot be claimed because of simultaneous occurrence of plural failures unless a primary-secondary relationship can be unquestionably established. Hence simultaneous (plural) failure recognition will often result in plural relevant failure counts.
- (e) Design changes cannot be made at the time of repair unless mutually acceptable and applied to all production. Otherwise repair is limited to returning equipment to pretest condition.
- (f) Activity logs kept in detail to record performance measurements made during test must be sufficiently detailed to permit reconstructing exact sequences of events in case of dispute.
- (g) Agreement must be reached on kind and frequency of preventive maintenance to be allowed during test.

READYING FOR RELIABILITY TEST

The need for a thermal survey of the equipment to be tested to permit developing a thermal profile for control of the test chamber has been often mentioned. The need to identify the point of greatest thermal inertia within the equipment often means that one unit of equipment, the unit for the thermal survey test, must be fabricated with thermocouples already installed. The most convincing means to identify the point of greatest thermal inertia is to have ten or twenty thermocouples fabricated into all likely locations and then choose by recording all thermocouple temperatures repeatedly on a fast cycle during chamber thermal excursion. The essential outcome is the thermal relationship between chamber air and that of the point of greatest thermal inertia. Remember that the greater the thermal inertia, the lower the chamber cyclic frequency and the fewer cycles during the reliability demonstration test. (The test length is not related to thermal cycle count but rather to operating time and failures encountered.)

It is strongly recommended that development testing always be conducted which will include performance experience with such chamber environments as are later needed by the reliability demonstration test. This may be the only way to provide insight into any environmental difficulties sure to follow. This development testing if carried to the extreme should give a very accurate indication of what to expect from the reliability demonstration test, especially if the former can qualify as a careful dress rehearsal of the latter. Remember if such exploratory testing is conducted on development hardware not destined for the later official test, there can be no injunction limiting the testing activity. Special tests, dry runs, etc., made with the equipment assigned to the formal reliability demonstration test may be classified as part of the formal test (as burn-in or the like) and be required of all production prior to acceptance.

RETEST RULES

Personnel in charge of reliability testing sometimes are not aware of the stringent rules that must apply to a test whose outcome is based on statistical data. As long as there is any probability of a faulty decision (i.e., accept bad equipment, reject good equipment), the faulty decision (if desired) can be reached by sufficient repetition of the test. Practically speaking, the test's operating characteristic which relates probability of acceptance to MTBF will change (for a given MTBF, P will rise) if two trials are allowed, thus reducing confidence in the acceptability of the equipment which passes the test.

To get around this statistical ban on retest, it is customary, following test conclusion with adverse decision, to require such design change (for MTBF improvement) as will establish a basis for claiming the next test (retest) is a test of a different design. Reasonable and unbiased judgment that the extent of design change is bound to produce at least significant (if not completely sufficient) improvement in MTBF is the customary basis for agreement on retest. A complete reliability demonstration test with decision, conducted as a dress rehearsal on different hardware and preliminary to the formal reliability demonstration test, does not create a problem of retest, since the outcome of the dress rehearsal has no effect whatever on the statistical decision that results from the formal test which will be conducted regardless of dress rehearsal outcome.

RELIABILITY GROWTH

Occasionally one can encounter a development program beset with difficulties and no forethought or preparation for the formal reliability demonstration test required by contract. Undoubtedly some find it tempting to put "first things first" and defer concern over reliability until after other performance requirements are met. Then as much attention as possible in the time remaining will be given to reliability and if a deficiency remains, "reliability growth" will in time solve this problem. Closer scrutiny of such philosophy often uncovers the mistaken conviction that reliability (MTBF) will continue to improve indefinitely so long as failures are always intelligently remedied. A number of case histories were collected and studied and growth, decay, and cyclic change of reliability could all be illustrated repeatedly among the cases studied. [The change in reliability here considered is apart from the initial short term improvement which results after elimination of early failures.] With this in mind, it is believed pointless to repeat adverse outcome reliability tests without basic design improvement.

Some concern has been shown that an equipment undergoing reliability demonstration test without sufficient burn-in to eliminate early failures may luckily avoid rejection from too many early failures and then use the extended duration of test to progress from low initial reliability to acceptable reliability and a test acceptance decision. Under such circumstances the need for burn-in by all the remaining untested equipment in the production lot would go unrecognized, and many needless early failures would be suffered in field use. This condition, when suspected, can be avoided by significant shortening of test by placing many more equipments simultaneously on test. Then the presence of early failures will have much greater probability of producing a reject decision, and the foreshortened test duration will likely fall short of providing the needed burn-in for an accept decision.

Continuous logging of all equipment operating time and equipment failures experienced during development can provide amazingly good early indication of development progress in reliability and of future

difficulty while there is time and much better chance for remedy. This kind of continuous scrutiny is mightily encouraged, with concurrent attempt at all conceivable correlation.

CONCLUSION

Testing is often considered as a sometimes necessary evil, for it can only serve to provide operational insight which should already be known by theory and design, or to provide assurance of design adequacy, and as insurance the premium is so high that there must be more cost effective insurance methods. This author believes reliability demonstration testing is only justified during this technological era when imperfect design capability can find so large a market-place. The experience gained through extensive reliability testing has already in many cases led to claims of design capability more than adequate for quite difficult test environments, and to clear recognition of the location of pertinent state-of-the-art, with ready definition of the level of reliability offered.

REFERENCES

1. MIL-STD-781B "Military Standard Reliability Tests: Exponential Distribution," U. S. Government Printing Office, 15 November 1967.
2. Epstein, B., Patterson, A. A., and Qualls, C. R., "The Exact Analysis of Sequential Life Tests with Particular Application to AGREE Plans," Proceedings of Aerospace Reliability & Maintainability Conference (AIAA), Washington, D.C., May 6-8, 1963.

LA TECHNIQUE DES ESSAIS ACCELERES

par

P. Blanquart

L'Ingénieur en Chef des Télécommunications
Adjoint au Directeur Régional chargé du
Centre National d'Etudes des
Télécommunications de LANNION

1 - INTRODUCTION. DEFINITION ET NECESSITE DES ESSAIS ACCELERES

Bien que la technique des essais accélérés puisse s'appliquer à n'importe quel dispositif dont on cherche à déterminer la fiabilité (composant, sous-ensemble, équipement complet) nous nous appuierons dans cet exposé sur des exemples concernant des essais de composants électroniques. Nous verrons d'ailleurs que cette technique est surtout intéressante pour les composants.

Les essais accélérés sont des essais au cours desquels le niveau des contraintes appliquées est choisi au-delà du niveau rencontré au cours de l'utilisation courante en vue de diminuer le temps nécessaire pour observer les dégradations.

Pourquoi fait-on des essais accélérés ?

Nous allons énumérer tout à l'heure les nombreuses difficultés auxquelles on se heurte lorsque l'on entreprend de tels essais et les précautions délicates dont on doit s'entourer pour pouvoir extrapoler des résultats obtenus avec des conditions de fonctionnement très éloignées des conditions normales d'emploi. Pourquoi ne pourrait-on pas se contenter des essais non accélérés où ce risque d'erreur d'extrapolation est certainement minimisé ?

Les réponses à ces questions sont simples :

- Les essais non accélérés, c'est-à-dire les essais au cours desquels les pièces étudiées fonctionnent dans les conditions normales d'emploi sont coûteux et d'autant plus coûteux que la fiabilité de ces pièces est bonne.

Par exemple, pour annoncer un taux de défaillance de 10^{-8} par heure x pièce avec 10 chances sur 100 seulement de se tromper, il faut accumuler $2,3 \cdot 10^8$ pièces x heures et ne tolérer aucun défaut (soit 23 000 pièces pendant plus d'un an). Le nombre de composants à essayer, l'immobilisation de baies de durée, le nombre de mesures à faire rendent donc de tels essais très onéreux au-delà d'un certain niveau de fiabilité. La durée elle-même de ces essais leur enlève une bonne partie de leur intérêt. En pratique, les essais non accélérés sont très rares.

- La possibilité d'accélérer la vitesse de dégradation des composants étant admise - nous reviendrons sur cette question importante - il est justement intéressant de déterminer expérimentalement les lois d'accélération par des essais accélérés.

C'est en particulier le cas lorsque l'on recherche des renseignements statistiques sur les dérives de caractéristiques : on sait en effet que si la fabrication que l'on veut juger est homogène, des échantillons de petite taille suffisent ce qui ne justifierait pas ici la technique des essais accélérés. Celle-ci se justifie uniquement parce que l'on désire mettre en évidence l'influence des contraintes sur les dérives.

2 - HYPOTHESES DE BASE

- 2-1. Enumérons maintenant les hypothèses de bases qui complètent la définition et sur lesquels repose la validité des essais accélérés.

Remarquons d'abord que la définition suppose implicitement qu'il existe effectivement des lois physiques reliant les mécanismes de dégradation des composants à certains facteurs qui sont appelés des contraintes. Nous reviendrons plus loin sur ce point mais nous savons que l'on peut en effet exprimer un paramètre s représentant l'état interne d'un composant en fonction d'un certain nombre de paramètres (temps t , température T , tension u , courant I puissance dissipée P)

$$s : f(t, u, P, I, T)$$

Dans les formules ainsi obtenues, le temps est un facteur d'influence comme les autres contraintes et la technique des essais accélérés revient à modifier l'un de ces facteurs afin d'augmenter la dégradation ou encore afin d'obtenir la même dégradation tout en donnant au facteur temps une valeur plus faible.

Le paramètre s peut être une composition chimique d'une partie active d'un composant (oxydation d'une résistance, concentration d'impuretés dans un semiconducteur) ou une dimension mécanique d'une partie active (épaisseur de métallisation).

Ce paramètre s est ainsi lié soit à une caractéristique électrique (résistance électrique d'un matériau) - et sa variation en fonction du temps se traduira par une dérive -, soit à une fonction électrique simple comme par exemple l'isolation ou la continuité électrique. Dans ce dernier cas la dégradation de ce paramètre aboutit à une défaillance catalectique (l'épaisseur d'une métallisation peut diminuer jusqu'à la coupure).

Dans le cas d'une défaillance catalectique, on a l'habitude d'incorporer le paramètre "temps" dans un paramètre de fiabilité (durée de vie moyenne, taux de défaillance) qui devient alors fonction des contraintes.

Ainsi, nous venons de le voir, la validité des essais accélérés repose d'abord sur le fait que le temps intervient dans le phénomène de dégradation et qu'il est lié aux autres contraintes. Nous donnerons tout à l'heure des exemples.

Les autres hypothèses sont les suivantes :

- Les modes de défaillance obtenus par les essais accélérés doivent être les mêmes que ceux qui peuvent exister dans les conditions d'utilisation.
 - Les modes de défaillance observés doivent être le résultat de la contrainte choisie.
 - Les résultats obtenus à partir des lots donnés doivent pouvoir être extrapolés aux composants de la même fabrication (un changement minime de technologie pouvant fausser entièrement les résultats).
 - Les lots essayés sont homogènes et leur fractionnement en échantillons d'essais de taille plus petite et réputés identiques est possible.
- 2-2. La définition des essais accélérés étant ainsi rappelée, essayons de délimiter le domaine des essais accélérés. Nous constatons qu'elle ne s'applique pas aux exemples suivants :
- L'"usure" d'un contact de relais pouvant être reliée au nombre de battements du contact il est facile d'"accélérer" la dégradation en augmentant la cadence des battements. Par exemple, on pourra essayer en 3 mois un relais conçu pour résister à 100 millions de battements en le faisant battre 10 fois par seconde ce qui peut correspondre à 20 ans d'exploitation normale.

La technique est ici différente car on n'a pas modifié les autres facteurs de dégradation ni même le facteur "temps", puisque celui-ci n'intervient ici que par l'intermédiaire du nombre de battements.

- Toutes les spécifications de composants comprennent des essais d'endurance qui sont un peu des essais accélérés mais on ne cherche pas alors à déterminer une loi d'accélération : on souhaite seulement comparer des lots de pièces entre eux.
- Le temps doit intervenir dans la loi qui détermine la dégradation : cette remarque peut paraître évidente mais la réalité des expériences dissimule souvent ce fait.

Il est certain que des essais de rupture sur des pièces mécaniques permettent de comparer la résistance de plusieurs échantillons entre eux mais ne nous donne en aucune façon la durée de vie utile de ces pièces puisque le temps n'intervient pas ici.

Il peut arriver que des essais accélérés effectués sur des composants électroniques conduisent à de tels phénomènes sans qu'on s'en aperçoive : c'est en particulier le cas des mécanismes à "seuil" sur lesquels nous reviendrons. Il est évident par exemple que des essais sur des composants à semiconducteurs qui seraient effectués à une température supérieure à la température de fusion de l'eutectique or-silicium employé pour braser la pastille, conduiraient à des résultats aberrants.

- Enfin, nous rappelons que nous nous occupons ici de dégradations, c'est-à-dire de phénomènes irréversibles et non simplement d'effets réversibles que l'on appelle coefficients lorsqu'ils sont linéaires (coefficient de température, de tension ...)

3 - LES LOIS D'ACCELERATION

Pour prouver la validité de la technique des essais accélérés, nous allons donner quelques exemples de lois reliant les caractéristiques de fiabilité à des contraintes.

- La contrainte la plus fréquente est la température. On sait en effet que la température modifie la vitesse des réactions chimiques selon une loi exponentielle.

La loi souvent appelée loi d'Arrhénius s'écrit

$$\frac{ds}{dt} = A e^{-\frac{B}{T}} \quad \text{ou} \quad A e^{-\frac{U}{KT}}$$

Elle relie un paramètre interne s , le temps t , la température absolue T . B ou U sont des paramètres : B s'exprime en degrés alors que U appelé énergie d'activation de la réaction s'exprime en volt.

On a trouvé expérimentalement par exemple que le coefficient B intervenant dans la dérive de résistances à couche de carbone était de 6000° K à 10 000° K selon les types.

- Les métallisations en aluminium assurant les interconnexions internes des composants à semiconducteurs ont une durée de vie limitée par le phénomène d'électromigration d'aluminium dès que la densité de courant qui les parcourt est grande. Rappelons qu'il s'agit de conducteurs en aluminium ayant une épaisseur de l'ordre du micron, une largeur d'une dizaine de microns et que les densités de courant y atteignent des valeurs considérables de l'ordre de 10^5 A/cm². A ce régime il y a transport d'aluminium -jusqu'à la coupure d'une zone désertée- comme l'ont montré de nombreuses études. En particulier J.R. BLACK a déterminé la loi reliant la durée de vie moyenne t_0 d'une métallisation, sa section S, la densité de courant J, la température absolue T

$$\frac{1}{t_0} = A S J^2 e^{-\frac{U}{KT}}$$

Nous avons ici un exemple d'une loi faisant intervenir deux contraintes, courant et température et le temps.

On peut donc à volonté obtenir les mêmes effets en jouant sur l'intensité de courant ou sur la température.

Les valeurs des coefficients dépendent de la structure de l'aluminium, U valant de 0,6 v à 1,2 v selon les cas.

4 - LES ESSAIS ACCELERES CLASSIQUES

On porte différents lots de composants à des températures différentes T₁, T₂, ... T_n pour une durée de quelques milliers d'heures et on effectue les mesures à différents intervalles de temps (les mesures sont faites toujours dans les mêmes conditions à température ambiante et si possible stabilisée).

L'exploitation se fait de deux façons selon que l'on s'intéresse aux défaillances catalectiques ou aux dérives :

4-1. Cas où une seule contrainte est appliquée

4-1-1. Cas des défaillances catalectiques

On compte après chaque mesure le nombre N(t) de pièces encore en vie (d'après le critère de défaillance adopté) et pour chaque lot essayé c'est-à-dire pour chaque niveau de contrainte (pour exemple la température T₁ ou T₂ ...). Si N₀ est le nombre initial de pièces (pour un lot à une contrainte), on sait que le rapport $\frac{N(t)}{N_0}$ est un estimateur de la fiabilité du lot.

Si l'on observe - ΔN défaillances pendant l'intervalle de temps Δt, on sait qu'un estimateur du taux de défaillance λ est donné par

$$\lambda = \frac{-\Delta N}{N(t) \cdot \Delta t}$$

On sait également qu'il convient d'encadrer ce nombre d'un intervalle de confiance qui est complètement déterminé par le nombre de défaillances : l'intervalle de confiance est grand lorsque le nombre de défaillances observées est faible.

Par exemple, on a observé 4 défaillances sur un lot de 1000 pièces au bout de 1000 heures. En se reportant aux tables appropriées (non reproduites ici), on peut annoncer qu'il y a 90 chances sur cent pour que le taux de défaillance réel du lot soit compris entre $1,4 \cdot 10^{-6}$ par pièce-heure et $9,2 \cdot 10^{-6}$ par pièce-heure, le taux observé étant de $4 \cdot 10^{-6}$ par pièce-heure.

On dispose alors à la fin de l'expérience d'un ensemble de courbes expérimentales donnant chacune la fiabilité en fonction du temps à une température donnée ou encore le taux de défaillance en fonction de la température : la figure 1 illustre cette méthode.

4-1-2. Cas des dérives

On trace l'évolution statistique de tous les paramètres intéressants d'un composant en fonction du temps et pour différentes contraintes.

On peut prendre par exemple l'évolution de la valeur d'un percentile (décile, médiane ...) ou de la valeur moyenne.

Les paramètres intéressants peuvent être soit des paramètres caractérisant la fonction du composant (capacité d'un condensateur, gain d'un transistor) ou des caractéristiques parasites d'un composant (angle de perte d'un condensateur ...). Il est certain que l'évolution de tous les éléments du schéma équivalent d'un composant seraient à considérer mais ces éléments sont liés les uns aux autres ce qui diminue

le nombre de mesures.

On cherche ensuite l'équation de ces courbes en fonction du temps à température constante d'une part puis en fonction de la température.

Enfin, la connaissance de la distribution des paramètres permet de caractériser entièrement le phénomène.

La figure 2 donne des exemples obtenus sur des résistances à couche métallique au Centre de Fiabilité en France.

On trouve ici une loi donnant la dérive de ces résistances en fonction du temps selon une loi un peu différente de la loi d'Arrhénius puisque la dérive n'est pas une fonction linéaire du temps.

$$\frac{\Delta R}{R_0} = M t^n e^{-\frac{U}{KT}}$$

Dans cette expression, n vaut environ 0,3.

De même des essais faits sur des résistances à couche de carbone par un fabricant français au cours d'un contrat d'étude de fiabilité ont donné des lois analogues variant selon les types (figure 3).

$$\frac{\Delta R}{R_0} = 1,23 t^{0,6} e^{14 - \frac{5900}{T}}$$

Remarque - Il est possible de traiter comme des défaillances catalectiques le cas des pièces dont une caractéristique a franchi une valeur déterminée. Par exemple, on considérera comme défaillant tout transistor dont le gain est devenu inférieur à 30.

On peut soit considérer des dépassements de limites fixes (exemple ci-dessus) soit considérer des dérives relatives. Par exemple, on comptera comme défaillance toute résistance dont la valeur a dérivé de plus de 10 %.

Ces deux méthodes sont également utiles car certains organes peuvent être sensibles à la valeur absolue d'un paramètre ou à une dérive relative (cas où un dispositif de réglage a permis de s'affranchir de la dispersion initiale des pièces).

4-1-3. Exemple d'un plan d'essai

Essayons de trouver le nombre minimal de condensateurs à mettre en essai pendant un an pour en déduire le taux de panne à 25° C pour une tension appliquée égale à la moitié de la tension nominale.

Nous allons bâtir un plan d'essais accélérés en faisant quelques hypothèses :

- Nous ne nous intéressons qu'à une seule fabrication
- Nous voulons étudier deux valeurs de capacité pour des condensateurs ayant la même valeur nominale (valeurs extrêmes pour un boîtier donné par exemple).
- Nous supposons qu'il peut y avoir deux mécanismes de défaillance et que le taux de défaillance est de l'ordre de 10^{-6} par pièce-heure dans les conditions les plus sévères de notre essai.

Le plan d'essai pourra se représenter par le tableau du cliché suivant sachant que les pièces seraient polarisées à la moitié de la tension nominale dans chaque cas :

Température	75° C	100° C	125° C
Nbre de pièces	N1	N2	N3

Si nous prévoyons deux mécanismes de défaillances conduisant l'un au court-circuit l'autre au circuit ouvert par exemple, il faut observer au moins deux défauts à 125° C température pour laquelle nous supposons que le taux de panne est de l'ordre de 10^{-6} par pièce-heure.

Il faut donc accumuler plus de 2×10^{-6} pièces-heures à 125° C et à fortiori encore plus dans les autres conditions ce qui conduit pour chaque valeur à essayer pendant

un an au moins 600 pièces

4-2. Cas de deux contraintes

4-2-1. Les contraintes thermique et électrique sont les contraintes le plus couramment simulées en laboratoire.

La contrainte thermique est appliquée à des niveaux différents, la contrainte électrique peut être appliquée selon diverses variantes (courant continu, courant alternatif, contrainte en courant, contrainte en tension ...) susceptibles chacune de différents niveaux.

Si on appelle T_i les niveaux de température et E_j les variantes ou niveaux de la contrainte électrique, le plan d'essai pourra être représenté par un tableau tel que celui de la figure 4 dans lequel on notera dans chaque case le nombre de pièces à essayer.

Remarque - On suppose ici que les lots répartis dans chaque case sont identiques (technologie, provenance). S'il n'en est pas ainsi, il faut dresser autant de tableaux identiques que de "variantes" : ceci peut se produire par suite de différences de technologie connues ou lorsque l'examen statistique des mesures électriques préliminaires a mis en évidence des populations distinctes.

4-2-2. Exploitation dans le cas de l'évaluation des défaillances cataclysmiques

On calcule, pour chaque couple de contrainte, le taux de défaillance pour la durée totale de l'essai, en le supposant indépendant du temps, que l'essai soit arrêté après une période fixée à l'avance (essai dit "tronqué") ou qu'il soit arrêté après un nombre de défaillances donné (essai dit "censuré").

Les intervalles de confiance déduits de ces observations peuvent être reportés sur un graphique donnant le taux de défaillance λ en fonction de la température et pour les diverses contraintes électriques (figure 4). L'exploitation ne sera possible que si les effets des divers couples de contraintes sont notablement différents.

En effet, si par exemple on considère un essai dans lequel on veut faire intervenir trois températures et trois tensions, il faudra sacrifier 9 lots de composants. Les considérations économiques conduiront alors à diminuer le plus possible le nombre de pièces dans chaque lot de sorte que la précision sur le taux de défaillance associé à chaque couple de contraintes sera médiocre. Il en résulte que seuls les effets importants pourront être détectés.

4-2-3. Exploitation dans le cas de l'étude des dérives

On construit les graphiques donnant l'évolution de chaque paramètre (par exemple en représentant les déciles, la moyenne et la dispersion) en fonction du temps comme dans le cas d'une seule contrainte, mais pour chaque couple de contraintes.

La recherche d'un modèle mathématique décrivant cette évolution est toutefois plus compliquée puisque chaque paramètre de distribution est ici fonction de trois variables (temps, température, contrainte électrique).

4-3. Remarque sur la recherche de modèles mathématiques

Pour déterminer de façon rigoureuse les relations mathématiques pouvant exister entre le taux de défaillance, le temps et les contraintes, il faut faire un calcul de régression multiple. Cette méthode n'est praticable qu'à l'aide d'un calculateur.

De même, un calcul de régression multiple est nécessaire pour trouver la loi reliant les paramètres de distribution des dérives au temps et aux contraintes.

5 - ESSAIS EN CONTRAINTES ECHELONNEES

Une grosse difficulté de la méthode précédente vient du choix arbitraire des sévérités des contraintes. Si elles sont peu sévères, le temps d'apparition des dégradations est trop long et si elles sont trop sévères, elles peuvent entraîner des mécanismes de défaillance très différents de ceux rencontrés en utilisation.

La méthode des contraintes échelonnées permet de s'affranchir en partie de cet inconvénient.

Dans un essai en contraintes échelonnées, on soumet successivement pendant des périodes d'égale durée un même échantillon à des contraintes de plus en plus grandes. On recommence avec un autre échantillon en changeant la durée.

On détermine alors pour chaque durée choisie la contrainte à laquelle un pourcentage donné de l'échantillon est dégradé : on trouve par exemple que pour une durée de 4 heures, c'est à partir de 175° C que 10 % des pièces ont des dérives supérieures à 5 % et que

le même résultat s'obtient pour une durée de 20 heures à 125° C et pour une durée de 100 heures à 100° C.

Les couples durée-température donnant la même dégradation des échantillons permettent de connaître la loi d'équivalence entre temps et contraintes (ici la température).

Si on suppose que le mécanisme de dégradation suit une loi d'Arrhénius, 3 couples de valeurs durée-température suffisent pour déterminer les coefficients de cette loi (figure 5). On utilise à cet effet un graphique où l'on porte le logarithme du temps en abscisse et $\frac{1}{T}$ en ordonnée : une loi d'Arrhénius est représentée par une droite dans un tel graphique.

On utilise couramment des temps de 4 heures, 20 heures et une centaine d'heures.

On doit corriger les valeurs des couples durée-température observées expérimentalement avant de tracer la droite de prédiction. En effet, si on observe par exemple une dégradation donnée pour le niveau de contrainte de 125° C ce n'est pas le seul séjour à 125° C qui est responsable de la dégradation : celle-ci est en effet due en partie aux séjours précédents.

Dans le cas du modèle d'Arrhénius, cette correction est relativement simple à calculer et donne, par exemple, pour la correction du terme donnant la durée t du palier

Durée corrigée

$$t_i = \tau_i \frac{1 - e^{-n u m}}{1 - e^{-u m}}$$

où les lettres ont la signification suivante :

t_i	durée corrigée du palier (i) de contrainte
τ_i	durée observée du palier (i) de contrainte
n	nombre de paliers
u	énergie d'activation de la réaction
m	$\frac{1}{T_i} - \frac{1}{T_{i-1}}$
T_i	température (absolue) du palier i

L'avantage des essais en contraintes échelonnées par rapport aux essais accélérés ordinaires provient du fait que le choix des niveaux de contraintes y est moins arbitraire et que l'on risque moins de laisser échapper les niveaux de contraintes utiles ou de choisir des contraintes exagérées.

Les figures 5 et 6 qui ont servi d'exemple montrent les résultats obtenus sur des transistors destinés à équiper des répéteurs téléphoniques enterrés à 2700 voies : la durée de vie moyenne donnée ne concerne évidemment que le mécanisme de défaillance observé ici c'est-à-dire l'électromigration d'aluminium. Cette étude a pu montrer que dans les conditions de fonctionnement ce défaut ne devrait pas apparaître de façon systématique sur les répéteurs en service.

6 - LES DIFFICULTES RENCONTREES ET LEURS REMEDES

6-1. Nous allons d'abord énumérer quelques difficultés qui mettent effectivement en cause le principe des essais accélérés puis nous rappellerons les autres difficultés que l'on rencontre aussi dans tous les essais de fiabilité.

- Les lots d'essais doivent être homogènes

Nous l'avons vu, les résultats d'un essai accéléré ne sont exploitables que si les différents lots soumis à chaque niveau de contrainte sont identiques : en effet, dans les mécanismes de dégradation seules les contraintes doivent varier d'un lot à l'autre, les coefficients des lois d'accélération étant supposés identiques.

On vérifie l'homogénéité des lots de livraison en étudiant la distribution des paramètres électriques (on tracera les droites de HENRY) et en faisant l'analyse physique de quelques pièces.

Chaque fois que des lots distincts seront mis en évidence, on fera une répartition proportionnelle à l'importance des lots élémentaires pour chaque niveau de contrainte, ce qui revient en fait à effectuer autant d'essais que de lots élémentaires.

- La contrainte choisie ne doit accélérer qu'un seul mécanisme de dégradation

La technique des essais accélérés repose sur l'existence d'une loi reliant une ou plusieurs contraintes, le temps et la dégradation d'une caractéristique interne du composant. Si plusieurs mécanismes de dégradation existent, l'extrapolation pour un niveau de contrainte différent pourra être erronée : si les lois d'accélération de chaque mécanisme sont voisines, il en résultera seulement une assez grande marge d'incertitude sur les chiffres annoncés. Par contre, s'il existe deux lois très différentes, l'une pourra être prépondérante pour les forts niveaux de contrainte et l'autre pour les faibles niveaux. On conçoit que dans ce cas l'extrapolation vers les conditions normales de fonctionnement (niveaux faibles) d'après des résultats obtenus pour les niveaux forts soit complètement erronée. La figure 7 illustre l'erreur grossière que l'on fait ainsi sur l'estimation d'une durée de vie moyenne.

Peut-on éviter les inconvénients de la multiplicité des mécanismes de dégradation ? On peut effectivement s'affranchir - en partie - de ces inconvénients grâce à l'analyse des défaillances. En effet l'analyse électrique et physique des défaillances permettent de séparer les différentes défaillances et leurs mécanismes. On traite alors séparément chaque mécanisme de dégradation à condition toutefois de disposer d'un nombre suffisant de pièces défectueuses. Il suffit alors d'ajouter les effets de chacun des mécanismes pour les conditions de fonctionnement souhaitées.

Les figures 8, 9 et 10 illustrent l'intérêt fondamental de l'analyse des défaillances pour les essais accélérés.

Malheureusement, ce procédé ne réussit que si l'on a effectivement fait apparaître les défaillances qui se produiront dans le cas des conditions normales : l'analyse des défaillances n'apporte aucun remède dans le cas de la figure 7, c'est-à-dire dans le cas où une loi de dégradation est très différente des autres et où le défaut intéressant n'est pas apparu.

- Le niveau de contrainte choisi ne doit pas entraîner de mécanisme de dégradation à seuil

Dans le cas d'un mécanisme à seuil, le temps n'intervient pas en fait, ce qui élimine toute possibilité de relation entre le temps et les contraintes.

Ici encore l'analyse des défauts est un remède efficace contre ce danger comme le montre encore la figure 10 : le défaut produit vers 400° C sur des circuits intégrés est dû à la fusion du mélange or-silicium et à la migration de l'or sur les fils d'aluminium.

6-2. Enfin citons des difficultés d'ordre matériel que l'on rencontre dans les essais de fiabilité ordinaires :

- La simulation des contraintes

La production des contraintes nécessite la mise en place d'une infrastructure très importante et assez onéreuse, compte tenu du grand nombre de dispositifs à essayer.

Cette infrastructure devra produire des contraintes avec précision et reproductibilité grâce à un étalonnage soigné. C'est ainsi qu'il faut établir des cartes thermiques pour des étuves par exemple. En outre les contraintes doivent être enregistrées et surveillées attentivement.

Une autre difficulté provient du fait que les essais ne sont pas toujours normalisés. Par exemple la façon de mesurer la température d'une résistance (température ambiante à l'infini, température de surface, ...) la façon de produire cette température

(étuve en air calme ou brassé) modifient beaucoup les résultats.

- Les conditions de reprise

Le temps de reprise après contrainte doit être déterminé à chaque essai et maintenu constant.

A ce propos indiquons que la façon de supprimer les contraintes après un essai ne doit pas être quelconque. Lorsque deux contraintes sont appliquées simultanément, le maintien de l'une d'entre elles peut fausser les résultats. Par exemple des effets de surface sur des semiconducteurs sont accélérés par la présence simultanée d'une tension électrique de blocage et d'une température élevée. L'effet produit disparaît si la température seule est maintenue. Il faut donc maintenir la tension électrique pendant le refroidissement des pièces.

- La précision des mesures

Rappelons ici les précautions indispensables et les moyens à mettre en oeuvre pour pouvoir détecter à coup sûr les dégradations se traduisant par des dérives des caractéristiques. Il faut être sûr lorsqu'on énonce un résultat qu'une dérive est bien due à la contrainte et non à diverses causes "parasites" dont les principales sont les suivantes :

- a) La précision et la sensibilité des instruments. Les étalons seront soigneusement stockés et vérifiés mais il faut insister sur le fait que ce sont surtout les erreurs de fidélité qui sont à redouter : des erreurs systématiques qui restent identiques à elles-mêmes à chaque série de mesure ne faussent pas le calcul des dérives.
- b) Les conditions d'environnement : les locaux de mesure doivent être climatisés pour que les conditions de mesure soient reproductibles. A défaut, il faut enregistrer la température et l'hygrométrie au moment de la mesure : des corrections sont avantageusement traitées par un calculateur au cours de l'exploitation des mesures.
- c) Les parasites extérieurs (champs électromagnétiques) dont on se protège par des blindages.

Il est possible d'évaluer la reproductibilité des mesures de la façon suivante : On mesure une dizaine de pièces 20 fois par exemple, en quelques jours (on suppose que ces pièces ne subissent aucune contrainte et qu'elles ne sont pas modifiées jusqu'à la fin des 20 mesures). Les mesures sont effectuées à des heures différentes de la journée. Pour chaque pièce on calcule la moyenne des 20 résultats qui est en principe la valeur vraie du paramètre. On en déduit les 20 écarts entre les moyennes et chaque résultat et on trace la répartition de ces 200 écarts. On en déduit l'écart type qui donne la précision de la mesure et l'écart maximal qui a une probabilité faible d'être dépassé.

Remarque

Nous l'avons dit, la précision des mesures - plus exactement leur fidélité - joue un rôle capital dans la mesure des dérives : pour pouvoir annoncer qu'une dérive relative d'un paramètre est de 1 % avec une probabilité d'erreur faible, il faut que la précision globale de la mesure de cette dérive soit environ dix fois meilleure, c'est-à-dire de 10^{-3} . (Précision sur la valeur moyenne : la précision des mesures individuelles peut être moins bonne).

En quelque sorte les dérives détectables sont d'autant plus faibles que la précision des mesures est grande. Autrement dit, la durée d'un essai destiné à mettre en évidence la loi donnant la dérive d'une caractéristique en fonction du temps est d'autant plus petite que la précision des mesures est grande.

La précision nous apparaît ici comme un moyen d'accélérer les essais de fiabilité.

7 - LES ESSAIS ACCELERES ET LES CONTRAINTES D'ENVIRONNEMENT

Nous avons surtout parlé des contraintes électriques et assez peu des contraintes d'environnement - exception faite naturellement pour la température qui est bien la contrainte la plus utilisée.

Que peut-on dire des autres contraintes d'environnement ?

Nous pensons que les précautions à prendre sont peut-être encore plus délicates avec les contraintes d'environnement telles que les chocs, les vibrations, l'humidité. En effet, l'action cumulée de plusieurs contraintes conduit à des résultats très dispersés, ce qui explique l'importance que l'on attribue généralement à l'environnement dans les recueils de données de fiabilité (très souvent les valeurs des taux de défaillance varient dans un rapport de 1 à 100 suivant l'environnement).

Si l'action cumulée de plusieurs contraintes d'environnement est très critique, l'action successive de certaines d'entre elles joue un rôle encore plus décisif : il est bien connu par exemple que la pénétration d'humidité à l'intérieur de composants enrobés est facilitée par un fonctionnement intermittent dans l'air humide.

En effet l'humidité pénètre plus facilement pendant les périodes de repos (composant froid) et crée des dégradations pendant les périodes de fonctionnement (température élevée, électrolyse) par exemple par destruction de métallisations.

L'interprétation des résultats est donc peut-être plus délicate pour les contraintes d'environnement mais des essais en chaleur humide sont de pratique courante et des essais accélérés avec extrapolation aux conditions normales de température et d'humidité ont été réellement effectués par des fabricants de semiconducteurs.

8 - ROLE DES ESSAIS ACCELERES

Ayant examiné successivement le principe des essais accélérés, leur intérêt, leurs inconvénients, et ayant vu des exemples de réussites ou d'échecs, nous voudrions résumer maintenant le rôle de ces essais.

- A notre avis les essais accélérés, malgré les nombreuses difficultés d'interprétation que nous avons soulignées, sont effectivement utilisables pour "mesurer" la fiabilité de composants en "économisant" le temps et la quantité de pièces nécessaires. Autrement dit, eux seuls rendent possible la mesure de niveaux de fiabilité élevés.
- Les essais accélérés sont indispensables pour déterminer les lois qui relient la fiabilité et les contraintes, c'est-à-dire les lois d'accélération. La connaissance de ces lois est absolument nécessaire : on ne peut en effet songer à optimiser la fiabilité d'un sous-ensemble si ces lois ne sont pas connues : par exemple, on doit savoir de quelle manière la fiabilité des transistors dépend de leur température pour faire le bilan de la fiabilité d'un équipement et pour l'améliorer.
- Lorsqu'on s'est assuré qu'un seul mécanisme de défaillance ou de dégradation est en cause, la connaissance de la loi d'accélération peut permettre de déterminer le mécanisme physique. La recherche des réactions physiques ou chimiques possibles est en effet facilitée par la connaissance de l'énergie d'activation observée, par analogie avec celle des réactions connues.
- On entreprend en général des essais en contraintes échelonnées avant de commencer des essais de fiabilité de longue durée afin de déterminer rapidement les niveaux de contrainte à appliquer.
- Si l'on hésite parfois à employer des essais accélérés pour "mesurer" la fiabilité, il est certain que ces essais sont d'un emploi universel chez les fabricants de composants pour suivre la qualité des fabrications et pour corriger rapidement les erreurs de production, et notamment les erreurs de conception de produits nouveaux.

9 - CONCLUSION

Nous avons annoncé au début de cet exposé que la technique des essais accélérés était valable aussi bien pour les composants que pour les équipements complets mais qu'elle convenait mieux aux composants.

En effet, il est moins utile d'accélérer les contraintes pour des essais d'équipements complets car leur taux de défaillance est forcément moins bon que celui des composants. De plus les difficultés d'interprétation sont considérablement accrues dans ce cas par suite de la multiplicité des mécanismes de défaillances. Enfin, il n'est pas facile de choisir les contraintes : les contraintes réelles appliquées aux composants ne sont pas reliées simplement aux contraintes dont on peut alors disposer (la tension générale d'alimentation par exemple).

Pour terminer, disons que nous avons voulu montrer au cours de cet exposé tout l'intérêt des essais accélérés. Beaucoup de spécialistes, frappés par les nombreuses erreurs d'interprétation auxquelles on s'expose au cours des essais accélérés, refusent de leur accorder la moindre confiance.

Nous avons cherché au contraire à montrer tout le parti que l'on pouvait en tirer à condition de travailler avec prudence.

Cette technique rend tous les jours des services très précieux : comment pourrait-on sans elle annoncer ce que pourra être la dérive du gain de transistors destinés à fonctionner 20 ans dans des répéteurs sous-marins ?

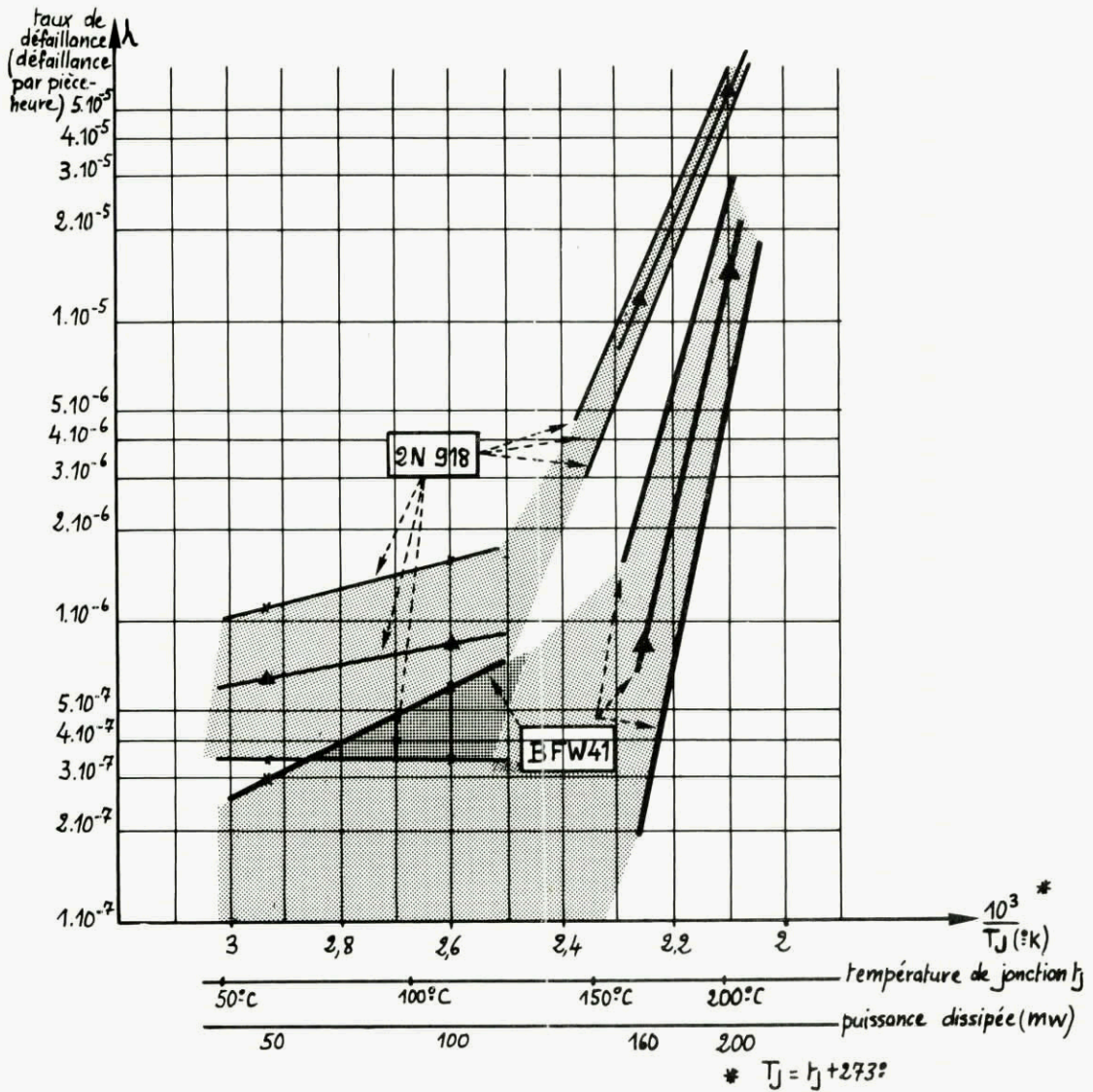


Figure 1

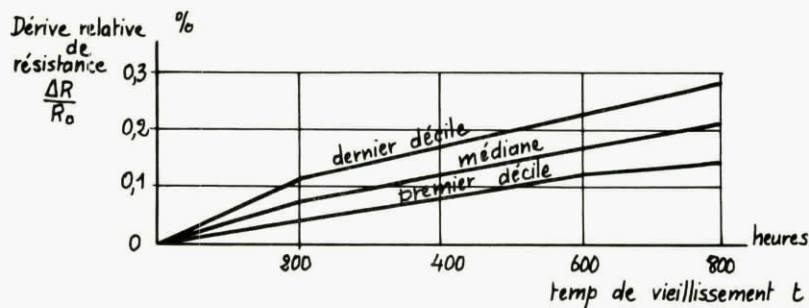
Essais accélérés de longue durée (15 000 heures) sur des transistors destinés à équiper des répéteurs téléphoniques à 2700 voies.

Le BFW 41 a des caractéristiques électriques semblables à celles du 2 N 918 mais sa fabrication comprend un programme de fiabilité.

Les intervalles de confiance à 60 % ont été figurés.

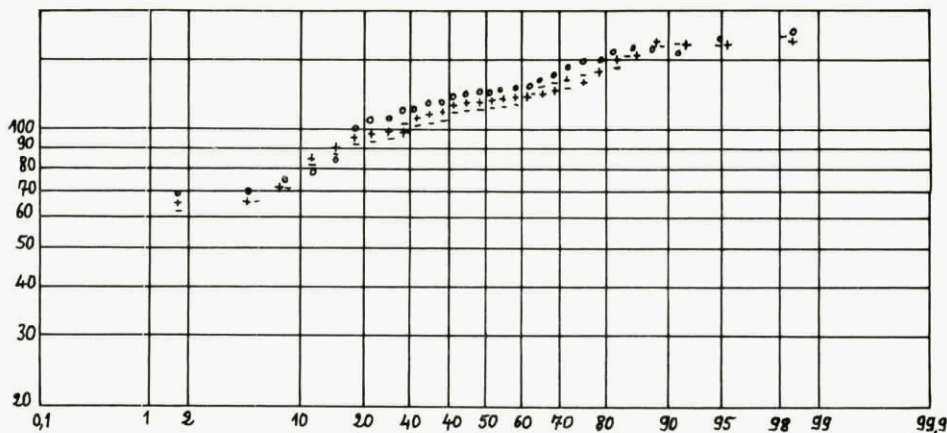
Pour les 2 N 918, le changement de pente correspond à l'apparition d'un nouveau défaut (piste pourpre) au-dessus de 100 mW.

Pour les BFW 41, il n'y a pas de défaut au-dessous de 100 mW.



- Figure : 2a -

Dérive normalisée Xi



- Figure : 2b -

Proportion des pièces
• t = 1000 heures ; T = 458°K
+ t = 500 heures ; T = 486°K
- t = 600 heures ; T = 486°K

Figure 2 - Recherche d'une loi de dérive (résistances à couches métalliques)

La figure 2a représente l'évolution des dérives de 30 résistances de 100 KΩ à 120° C sous 220 volts.

La loi de dérive moyenne peut s'écrire ici

$$\frac{\Delta R}{R_0} = 37 \cdot 10^{-5} t^{0,26}$$

ou plus généralement :

$$\frac{\Delta R}{R_0} = A t^{0,26}$$

En donnant à A l'expression $A = M e^{-\frac{qU}{KT}}$ (loi d'Arrhénius) on calcule M et U d'après les résultats obtenus à plusieurs températures T différentes.

Si on divise les dérives individuelles de chaque pièce pour chaque instant de mesure et pour chaque température, par $t^n e^{-\frac{qU}{KT}}$, on constate que l'on obtient effectivement une

série de nombres Xi qui appartiennent à une même distribution quelles que soient les valeurs de t et T.

La figure 2b montre la répartition de ces nombres ou dérives normalisées

$$Xi = \left(\frac{\Delta R}{R_0} \right)_i \times \left(t^n e^{-\frac{qU}{KT}} \right)^{-1}$$

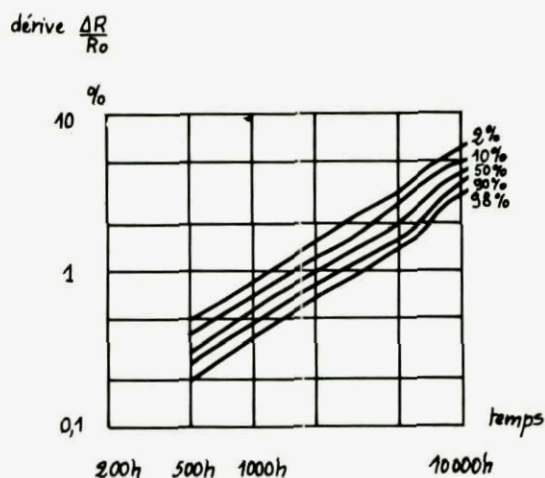


Figure 3

Dérive $\frac{\Delta R}{R_0}$ de résistances à couche de carbone en fonction du temps. (d'après une étude faite par la société LCC-CICE sur contrat du Centre de Fiabilité).

Résistances de 270 K Ω

Température de l'essai : 125° C

Puissance dissipée : $\frac{1}{8}$ Pn (Pn = puissance nominale)

Une série de courbes analogues a permis d'établir la loi d'accélération expérimentale :

$$\frac{\Delta R}{R_0} = D_0 t^{0,6} e^{\left(14,1 - \frac{5900}{T}\right)}$$

t = durée en milliers d'heures

T = température absolue de la couche

$D_0 = 0,54 + 0,128 \log R$.

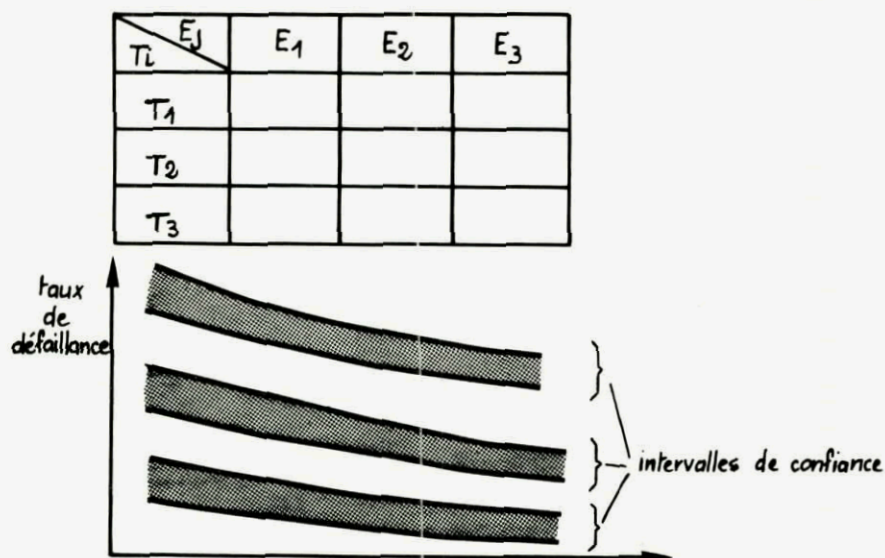


Figure 4.

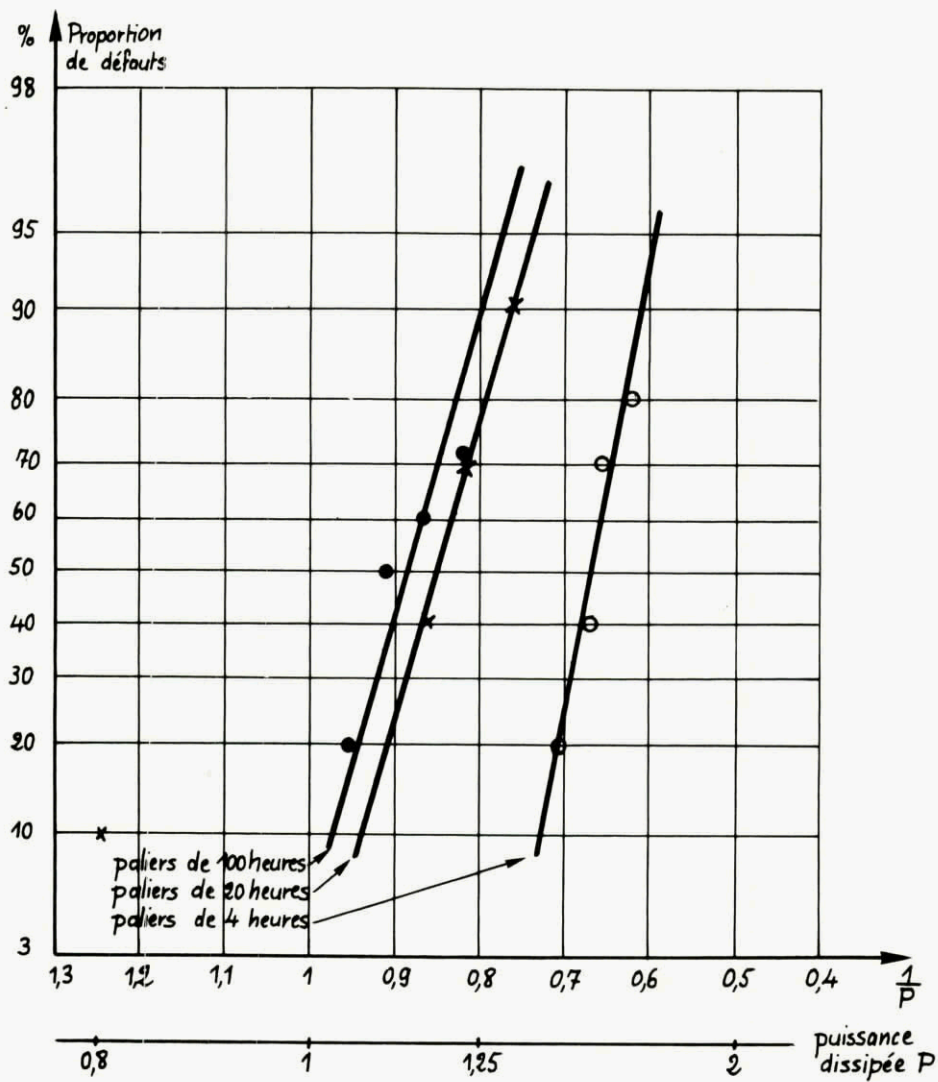


Figure 5 - Essais en contraintes échelonnées de transistors 2 N 3137

Proportion de défauts en fonction du niveau de contrainte (puissance dissipée).

Ces courbes servent à tracer l'une des courbes de la figure 6. Ici les essais portent sur une fabrication (fabrication B), les transistors étant sans radiateur.

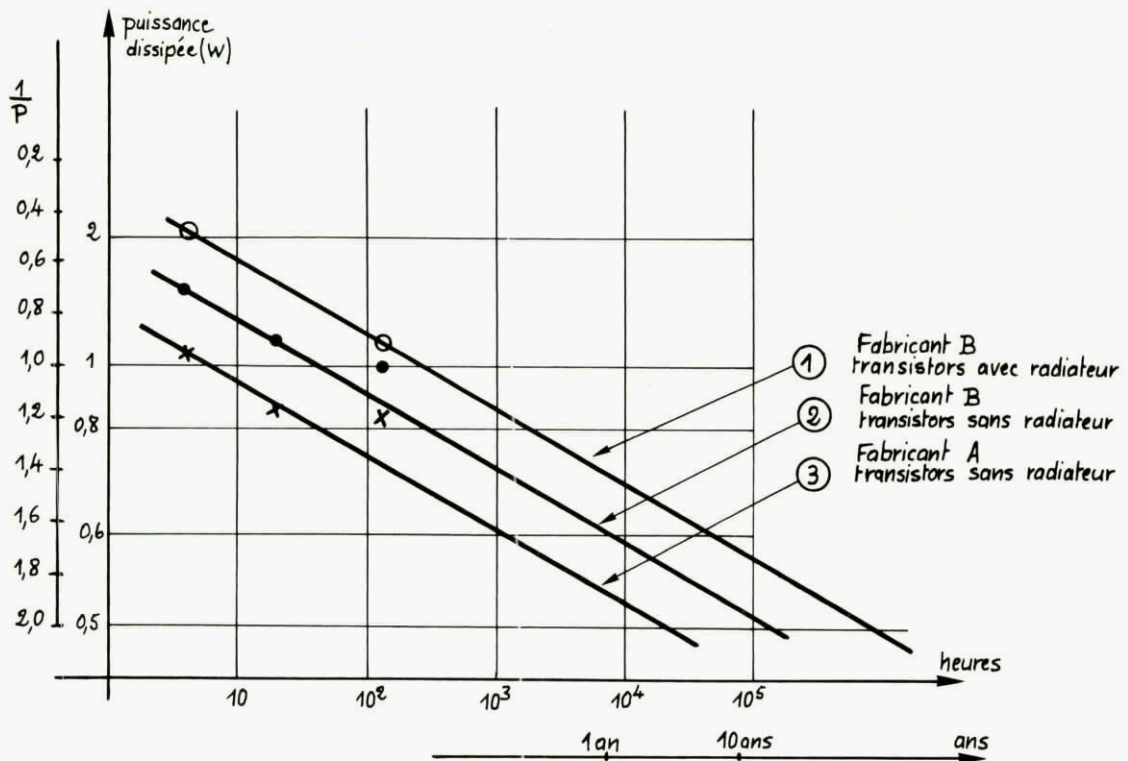


Figure 6 - Essais en contraintes échelonnées de transistors 2 N 3137
 (courbes à 20 % de défauts)

Ces courbes sont obtenues à partir des points donnés par les courbes de la figure 5 qui correspondent à la courbe (2)

On constate que - pour une puissance dissipée de 550 mw avec radiateur - 20 % des transistors B seront défectueux au bout de 12 ans. Pour une puissance de 500 mw la durée serait beaucoup plus grande (100 ans); Mais ce résultat est à considérer avec prudence car il ne concerne que le type de défaillance mis en évidence au cours des essais, c'est-à-dire ici l'électromigration d'aluminium.

Le but pratique de cet essai est de vérifier que pour la fabrication choisie, en adoptant des radiateurs et en limitant la puissance dissipée à 500 mw, la proportion de pièces défectueuses due à l'électromigration d'aluminium sera très faible au bout de 20 ans, par exemple 3 %.

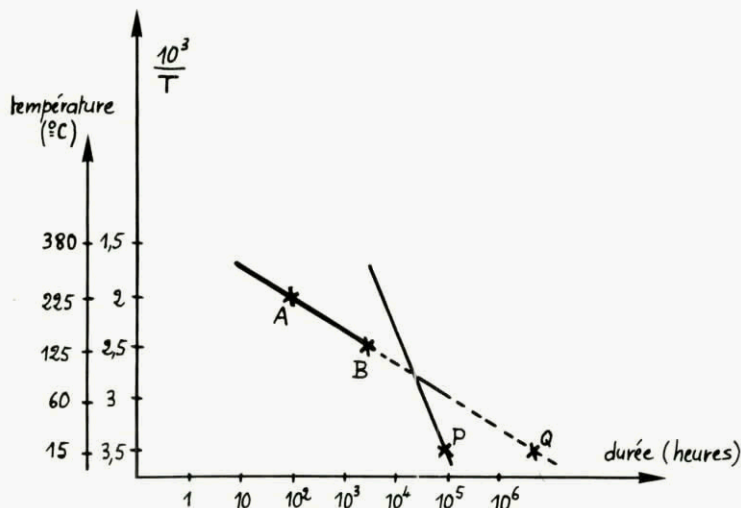


Figure 7 - Exemple de résultat erroné d'essais en contraintes échelonnées

Des essais effectués à 125° C et 225° C (points A et B), on déduit le point Q à 15° C alors que des défauts non prépondérants à température élevée donnent en réalité le point P.

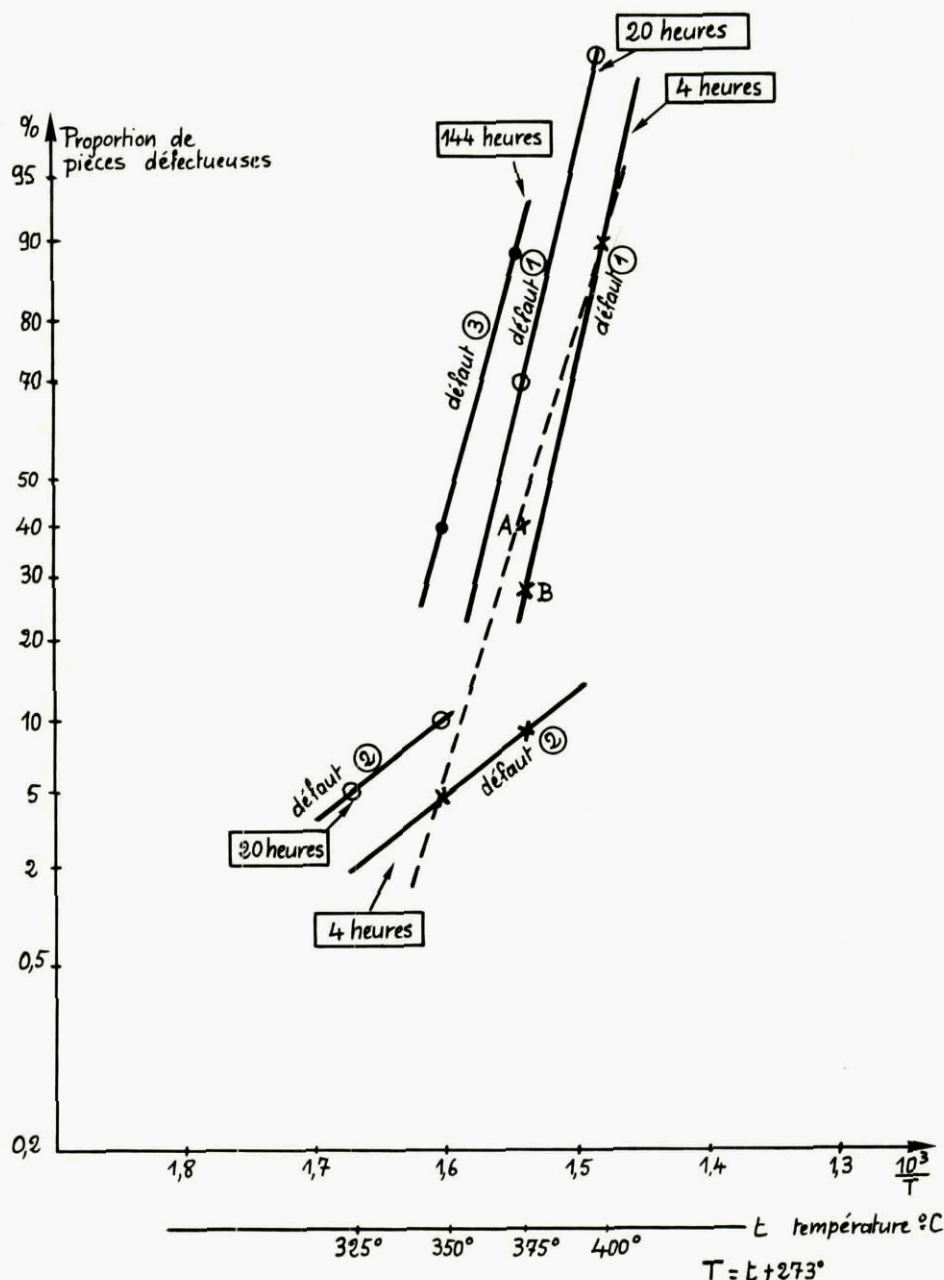


Figure 8 -

Des essais en contraintes échelonnées effectués sur des circuits intégrés n'ont produit aucun défaut jusqu'à 325° C (contraintes échelonnées en température depuis 175° C avec des paliers de 25° C, (20 pièces par lot).

Aucun des défauts obtenus à partir de 325° C ne peut se produire au-dessous de 200° C :

- pour le lot des paliers à 144 heures, le défaut observé (3) est la formation d'un composé or-aluminium sur la thermocompression des fils de sortie (fil en aluminium), entraînant la rupture du fil.

Ce défaut n'a pas été observé sur les autres lots car il aurait fallu 40 heures à 400° C pour le produire (et à 400° C, d'autres défauts sont prépondérants).

D'autre part, ce défaut a empêché les autres défauts observés avec les paliers à 20 H et à 4 H de se produire à cause de la rupture des fils.

- pour le lot des paliers à 20 heures, il y a eu deux défauts très différents au-dessous et au-dessus de 375° C, d'où la cassure de la courbe de distribution

a) au-dessous de 375° C, il y a formation d'un composé entre la dorure du fond du boîtier et l'aluminium des connexions reliant celui-ci au cristal. Ce composé gagne progressivement tout le fil puis les métallisations et dégrade les jonctions par pénétration sous l'oxyde de : défaut 2

b) au-dessus de 375° C, les pastilles sont décollées par fusion de l'entectique or-silicium : défaut 1.

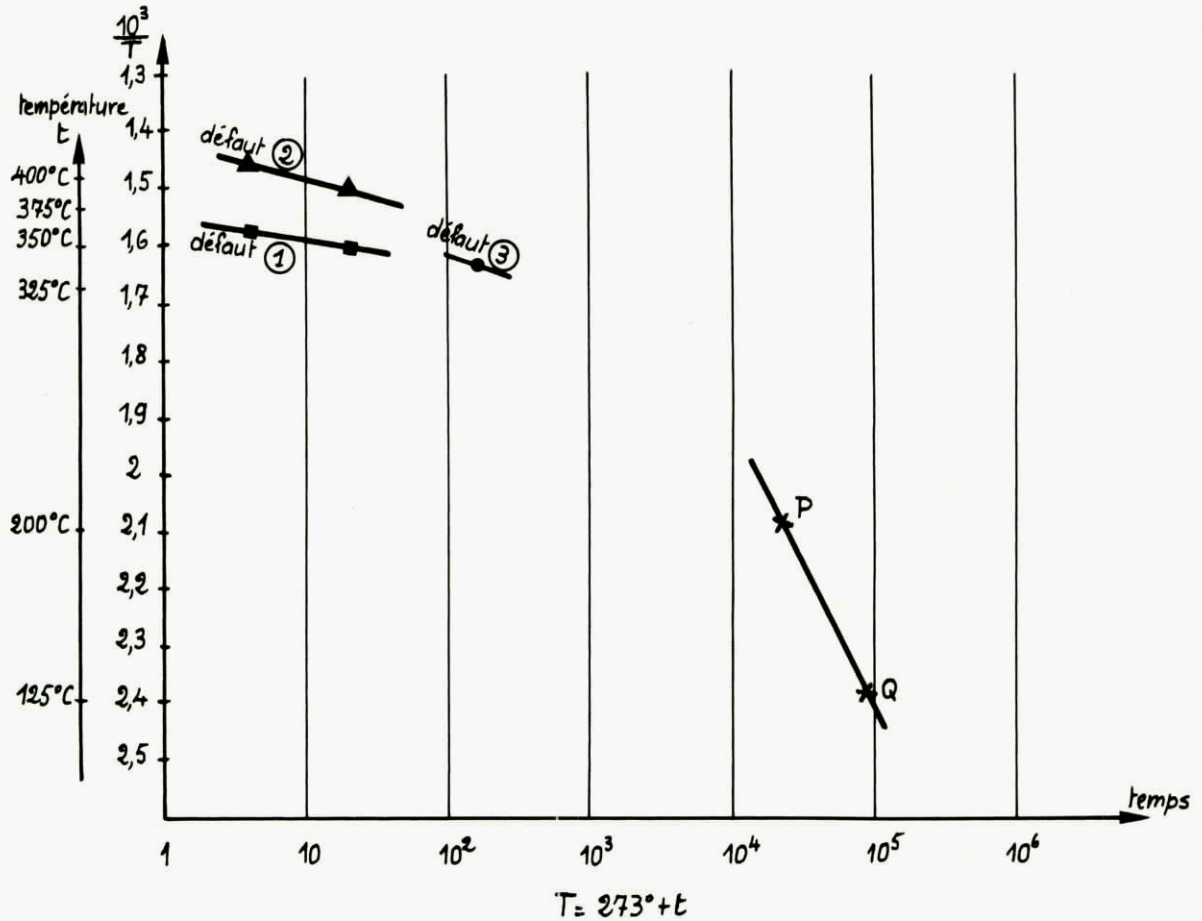


Figure 9 - Essais en contraintes échelonnées
 (courbes à 20 % de défauts)

Ces courbes obtenues à partir des courbes de la figure 8 montrent qu'il n'est pas possible dans ce cas d'extrapoler vers les températures faibles les résultats obtenus au-dessus de 325° C :

- il y a plusieurs courbes possibles suivant les défauts.
- l'extrapolation donnerait des durées très grandes alors que des essais de stockage effectués à 200° C et 125° C sur plusieurs milliers de pièces ont donné les points P et Q avec des défauts très différents.
- Pour le lot des paliers de 4 heures les conclusions sont les mêmes que pour les paliers de 20 heures.

Toutefois, sans l'analyse des défauts et en utilisant le point A pour 375° C, on obtient la droite de répartition en pointillé.

Avec l'analyse des défauts, on observe deux tronçons de droite (A 375° C, les points B et C remplacent le point A) pour chacun des défauts examinés plus haut.

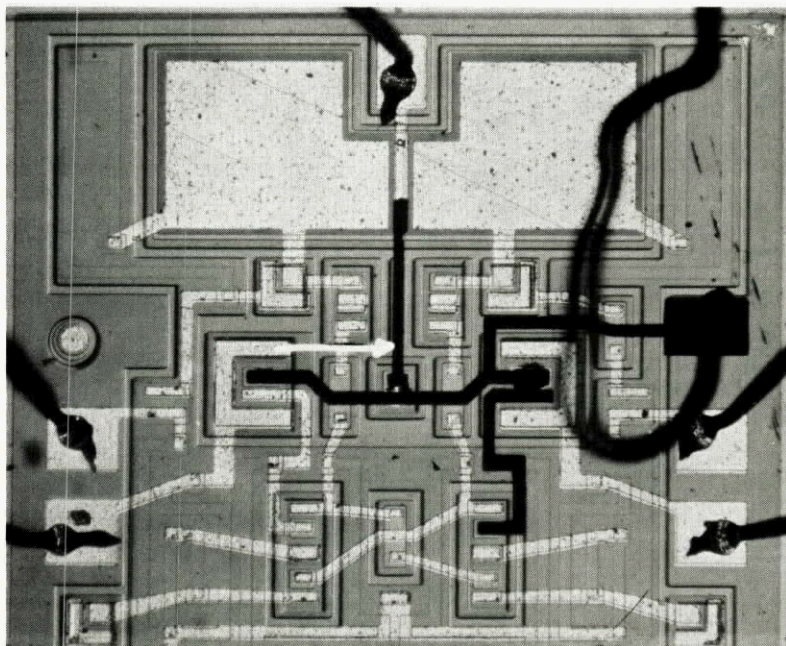


Figure 10

Cette photographie illustre l'aide précieuse qu'apporte l'analyse des défaillances dans l'interprétation correcte des essais accélérés.

Le défaut ici mis en évidence - qui ne se produit pas dans les conditions normales d'emploi - est la migration de l'or du fond du boîtier d'un circuit intégré le long des fils de connexions internes puis le long des métallisations (en noir sur la photographie).

Il s'agit du défaut (2) des figures 8 et 9.

THE BENEFITS OF A TOTALLY INTEGRATED RELIABILITY TEST PROGRAM

by

J. J. Bussolini
Director of Engineering Operations and Administration
Grumman Aerospace Corporation
Bethpage, New York

SUMMARY

As system development funds become more limited and development calendar periods are shortened, continued emphasis will be placed on system effectiveness; and the focus on design reliability will shift from software to hardware elements. Only those segments of the conventional reliability program that pay true dividends will survive in the design process. What is highlighted in this austere environment is the necessity to realize maximum benefit from the investment in component, equipment and system testing. More than 50% of the funds normally invested in system development are earmarked for some element of the test program. Evaluation of a typical system development program reveals several hundred individual test programs all leading to the successful integration of complete system. Considering the vast network of contractors, subcontractors, suppliers, vendors, parts, subassemblies, assemblies and subsystems all under concurrent development, it becomes immediately obvious that proper test sequencing and control is a necessity.

The effectiveness of a test program can be greatly enhanced if pre-planning is strengthened, providing interplay and interchange of data between test elements. Evaluation of output data from an early test can often obviate the need for or significantly modify a later test. Similarly, integration of evaluation and demonstration type testing can reduce test times while providing confidence in system performance. Also, the value of early developmental testing versus system demonstrating techniques can be traded off.

This paper discusses each of these considerations to demonstrate the benefits derived from a totally integrated test program in terms of cost, schedule and resultant system reliability.

INTRODUCTION

During the past two decades world technology has witnessed a dramatic escalation in system complexity, from the development of comparatively simple devices during the 1950's to man's most complex and sophisticated apparatus of the 1960's. As system development became more complex,⁽¹⁾ utilizing networks of subcontractors and suppliers, the integration process necessary to develop a single end product grew in importance. It also became obvious that once the basic individual design concepts were solidified, the remainder of the system development process involved a long series of tests to check the validity of initial design assumptions. Today, program test costs for major system procurements range from 50% to 80% of total program costs. As it became evident that test related costs were escalating, industry became more attentive to developing techniques for maximizing test effectiveness while minimizing test expenditures. This process generally concentrated on a search for test redundancy and duplication and in-depth evaluations to determine the best methods and levels of testing. Inherent to this search was the process of utilizing early program test results to supplement, improve or even eliminate later testing. As performance demonstrations grew in their sophistication, it became more important to insure adequate advance test planning so that proper contractual practices could be adapted at very early phases of negotiation. What evolved from all of this was a better understanding and appreciation of the concept of an integrated and well-planned test program, spanning all levels of system development.

INTERRELATED ELEMENTS OF RELIABILITY PROGRAMS

Perhaps the simplest way to shed the proper light of importance on the need for an integrated approach to reliability testing is to examine the contents of a recent aircraft systems specification that defined the reliability demonstration requirements of a modern aircraft weapon system which reads:

"The preproduction demonstration test shall determine whether the Airplane Weapon System has met the requirements defined in Section 3 of this specification. The test shall consist of (x) flights followed by the maintenance needed to bring the Airplane Weapon System to full operating status as defined by the criteria of the mission models. The reliability of the Airplane Weapon System shall be determined by a measurement of operational parameters indicative of mission functions, defined by the mission success modes of operation. . . . The quantitative reliability requirements have been met if none of the values given in Table () is exceeded."

The significance of the above paragraph is further highlighted when noting that the minimum level of mission success defined by the mathematical models referenced involve the successful performance of 14 major systems, 49 subsystems, 400 black boxes, and several hundred thousand components developed by a network of several hundred subcontractors and suppliers.

To the single Weapon System contractor involved, the successful completion of the reliability demonstration test was tied to a fixed price incentive contract which through interrelated incentives and penalties offered a 6% effect on resultant profit or loss tied directly to reliability. Still further, the approved and signed specification containing the above statements was required by the customer prior to contract award.

To prevent a disastrous outcome, the contractor in this situation must develop a totally integrated approach to all elements of program planning beginning with the development of mission models; success criteria; component, subsystem and system demonstration requirements, reliability estimates; risk assessments; flight test profiles; and performance parameters. All of this is required in order to begin the iteration process necessary to generate reliability goals sufficiently high to allow a reasonable chance of success and yet realistic enough to allow the job to be done at a fair and competitive price.

A contractor's success in this type of situation requires that he establish a reliability program that builds confidence at each step along the way. The only way to develop this confidence is through a carefully preplanned test program that is interrelated to many other program elements providing constant checks and balances on progress.

Examining only the reliability test related elements of such a program simply illustrates the complexity of this situation and highlights the need for thorough and continuous visibility of the test program (see Figure 1).

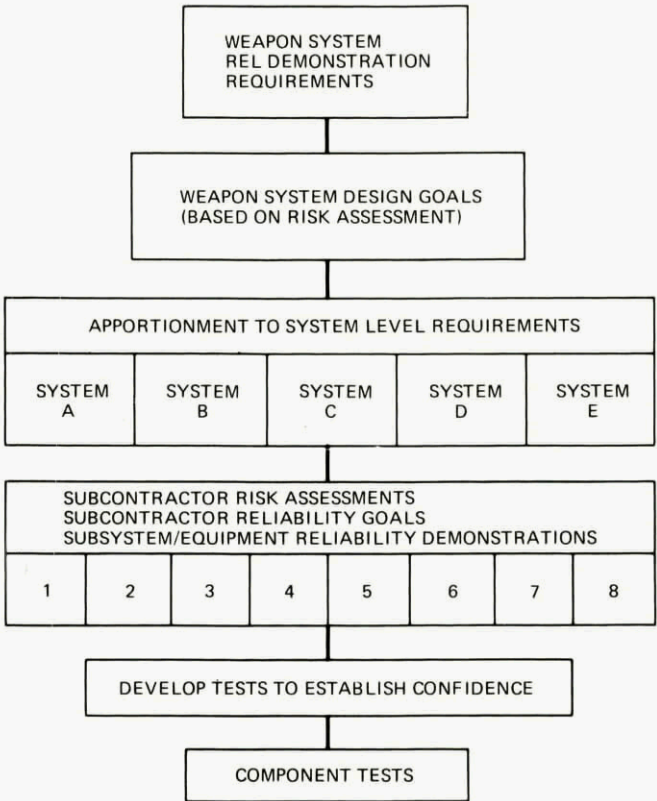


Fig. 1 Summary of Test Program Elements Related Only to the Reliability Program

An integrated approach to reliability testing, when properly planned, can form a reference against which nearly every element of a reliability program can be compared.⁽²⁾ The demonstration elements of Figure 1 and their arrangement in a time sequence flow of events as they interrelate to other program elements is shown in Figure 2.

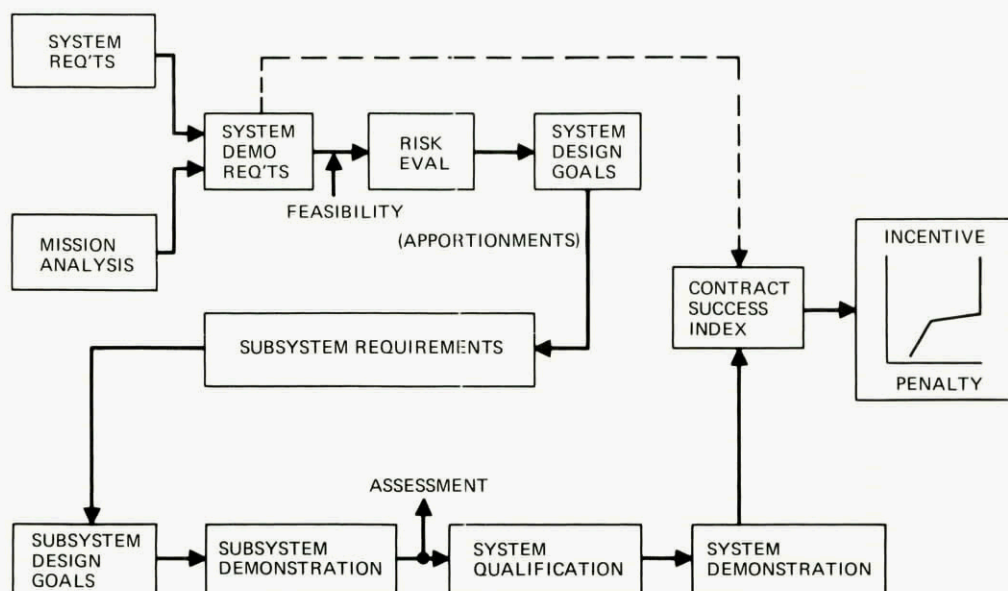


Fig. 2 Demonstration Program Flow

Relating the program elements to the demonstration criteria offers the advantage of identifying all areas of a reliability program against a meaningful end item, profit or loss expressed in terms of incentive or penalty. This ability to relate program elements and their associated costs to product reliability and its associated incentive allows intelligent reliability trade-offs to be made on an equal basis with trade-offs of other parameters.

An equally important consideration influencing the total test program is the need to visualize total program implications at every tier of contracting. Each participant in the program, regardless of his level of involvement, must recognize the effect of this performance on the ability of the systems contractor to meet his program commitments.

Current trends toward compressed development schedules and the ever present competition for funds requires a well-organized integrated test program capable of yielding a step-by-step growth in system capability.

Since the earliest birth of the reliability technology and the development of AGREE testing techniques, most theoreticians have claimed that reliability must be designed into a product and if not introduced then, can never be realized. Classical growth curves have always been related to confidence growth rather than actual reliability growth. Contrary to this theory, this author believes that history has proven this concept to be untrue. Perhaps during the late 1950's and early 1960's when testing was used as a measurement tool rather than an evaluation tool this was more nearly true. However, as more complex systems evolved, it was realized that testing had to be a truly flexible process used to assist the design effort, supplementing design analysis with corrective feedback data. Simple designs for known environmental applications usually permit the use of conventional testing techniques as a measurement tool. As designs become more complex, use environments are less than precisely defined, and program parameters vary from day to day, test flexibility and program visibility become more important.

BUILDING RELIABILITY GROWTH

Reliability growth through testing can perhaps be best visualized using the simplified example as shown in Figure 3.

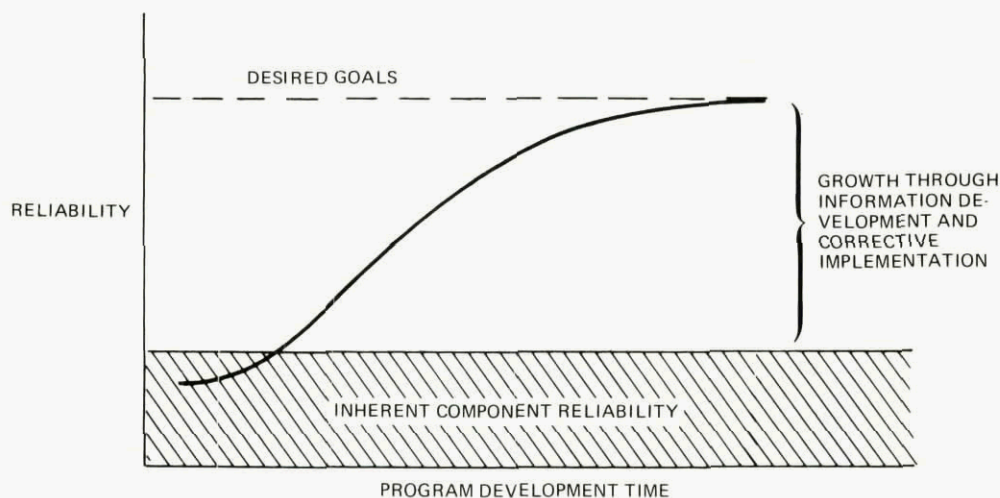


Fig. 3 Simplified Reliability Growth Process

The ability to achieve the desired reliability goals is a function of two basic items: the inherent reliability of the component parts used and the amount of growth realized through testing and information feedback to a corrective design process. The information feedback process takes many forms, a typical one is shown in Figure 4.

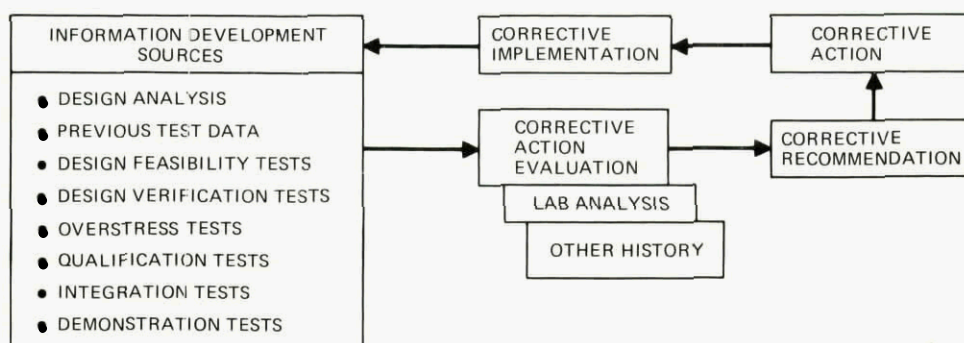


Fig. 4 Typical Information Feedback

Many elements of an integrated reliability test program will be discussed in this paper. If properly applied, each of these elements must contain some form of the above feedback process. Regardless of the test source, failure related information must be evaluated for corrective action. This can be assisted by further laboratory analysis of failed hardware or in some cases simply an examination of past history. Corrective recommendations must result, leading to corrective action and action implementation through a design "fix." A typical development program requires thousands of similar iterations of this process, each iteration contributing its share to equipment reliability growth.

Developmental reliability tests are designed to yield the maximum amount of test information at the earliest possible time and provide a continuous source of supplementary design information. As it pertains to reliability growth, the information required from the developmental test is failure information. Success oriented tests offer little more than an index measurement or perhaps provide confidence in design integrity and should come only at the end of the design process to measure specification or contractual compliance.

Within the total scope of a system development program, an unending series of tests offer a potential wealth of data applicable to failure analysis and corrective action.⁽³⁾ The more definable elements of a comprehensive reliability test program include:

- Design Feasibility Tests
- Design Verification Tests
- Overstress Tests
- Burn-in Tests
- Qualification Tests
- Demonstration Tests
- System Tests
- Flight Tests (where applicable)
- Acceptance Tests
- Operational Tests

Although each of these phases of testing offers a contribution toward reliability growth, a well planned test program will provide the largest yield from the first three of these tests.

Design Feasibility Testing simply proves the functional integrity of a design. These tests are normally performed on breadboard or mechanical models and are primarily used to test analytical assumptions and evaluate alternate design schemes. Subassembly and packaging configurations and part and material selections are evaluated with this type of testing. Electrical breadboards are normally subjected to temperature excursions and mechanical models to vibration as a minimum during design feasibility tests. Since no pass-fail criteria is established for this test and it represents the first formal design evaluation, it provides the prime source of data relative to pure design integrity.

Design Verification Testing is used to develop confidence in the ability of a design to survive the expected operational environments. The test conditions are normally combined environments to represent simulated mission conditions. Although no formal quantitative reliability measurement is made as a result of verification testing, environmental limits are usually increased to at least qualification levels to provide a degree of assurance that the design will withstand its operational environments and successfully complete formal qualification testing. Related to its failure analysis elements, verification testing is a form of design "cleanup" and normally detects failures that are not basic component problems but rather problems of a nature related to manufacturing defects, procedures, quality errors, etc.

Overstress Tests are used as the last element of the development test program that has the potential for early reliability improvement. Implementation of overstress testing has been motivated by the knowledge that 68% of all electronic equipment failures are traceable to an environmental cause. Environmental design weaknesses are detected and corrected by the controlled application of combined environmental overstresses. Both design and fabrication deficiencies are detected from this type of test and because the test is of a destructive nature, it provides a significant input to the failure analysis process.

Overstress testing has been the most controversial of the developmental test elements. Like most techniques of destructive testing, the test and equipment costs versus the relative benefits are the subject of continued question. At the component part level, step-stress techniques have proven extremely valuable as a method of detecting potential failure mechanisms, for testing environmental susceptibility and for obtaining indices for stress-time correlations. At higher assembly levels the benefits of overstress testing lie largely in areas pertaining to design weaknesses, the measurement of environmental safety margins and as a prequalification indicator.

BURN-IN TESTING

MIL-STD-721B defines burn-in as "the operation of an item to stabilize its characteristics..." Although usually specified as a test option, burn-in testing has gained popularity especially among component manufacturers desiring to eliminate the defective product. Figure 5 illustrates some typical aircraft electronic equipment monitored over its first 300 hours of operation. Since several units of each equipment were monitored, sufficient operating time was accumulated to allow a basic measure of equipment MTBF. There is definite indication that the MTBF of this sample stabilizes after some period of initial operation. Because of the rather significant increase in MTBF that has been realized by the proper application of assembly burn-in, this test technique has gained popularity as a predemonstration test where reliability is subject to statistical measurement.

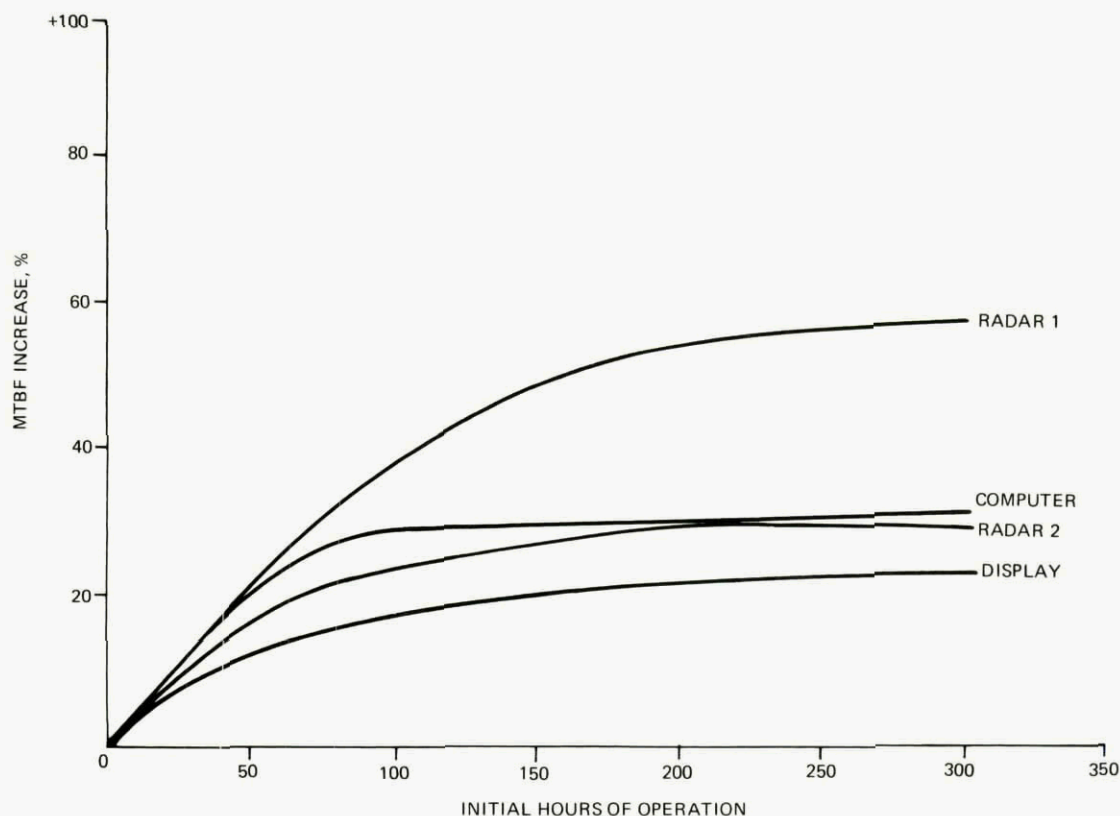


Fig. 5 MTBF Stabilization With Running Time

RELIABILITY DEMONSTRATION TESTING

Today, reliability demonstration is rather precisely defined by MIL-STD-781B which presents a variety of test plans and yet permits the flexibility to tailor the test environments to the specific expected operational conditions. The use of reliability demonstration testing as a measure of contract compliance has been reduced to routine. The subject of reliability demonstration, however, is marked with the scars of years of bitter argument extending back to the release of the AGREE report. Although the roots of these arguments still remain today, debate has subsided only as a result of the realization that if quantitative reliability requirements exist, so must exist a valid statistical method of measuring the attainment of these requirements.

FAILURE ANALYSIS TESTING

The benefits of performing one or more of the reliability tests mentioned can be completely nullified if each test is not accompanied by complete and effective failure analysis and its related tests.⁽⁴⁾ The increased popularity of all forms of reliability testing has provided the necessary motivation to develop new failure analysis procedures. Comprehensive knowledge of the physics of component failure, modes and mechanisms of malfunction and in many cases the basic material properties, is a prerequisite to being an effective failure analyst.

The complexity and sophistication of industrial failure analysis laboratories is visual proof of the importance of this segment of the reliability test technology. Perhaps the most rapidly moving segment of the technology of reliability testing currently is represented by failure analysis testing. Included among the reasons for the emphasis on failure analysis testing is the widespread use of integrated circuits, recent advances in LSI application and other highly sophisticated devices.

With the state-of-the-art in integrated circuits advancing at such a rapid pace, the need for complete analysis capability of all failure modes of these devices has increased tenfold. The advent of large scale integration is placing an unprecedented demand on design monitoring and failure analysis testing. The need to obtain complete and accurate data on the operational and thermal characteristics of these devices cannot be overemphasized.

RELIABILITY ACCEPTANCE TESTING

High quantity production presents serious problems when desiring to insure that inherent design reliability is maintained throughout the manufacturing process. A new form of reliability acceptance testing has emerged and is now being applied with some degree of success. The concept involves a supplement to the MIL-STD-781B acceptance tests involving a requirement for failure-free test operation on each deliverable end item. The time period of failure-free operation is dependent on the required level of equipment reliability in accordance with a variable scale similar to that shown in Figure 6. The maximum number of failure-free test hours in this example is 100 and the minimum is 25. Limitations are also established on the maximum period of acceptance test time available to accrue this failure-free period. If the failure-free goals are not achieved within this limit, the equipment is rejected. In addition to insuring the inherent quality of each delivered equipment, this technique allows cumulative tracking of acceptance test time and failures against the standard sequential test profiles of MIL-STD-781B.

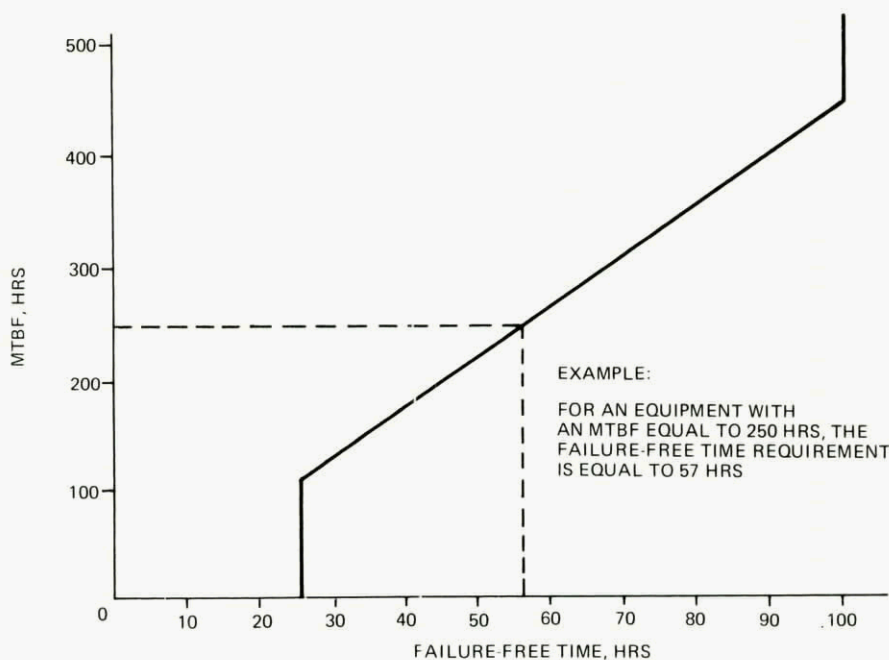


Fig. 6 Failure-Free Acceptance Testing

TESTING BENEFITS

The fact that reliability growth through testing can be realized is evidenced by the examples shown in Figure 7. The test and corrective processes of seven electronic systems were evaluated over the entire developmental test program and reliability measurements were related to major milestones in the test program. The growth in reliability was certainly not accidental, neither was it simply a function of the number of tests involved. What is significant in these examples is that the analysis of all test failures and the feedback of analysis results into the design process had a significant effect on equipment reliability growth.⁽⁵⁾

INVESTMENT AND RETURN

Perhaps the single parameter that has provided the greatest deterrent to progress in achieving design reliability is cost. As it applies to failure analysis, cost has an even more misleading effect since it is quite difficult to relate the investment in a strong failure analysis capability, to the resultant gains in design reliability. Most successful enterprises consider research as an investment in the future but on the other hand fail to recognize failure analysis as the same type of investment and view it rather as an after-the-fact corrective effort. Although rather academic, the same source that defines research as "careful inquiry or investigation" defines analysis as "the resolution of a compound into its constituent parts." Failure analysis must be considered as an inquiry and classified as the same form of investment as research. The return on this investment although a complex function in itself can be reduced to some simple statistics. Reliability improvements of between five and ten to one have been and can be achieved through the application of a well planned test and feedback program supplemented by a coordinated failure

analysis effort. A more definite illustration of the actual benefits of an effective test and failure analysis program is shown in Figures 8 and 9. Figure 8 illustrates actual results of a series of tests performed on spacecraft equipment where an effective failure analysis and data feedback system was an integral part of the test program. Marked improvements in reliability are evident at each successive stage of testing. Figure 9 conversely shows a less severe test program and a less effective feedback effort. Early testing here did not produce the proper engineering data to allow correction of problems. In addition to the slightly lower levels of reliability in the second case, of greater significance is the fact that by the third phase of testing, design and quality problems were still of serious magnitude. It must be noted that the tests #4 and #5 in both cases were non-environmental tests.

The timeliness of this reliability growth is the most critical factor. In the examples shown in Figure 7, the major improvements in reliability did not come until after qualification and as a result of reliability demonstration testing. Under normal circumstances, it is desirable to obtain reliability goals prior to these phases of the test program. It is, therefore, necessary to compress the growth period during development. There are three general ways to accomplish this compression: better components; more testing; and more effective failure analysis and feedback. Since no engineer will ever admit to deficiencies in the first element, the test and failure analysis elements become critical to the design reliability growth process.

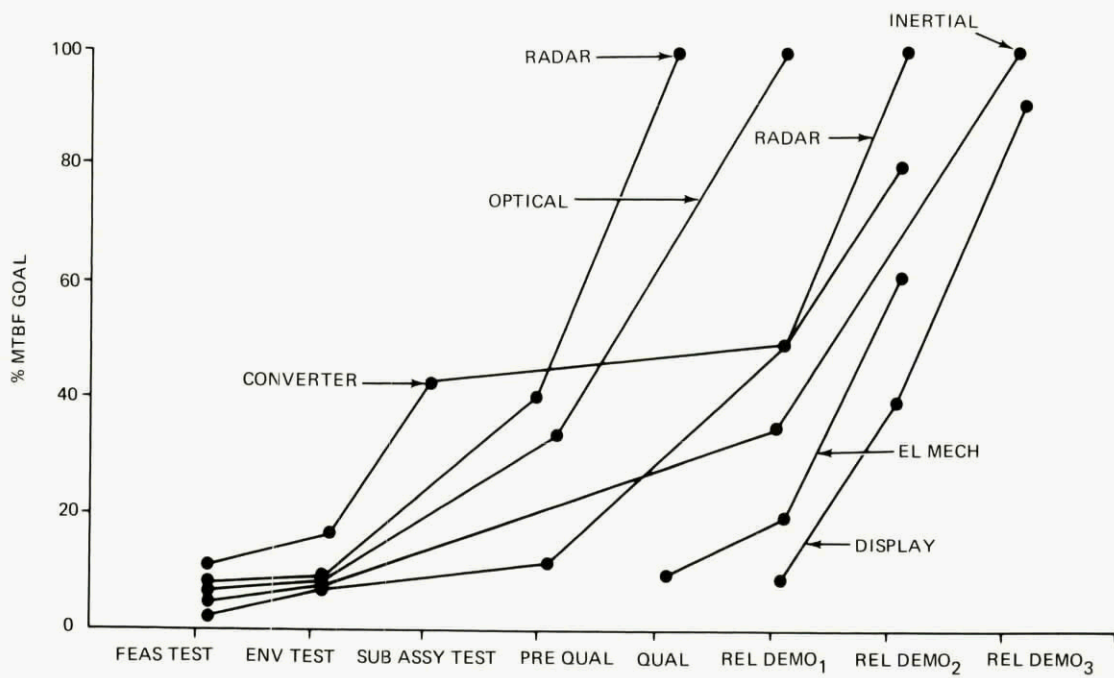


Fig. 7 Reliability Growth Through Testing and Failure Analysis

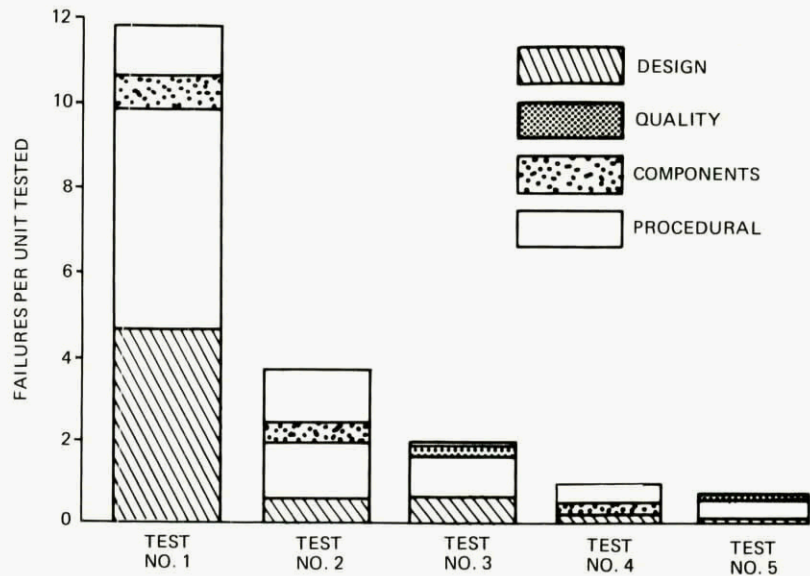


Fig. 8 Failure Trend With Integrated Test and Failure Analysis Program

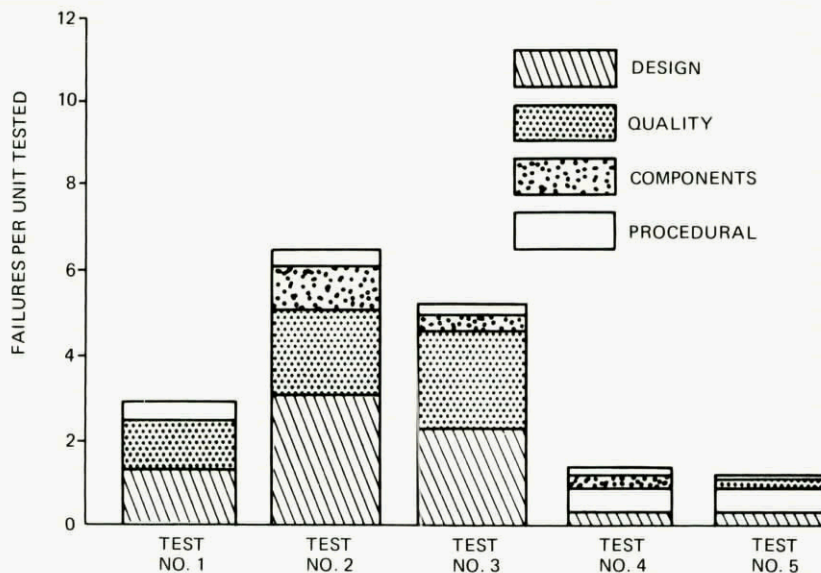


Fig. 9 Failure Trend Without a Severe Test and Failure Analysis Program

There are several ways to evaluate the relative effectiveness of an integrated reliability test program. One, as previously discussed, is to examine the ability of the test program to force the reliability growth during development. Another method, although not complete in itself, is to examine the cost of testing versus the resulting benefits. In planning a test program it is, of course, necessary to make many trade-off decisions. These decisions can be simplified by a good understanding of the cost elements involved.

Component testing is perhaps the earliest and simplest testing to be performed. It is the component test program that establishes to a large degree the inherent reliability of any design and determines the point from which growth begins.⁽⁶⁾ An illustration of the relative benefits of component screening tests is shown in Figure 10 below.

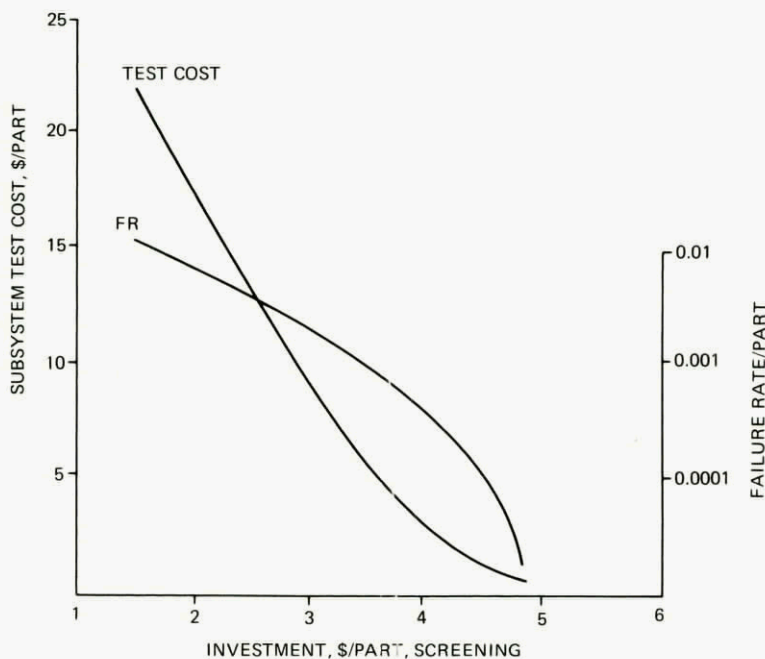


Fig. 10 Effectiveness of Screening Tests

The data for this curve was taken from component tests on several programs and compiled as a composite to increase its value. This example relates the investment costs per part for screening tests to the failure rate per part and resultant associated subsystems test costs. The obvious relationship here is that increased part testing lowers the failure rate, increases subsystem reliability and ultimately lowers subsystem test costs by reducing the number of failures during subsystem testing.

At one extreme of the curve, the average cost for part screening was \$1.5/part with a resultant subsystem test cost of \$22.0/part. At the other extreme, a higher initial investment of \$4.5/part for screening reduced subsystem test costs to \$1.0/part. The failure rate reduction per part which, of course, has the leading influence on subsystem costs, at the two extremes is more than two orders of magnitude different.

Examining a typical situation, if a 1000 part subsystem was developed with limited component testing -- say \$1.0/part, subsystem testing on that assembly might cost \$23,500.00 exclusive of qualification and demonstration. The same device with a \$3.0/part investment (\$3000 total) might cost on the average of \$5,500 for subsystem tests. The \$15,000 saving here attributed to less total failures during development.

Effective trade-off also requires knowledge of potential test costs for development and demonstration tests. Figure 11 is offered as a sample of test costs for typical electronic subsystems.

	#1	#2	#3	#4	#5
TYPE OF TEST	SEQUENTIAL DEMONSTRATION	FIXED TIME DEMONSTRATION	DEVELOPMENTAL SHAKE-DOWN	SEQUENTIAL DEMONSTRATION	BURN-IN TEST
MTBF REQM'T	350 HOURS	1000 HOURS	—	100	—
TOTAL TEST HRS	1300	10,500	1000	*700 EST	48/UNIT
TOTAL TEST COST	\$87,000	\$345,000	\$85,000	\$80,000	\$3500/UNIT
TEST COST/HOUR	\$67/HR	\$34/HR	\$85/HR	\$110/HR	\$73/HR
*ESTIMATED FIXED PRICE-COST					

Fig. 11 Typical Reliability Test Costs

Although the range of costs (from \$34/test hour to \$110/test hour) are generally related to the type of program, they are representative of contemporary test costs incurred during the development of fairly sophisticated electronic hardware.

Several items should be noted when evaluating this data. The costs incurred with the fixed time test are minimized by the capability to mechanize the test operation. During sequential tests on the other hand, the relative briefness of the tests does not induce mechanization and results in higher average (\$/hour) test costs. The sequential demonstration test figures for Equipment #4 represent a supplier fixed price estimate for demonstration testing. The average test cost estimate here is due to the supplier's attempt to reduce his financial risk by estimating the test to sequential truncation point of seven MTBF multiples. In reality, this test was actually completed in three MTBF multiples providing the supplier with a substantial financial reward for designing a product that exceeded specification requirements.

Hardware test costs are to a large extent influenced by the cost of failure. The later the test, the more costly the failure and more serious the effect on program schedules. It is necessary when attempting to accurately define test costs to examine those elements that contribute to the cost of failure. Figure 12 is the result of one survey taken to determine the cost of failure during development, qualification and demonstration testing. This example is for a typical inplant operation. The same investigations revealed that operational failure costs are double these figures.

To further evaluate the benefits of a well-planned reliability test program, it is perhaps best to examine the history of a development program where a non-integrated approach to reliability testing was taken. This example is shown in Figure 13. The example is a rather complex radar system whose procurement cost per system (hardware only) was in excess of \$150,000.

During initial development, no emphasis was placed on reliability testing and no demonstration was required. The reliability program cost during development was approximately \$50,000 and the system MTBF that resulted was about 5 hours. After about one year of operation, reliability improvement pressures were brought to bear and an overstress test program was instituted to detect and correct environmental related problems. Reliability program costs increased to about \$150,000 and the system MTBF improved to 18 hours. Still dissatisfied with system performance, a 30 hour bench burn-in program was instituted with its associated corrective action. Reliability program costs escalated to \$420,000 and system MTBF increased to 45 hours. In a follow-on buy, a 1000 hour environmental shakedown test requirement was imposed coupled with a 48 hour environmental burn-in on each deliverable system. Reliability program costs increased to more than \$600,000 with the resulting system MTBF measured at 90 hours in actual operation.

COST ITEMS	ESTIMATED COST
1. <u>TEARDOWN AND TROUBLESHOOTING</u>	\$ 50
2. <u>PART REPLACEMENT</u> PART REQUISITION, PART COST, REPLACEMENT TIME AND CHECKOUT	150
3. <u>DOCUMENTS CHANGE</u>	450
4. <u>FAILURE ANALYSIS AND REPORTING</u> ANALYSIS, INVESTIGATION AND REPORT, SUBCONTRACTOR/MANUFACTURER LIAISON	1200
5. <u>RECYCLING QUALIF OR RELIAB TESTS</u> <u>NOT INCLUDED:</u> PREINSTALLATION TEST, VEHICLE ACCEPTANCE FLIGHT TEST, PENALTIES OR LOSS OF INCENTIVE FEES	300
TOTAL	\$2150

Fig. 12 Average Cost of Parts Failure (In-Plant)

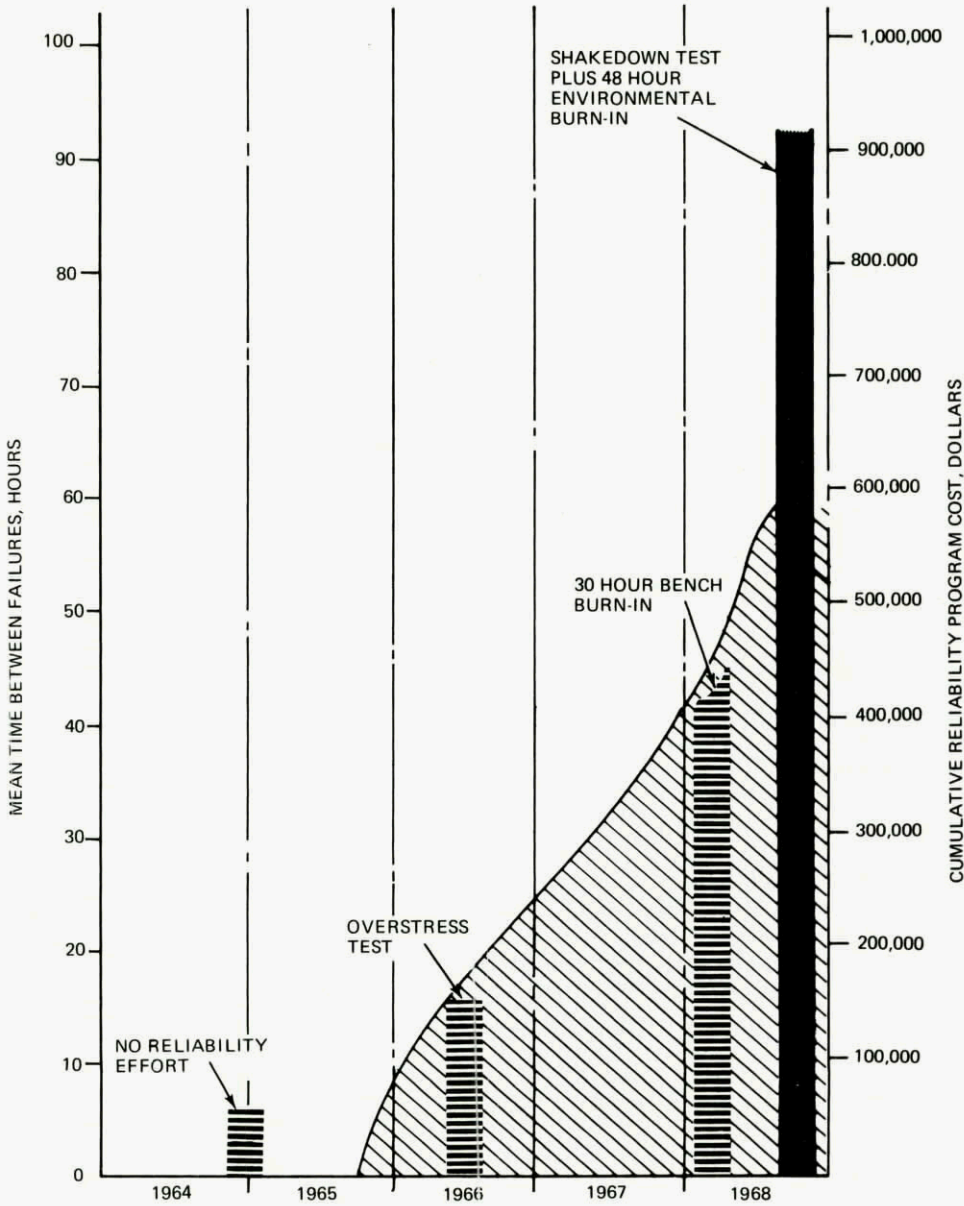


Fig. 13 Non-Integrated Test History

Had the proper amount of attention been paid to early testing of this system during initial development, the same problems could have been detected and corrected at a minimum cost, preventing the 10-to-1 increase in reliability costs, relieving the pressures brought about by substandard performance and protecting the image and reputation of the supplier.

THE SYSTEMS APPROACH TO RELIABILITY DEMONSTRATION

The vast amount of time that can expire between contract definition, specification preparation, test planning and actual test implementation, often makes it difficult to visualize the areas of interdependency between elements of a well planned reliability program. The popular "systems approach" to the solution of literally every visible problem of modern society has, if nothing else, focused attention on the need for a systematic process of evaluating and solving problems. This systems approach has quite properly been referred to in less sophisticated circles as the application of logic and common sense. Much to the dismay of those who must implement a reliability demonstration program, and even more perplexing to those who perform initial negotiations, the systems approach to reliability demonstration never seems to gain prominence with the modern managerial society. The result of this rather obscure situation has been an air of mystery and general confusion surrounding the "why" and "how" of demonstration and a tendency of view it as a problematic milestone that might just go away.

Reliability demonstration is real, and more important, is a critical element of the overall profit-loss structure. The evolution of reliability demonstration and its rather sudden surge to technical prominence has not been an accident. The trend toward more precise contract definition and the associated fixed price practices, and tendency toward incentive-penalty management at all tiers of contracting, the need for a success index to measure contractual compliance, and the use of demonstrations as a management tool to assure supplier sincerity, are but a few of the forcing functions that have driven this approach to prominence. These same factors make it imperative that a systematic approach be taken toward evaluation of requirements, assessment of economic risks, proper allocation of sublevel requirements, preparation of specifications, and eventual implementation of a comprehensive program of demonstration. Regardless of the level of contractual interest, i.e., system, subsystem, component, the same sequence of consideration occurs.

Referring back to Figure 2, the ties between related program elements can be discussed. The system requirements, generally established by the using government agency during precontract definition phases, are evaluated in conjunction with a mission analysis to determine the minimal performance relationships required for the weapon system reliability demonstration. The procuring agency will specify a risk that it is willing to take, of accepting a design, based on the system demonstration test which has not met the design requirements. Of course, during competition for the contract, a contractor might offer a demonstration requiring little risk for the procuring agency. System performance can be related to specific hardware configurations by the contractor and can then be analyzed in detail relative to the feasibility of achievement. The system design requirements and the feasible levels of achievement are then used by the contractor to evaluate the statistical and economic risks associated with not having the design accepted when the requirements have been met. This might necessitate that the contractor generate design goals higher than the actual design requirements, in order to minimize the risk associated with the demonstration test.

This process, if properly performed, establishes value and economic guidelines for the customer and contractor based on hypothetical risks. Generally, any situation of unreasonably high reliability requirements relative to feasibility, based on past performance, will become immediately obvious. Comparison of feasibility study results and the required design goals, should indicate the amount of improvement needed to attain the customer's requirements and achieve the contractors own design goals. This becomes even further refined when the system design goals are apportioned to lower levels to derive subsystem design requirements. At this point of transmittal of requirements to the next lower level of contracting, a reiterative cycle requires subsystem contractors to in turn, evaluate their risks based on their demonstration requirements and establish subsystem design goals to minimize that risk. At this point, far too many programs have gone astray by the interpretation of the difference between the design requirement and the design goal as a "buffer," rather than a technically justified risk margin necessitated by the imposed demonstration requirement.

The subsystem demonstrations provide the first statistical assessment of system reliability achievement; and after a period of system integration, the cycle is completed by a system demonstration. It should be mentioned that the primary purpose of any demonstration should be the verification that design requirements have been achieved. The results of this demonstration however, when compared to the original demonstration requirements, provide an index of contractual compliance which can be converted to incentive or penalty.

The imposition, then, of a system reliability demonstration requirement will affect not only the program cost and schedule but will additionally change the reliability goals at all levels of contracting.

SYSTEM LEVEL CONSIDERATIONS

An understanding of the system demonstration cycle requires that the cycle be dissected and each element individually examined. The system demonstration must be considered first. Although it is performed last, it is agreed upon by the procuring agency and system contractors, and directly influences all other tests. The first element of the total cycle is the process of converting the weapon system requirements into a set of demonstration criteria and the early establishment of contract success criteria. This effort, generally conducted during early contract definition phases, is critical in that it sets the tone of the entire reliability program. A sloppy effort here inevitably results in loosely defined specifications, lack of necessary program control and eventually an unhappy customer. The definition of system demonstration criteria is influenced by many qualitative and quantitative considerations such as numerical reliability requirements, mission profiles, mission success criteria, modal capabilities, degradation factors, financial risks, maintainability interfaces, demonstration hardware availability, program schedule time, retest requirements and the demonstration ground rules.

When a demonstration is part of the contract, it becomes extremely important that the reliability design requirement be specified in terms of a well defined mission or set of missions. Consider the case of a fighter which might be capable of flying combat air patrol, fighter escort, or intercept missions. Because of the differing functional requirements and time-mission profiles, the reliability objectives for each mission could differ. In specifying the design and test requirements it should be clear which mission is the basis for the requirement; or, if requirements for each mission are desired, they should not be conflicting. There are several alternative approaches to this problem of demonstrating when several design requirements exist. The simplest to define, but usually not economically sound, is to demonstrate each requirement in separate tests. Another is to demonstrate that mission with the most stringent reliability requirement; the one which generally appears to be the most difficult to achieve. Although this may appear to be a worst case test, there still might be functions not performed during this mission which are critical in other missions. A third approach is to specify the total number of demonstration missions and simulate each of the design missions in proportion to their expected operational utilization. The total number of successes that would be required to pass the test would be a weighted function of the individual mission requirements. The last to be mentioned is based on defining a "composite" mission, which could be used for demonstration but might not be an operationally feasible mission. This composite would exercise all of the functions and time profiles of the other missions and would be given a reliability requirements on this basis. The composite mission might also be used as a design reference mission for reliability trade-offs and evaluation. The approach to be used should be geared to the particular system involved. It appears that either of the last two approaches would be the most complete, in the sense of "exercising" the aircraft fully and that the extra work in defining and analyzing a composite or reference mission should prove worthwhile.

Along with a proper description of the mission, appropriate definition of the success criteria is needed. This implies definition of functional requirements, allowable degraded modes of operation including the minimum performance mode allowed for success, and the amount of degradation allowed for each function. A typical method for representing the functional requirements is shown in Figure 14.

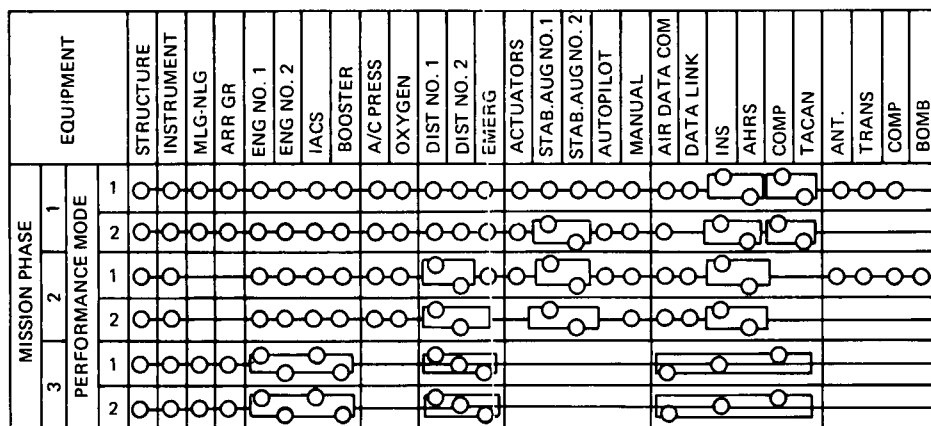


Fig. 14 Reliability - Modal Performance Diagram

This form of model presentation has proven particularly useful since it represents a performance-to-equipment conversion that can be directly inserted in a system specification. It defines two allowable modes of operation, for three mission phases for each of several functions. The system reliability model must evaluate mission phases, mission time or cycles of operation, modes of operation, redundant or back-up capability, mission criticality, etc. The mission reliability considerations must then be evaluate in terms of a probabalistic approach to actual use demonstration.

For the purpose of this discussion we will assume that the form of weapon system demonstration will consist of actual mission simulations with production type vehicles. It is possible, of course, to have a system demonstration based on assessment of equipment and subsystem level demonstration and other test data. This is a more economical approach but may not be a substitute for actual operation. Operation of the vehicle in a "real world" environment is the only means of adequately determining if the total integrated vehicle is reliable. This is the approach being taken by government agencies in current procurements. Although it imposes major burdens on the weapon system contractor in terms of schedules and risks, its value, if properly implemented to a program, seems well worthwhile.

Another important aspect of weapon system reliability demonstrations found in recent procurements is the integration with the maintainability demonstration. Thus, such interrelated reliability and maintainability parameters as mission success, mean corrective time, and maintenance man-hours per flight-hour can be measured in the same environment at the same time. Generally, in this type of test, all the reliability and maintainability parameters are measured on the results of a fixed number of flights performed in operational environment with properly rated pilots and maintenance personnel.

In order that any design deficiencies uncovered during the demonstration be remedied and the test be effective, it is necessary to schedule the test so that production type hardware, which itself has passed lower level reliability demonstrations, be employed; but before actual equipment production is underway. Because a test of even as few as 20 or 30 flights can take a few months, cost a reasonable amount of money, involve pilots, ground crews, engineering and maintenance personnel, it is necessary to carefully schedule the test as part of the total systems integration test program. Finally, it is necessary that all ground rules be established before the start of the test. If incentives and penalties are involved, it will be difficult for either for procuring agency or the contractor to be completely objective about decisions not covered by ground rules.

A major problem in this area, for system and equipment demonstrations, is the problem of retest criteria--what happens when the test is failed? Passing the test implies the reliability design requirements have been satisfied; and if everything else is satisfactory, the program continues. In the event that the reliability test is failed, certainly corrective action must be taken to remove the uncovered failure modes. But how will the system be retested? Who will pay and what will be the penalties? These questions should be carefully spelled out in the contract; not only the reliability specification, if the test is to have any reasonable meaning from a legal or contractual point of view.

After defining the parameters necessary to develop a mathematical model for system reliability, a potential design can be evaluated to determine the customer and contractor risks associated with the design requirements and possible demonstration test criteria.

EQUIPMENT DEMONSTRATION CONSIDERATIONS

As a result of the weapon system design and demonstration requirements, the system contractor will have arrived at a set of equipment objectives or apportionments based on the implied design goal. It is at this point that the evaluation of equipment demonstration methods and criteria must be firmly established, consistent with the system requirements and goals. The system contractor now becomes the customer. However, he has the additional burden of procuring many equipments such that some function of their individual reliabilities must meet the system goal. Should one or more of the equipments not have the apportioned reliability, the system goal might not be achieved and the demonstration test failed. If the contractor asks his vendors to overdesign, undue costs might result. Although the contractor might reject an equipment design on the basis of a demonstration test he would then be in the position of attempting to sell an incomplete system to his customer.

During the past few years reliability demonstration tests have been required in a large number of equipment specifications. They have generally been considered to be the best means for evaluating the reliability level of the item and for substantiating the achievement of the specification requirements. It can not be stated strongly enough that the primary purpose of the demonstration test should be verification of requirements and not the exact level of reliability. However, it is necessary that the contractor properly select the type of demonstration test, consistent with the reliability, cost, and program constraints, which optimizes the reliability information and confidence gained. The purpose of this section of the paper will be to briefly discuss some of the more common types of demonstration tests and establish some guidelines for choosing the statistical test parameters and criteria as a function of program constraints.

Equipment demonstration tests generally fall into two categories--fixed time tests, and sequential tests. Most of these tests are run in accordance with MIL-STD-781. For both types of test, methods of analyzing the results to evaluate achieved levels of reliability exist. However, there is not a clear guide or procedure for determining an optimum, or even near optimum, set of statistical test parameters consistent with program constraints. Parameters such as discrimination ratio, maximum test time, number of units to be tested, producer and consumer risks, retest criteria, test costs, and incentives must be defined and specified contractually in a consistent manner. In particular, it is a difficult problem to define exactly which equipments should be tested.

Before discussing some of the relationships between these parameters and suggesting some possible approaches to their selection, some necessary comments and definitions will be given. For the rest of the paper we will assume that the definitions of Military Standard 781 B (Reference 2) concerning the demonstration terminology apply and that the necessary mathematical techniques required are available. We will consider an optimal test to be the shortest test (in terms of equipment operating hours) that would insure that both the customer and producer risks are no greater than some predetermined value. Of course, this type of test might not be optimal from other points of view but it can serve as a reference when comparing test alternatives.

The following discussions concerning equipment demonstration tests are not meant to be complete or mathematically rigorous but to point out some of the problems and interesting aspects associated with the tests.

FIXED TIME DEMONSTRATION TESTS

In this type of test a maximum test time and a maximum number of allowable failures for a successful test are specified. If the number of failures during this time exceeds the maximum allowed the test should stop at that time. Thus, the test is actually misnamed since the time is only fixed for a successful test whereas for a failed test the actual test time is a variable. The test then could actually be considered a sequential test with the only accept point occurring at the fixed time as shown in Figure 15.

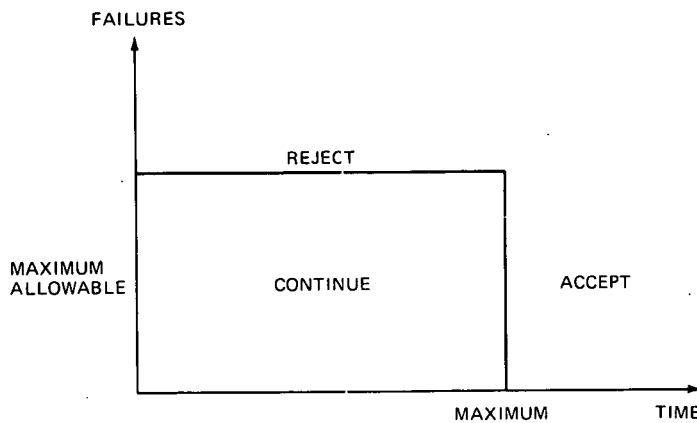


Fig. 15 "Fixed Time" Tests

Another misunderstood, or misapplied concept about fixed time tests concerns the use of minimum acceptable and specified MTBF or reliability. It is generally incorrectly assumed that the maximum test time (T), and the maximum number of failures (N), should be related only to the customer's desired confidence in accepting an equipment with some minimum reliability. The procedure involved in choosing the values of T and N should be related to some minimum MTBF level, and associated risk as defined by the producer. As in the discussion on system tests, the producer's own design goal might be higher than the specified MTBF in order to limit his risk. In reality, the producer's risk should be based on the MTBF which the product might actually achieve, and not be based on some predetermined specification value.

Assume that the specified MTBF θ_0 is a reasonable design value and the producer can accept a decision risk α based on θ_0 , and that the consumer desires a minimum acceptable MTBF of θ_1 and will accept a decision risk of β . The optimum "fixed" time test can be obtained from the formulas:

$$\alpha = \sum_{j=n+1}^{\infty} \frac{\exp(-t/\theta_0)(t/\theta_0)^j}{j!}$$

$$\beta = \sum_{j=0}^n \frac{\exp(-t/\theta_1)(t/\theta_1)^j}{j!}$$

The optimum test is given by the lowest integer value of n (maximum allowable number of failures) for which a value of t (maximum test time) exists, such that the right hand side of each equation is less than, or equal to, the left hand side of that equation. A test time greater than this optimal test value of t would tend to reduce both risks. This reduction in risk should be measured against the increased test costs and schedule delay.

SEQUENTIAL DEMONSTRATION TESTS

Though there are many types of sequential tests, the general philosophy and form can be discussed based on tests given in MIL-STD-781B and the analytical basis in Reference 1. Three tests from MIL-STD-781B are shown in Figure 16. The test times are shown here as functions of θ_1 which appears to be a better norm for the customer than θ_0 which is used in MIL-STD-781B. A comparison of test

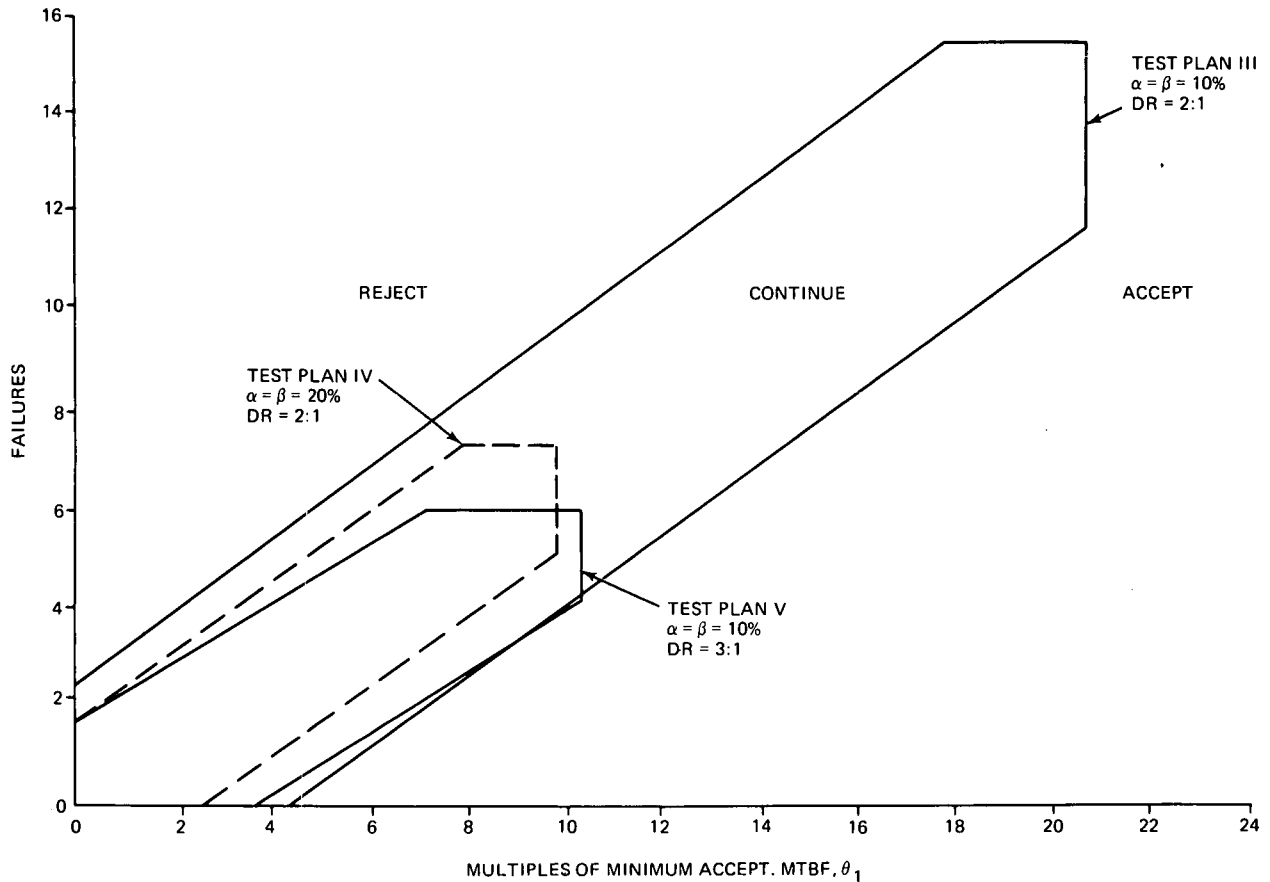


Fig. 16 Sequential Tests (MIL-STD-781B)

plans III and IV shows that the effect of increasing risks is to bring the accept-reject lines closer together and allow the truncation time to be lowered. Moving the lines closer eases both the accept and reject criteria, thus increasing the risk of accepting or rejecting incorrectly. Comparison of plans III and V shows that when the discrimination ratio is increased the effect is that only the reject criteria and truncation time are eased since the minimum acceptable is the same and the producer should be designing to a higher value for which he will have the same risk. Thus, if he designs a product which is only $2\theta_1$ rather than $3\theta_1$ the probability of failing should be greater than 10 percent. This point can be further seen by comparing plans IV and V. Although the discrimination ratios and risks differ, the two tests differ only in the accept line. Thus, it is possible to devise relatively similar tests by holding the value of θ_1 fixed and changing θ_0 , or by holding θ_0 fixed and changing θ_1 . This emphasizes the point that these values are means of specifying a statistical test requirement and that the actual risks must be based on the expected MTBF applied to the particular test plan.

One method of evaluating the effectiveness of a test is to examine the possible conclusions which could be reached based on the test data accumulated during the test. An example of this is given in Figure 17. For the various points at which the test can be concluded confidence statements are given based on the test time and number of failures at that decision point. The lower 90 percent confidence points are the multiples of θ_1 which can be used by the consumer (for accept points) and by the producer (for reject points) in comparing the test results to θ_1 .

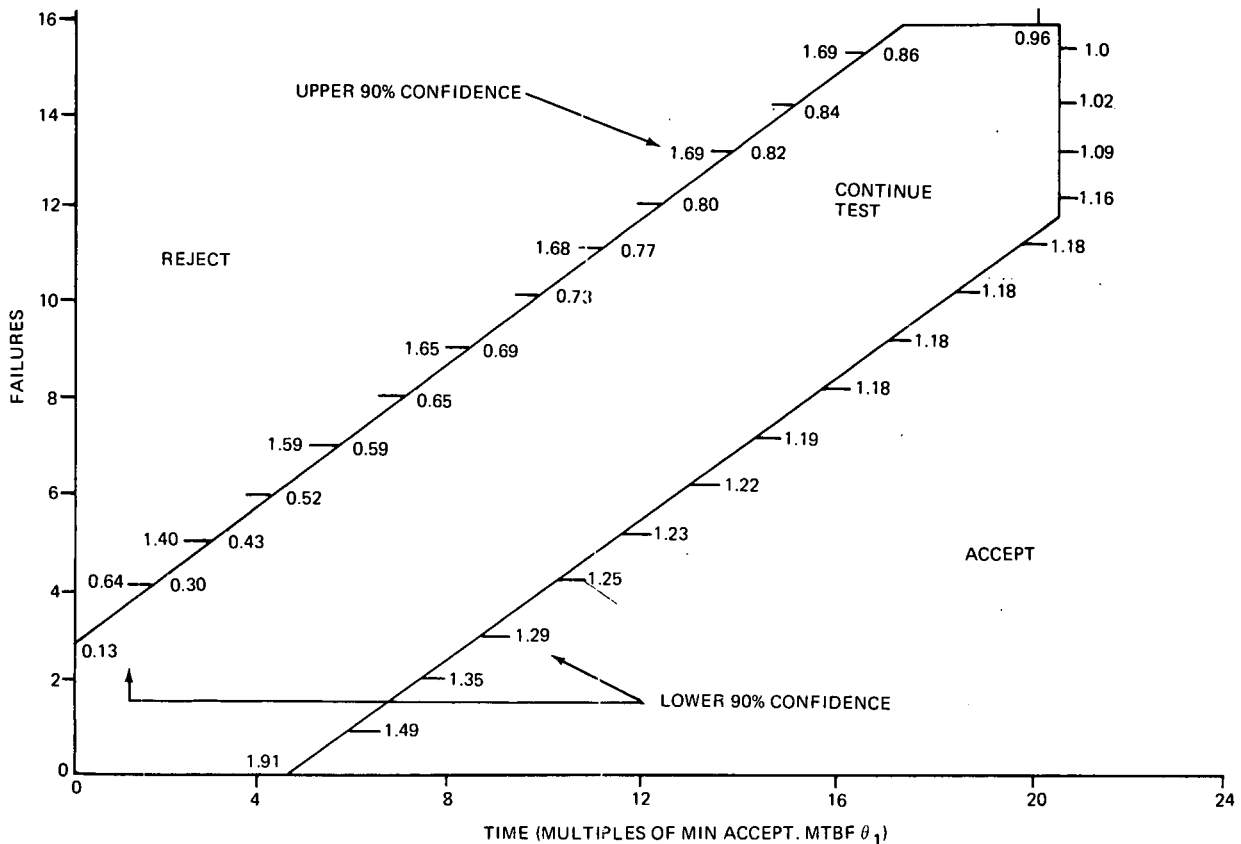


Fig. 17 Possible Test Results

These values show that for early accept points high multiples of θ_1 have been demonstrated. The longer the test lasts before an accept decision is reached the more marginal is the equipment. But it is at least θ_1 . Early reject points give low MTBF estimates. These estimates increase as the reject decision time increases, but are never greater than θ_1 . The upper 90 percent limits for reject points shows that the equipment is less than θ_0 and did not meet the specified design requirement. Thus, this type of analysis might be used to determine if, from an "after the fact" point of view, the test has violated either the producer or consumers risk levels.

Another way of interpreting Figure 17 is to note that good equipments, compared to θ_1 , will be expected to pass early. Poor equipments should be rejected early and only marginal equipments will use the maximum test time. One of the major advantages of sequential tests as a time saver is for equipments which are expected to be well above or well below θ_1 . In these cases, the sequential test should allow a decision much sooner than a fixed time test. For a marginal equipment there should not be a major difference in the test time for the two different types of tests. These values could also be used as a basis for awarding incentives based on test results.

The possibility of a marginal equipment requiring substantial test time makes the problem of appropriately choosing the truncation time an extremely important one. In order to limit test time, a truncation time is generally chosen and applied to a seemingly appropriate sequential test usually based on Reference 1. Unfortunately, this is generally done without re-evaluating and compensating for the alteration in the original risks. To some extent, this error is compounded since the accept-reject lines from Wald's equations are themselves approximations. The general effect of truncating would be to increase the risks above that of the non-truncated test. These increased risks are sometimes adjusted by changing the accept-reject lines as is done in MIL-STD-781B. However, these adjustments are usually not enough to compensate for the effects of truncation. For example, the true risks given in MIL-STD-781B for test plan III are $x = 12.6$ and $= 12.8$ as compared to the equal 10 percent risks which the test is "advertised" to be. Although these true risks are stated in the back of the document, most people using the test plan, especially non statistical types, are unknowingly committing an error of greater than 25 percent of the desired risk. This can be a rather costly error where incentives or penalties are involved.

If a shorter test is critical to a program, it should be remembered that accepting larger risks can shorten the expected test time as can a higher discrimination ratio. These approaches are effective when it appears that θ_1 is low compared to the true MTBF, and there is some other means to aid in substantiating the reliability level.

There are many guidelines used in industry for determining an optimum truncation point. Depending on whether the optimum point is meant to give the shortest expected test time or lowest truncation time, there might be many approaches. Some of these will be briefly mentioned. The oldest was to start with lines based on Wald's equation for the desired risks and truncate at 3 times the optimum fixed time test. This would not significantly affect the risks and, generally, would not reduce the expected test time. Another was to truncate the optimum time for the corresponding fixed time test and adjust the original lines as was the apparent MIL-STD-781B approach - without sufficient adjustment. A possible approach might be to truncate the test at the point where the lower confidence levels for the reject and accept lines become equal, as is the case in Figure 6. A simple approach is available to obtain a test which would be shorter than the corresponding optimum fixed time test and maintain the maximum desired risks. Consider that a test with a discrimination ratio of 2 and $\alpha = \beta = .10$ is desired. The truncation point could be chosen as the optimum point for the corresponding fixed time test and the accept-reject lines from sequential tests based on values of α and β less than .10. For example, with this approach using $\alpha = .05$, $\beta = .08$ a test where the true risks are $\alpha = \beta = .10$ is obtained.

TEST SELECTION AND CRITERIA

In addition to an understanding of the statistical concepts and tools of demonstration, the system contractor must have an understanding of program constraints and the ability to properly implement the demonstration program within these constraints. The contractor must decide which equipments are to be tested, the form of test, test criteria, method of specification, and possible incentive policy. For this discussion we will assume that the system contractor has properly evaluated his requirements and has established a reasonable set of equipment design requirements.

In order to insure that the system requirements are reached, the contractor might desire to have demonstration requirements on all equipment. However, due to schedule and cost constraints, this is not usually a realistic approach. Within these constraints, the contractor should attempt to optimize the value of demonstration testing by restricting the tests to those equipments where test results would have significant meaning. Consideration should be given to equipment criticality, state-of-the-art, complexity, other test program elements, development costs, testing costs, and the already available data. The decision, as to which units are to be tested, should be based on a weighting of these parameters.

The equipment criticalities might be assigned based on the effects of a failure. These categories, which could be obtained from the modal performance diagrams, might be: failure affects crew safety, failure affects mission success or imposes high maintenance or failure has little or no effect. Particular emphasis should be placed on those equipments whose failure alone would cause a loss of mission or possible injury to the crew.

The equipments should be compared to the state-of-the-art and could be categorized as: new design approach, state-of-art approach or off the shelf equipment. In evaluating those equipments, using state-of-the-art designs, consideration should be given to the available test and operational data for similar designs. The confidence in the reliability level of an equipment need not depend solely on a statistically designed test. Further statistical information could be gained from the development and qualification tests. This data, if valid and properly applied, could be used in lieu of demonstration tests to evaluate inherent reliability levels or to reduce the severity of test requirements and reduce test time.

Another measure of the need for demonstration is the expected level of inherent reliability based on prediction. The reliability design requirements could be compared to these predictions with the greatest emphasis being placed on those items where the ratio of requirement to prediction is the highest. The importance of this measure is based on the fact that the higher the requirement, or the ratio, the longer the test will run; another reason for not attempting to overdesign the equipment.

The cost of testing and development should be compared for the equipments as a function of facilities and manpower required, test set up time, and the number of units needed for testing. It might happen that a low cost procurement item will necessitate special or expensive test equipment and require many items for testing. These same factors might have an affect on the program schedule since the production of many test items might delay formal production.

The decision to have a demonstration test for an equipment leads to the consideration of the form of the test. Based on the previous discussions it, hopefully, is clear that not all equipments need have the same form of test nor require the same risk levels or discrimination ratio. The information used to determine the need for testing can again be used to determine the form of test. Generally, cost and schedule have the major impact on reducing the length of test and the number of units involved. Sequential tests are generally best for equipments whose expected MTBF is high or low compared to θ_1 . For marginal equipments, or where a new design is involved and maximum data is desired, a fixed

time test might be best. As discussed previously, a sequential test can usually be developed which requires less testing than the corresponding fixed time test. However, the sequential test in order to be most effective, from a test time point of view, might necessitate having fewer items on test at one time. The effect is that the fixed time test might be shorter in terms of calendar time and, thus, actually reduce test cost and schedule impact.

In order to insure that the design and test requirements are adhered to with a minimum of confusion, the specifications and purchase orders should be exceptionally clear. The requirements, form of test, test parameters, retest criteria and equipment utilization should be detailed and not left to interpretation. In general, production type hardware should be called for. If the production units are to be "burned in" prior to delivery, the test units should have burn-in.

If the consumer, based on his overall system requirements, needs only the minimum acceptable MTBF then the choice of the specified MTBF - θ_0 should be left to the producer. However, in order to protect against some of the producers not meeting their minimum acceptable MTBF's or to stimulate the producer's effort, a consumer might desire to state the specified MTBF as a design requirement. In this case, θ_0 can become a contractually binding design requirement and θ_1 a contractually binding test requirement. Care should be taken when preparing a vendor specification to clearly specify which is the minimum acceptable MTBF (test requirement) and specified MTBF (design requirement). In a properly written contract, the producer is obligated to take all reasonable measures to achieve the design requirement; and, verify this by some generally acceptable means, in addition to passing the demonstration test. This point would appear equally important to both producer and consumer, since the former must make the effort and the latter would pay for it. Thus, it might not prove practical for the consumer to ask for too much protection. This point applies, regardless of the form of the test chosen.

An important consideration associated with demonstration tests is the need for a production reliability test. The demonstration test, which occurs during the qualification phase and hopefully prior to production, should substantiate that the design has the inherent reliability desired. A production reliability test can be used to substantiate that actual production hardware has achieved the level of reliability in the engineering design.

The final consideration in determining and specifying the test is the matter of possible incentives and penalties. The value of such a policy is a result of the stimuli applied to the producer. Thus, the imposed incentives and penalties must be of a magnitude that the producer would strive for the extra profits, or at least to minimize losses. The incentives can be related not only to the reliability levels achieved but, also, to schedule adherence and test costs. The imposition of incentives on the demonstration allows the producer to evaluate the dollar effectiveness of the cost of reliability design improvements compared to the potential return from the incentive program. A reasonable policy for awarding incentives would give extra profit for achieved reliability levels above the specified design requirement, penalties for failing the test or missing schedules, and nominal profits for reliability levels between the test requirement and the design requirement.

INTEGRATED TEST PLANNING

In case after case examined,⁽⁷⁾ operational system problems were traceable back to similar related anomalies which occurred years earlier during testing but were not thoroughly evaluated for cause and effect and, therefore, not corrected. The element that causes this situation is the general lack of total test program visibility by a single program authority. In the U.S. space program, the contracting agency performed this central function, requiring that every test incident be carefully evaluated and corrective close-out implemented. The success resulting from this type of control is obvious.

To gain control requires visibility and to insure visibility requires a comprehensive plan that is agreed upon and implemented during the earliest possible conceptual program phases. It is not sufficient to look upon a reliability test program alone, but to look upon it as one complex element of the total integrated test program.

In addition to its other advantages, an integrated test plan provides a management tool to control the planning and execution of the entire test program from component, through subcontractor equipment development, to system demonstration. It provides the visibility needed to assure that required tests are performed at the lowest feasible level and that they are properly integrated into the next level to assure system compatibility. The test sequence flow also highlights the major testing interface relationships. The integrated test plan is developed to assure systematic planning of all required tests and realistic budget and schedule control.

Depending on the nature of the system being developed, the integrated test program can, by summing the individual test elements, demonstrate system compliance to contract requirements. The plan defines all of the tests to be conducted throughout the program and usually includes the objectives shown in Figure 18.

- TO PROVIDE A PICTURE OF ALL REQUIRED TESTS AND A PRACTICAL TOOL FOR MANAGING SYSTEM DEVELOPMENT
- TO INSURE TIMELY, EFFECTIVE AND LEAST-COST DEVELOPMENT WITHOUT DUPLICATION OR OMISSION
- TO PROVIDE EXPLICIT DIRECTION AND CONTENT DEFINITION OF TESTS WELL BEFORE THEY ARE INITIATED
- TO ASSURE COMPLIANCE WITH ALL INTERFACE REQUIREMENTS AND ADHERENCE TO CRITICAL PROGRAM MILESTONES
- TO USE EXISTING EQUIPMENT AND FACILITIES WHERE PRACTICAL IN ORDER TO LIMIT PROGRAM COST AND STRETCHOUTS
- TO PROVIDE A TOP LEVEL TEST DOCUMENT FROM WHICH ALL TESTS CAN BE PLANNED AND COORDINATED

Fig. 18 Integrated Test Plan Objectives

One method for evaluating and controlling an integrated test program being evaluated by NASA and several members of the aerospace industry is the failure flow analysis technique. The analysis assesses the effectiveness of a completed test program and its execution by investigating all of the defects that escaped each successive screening procedure during the component, subsystem, system and/or flight tests. The test method employs some of the tools that are similar to those commonly used by Quality Control personnel to plan and assess the effectiveness of their product appraisal system. The quality engineer identifies the "quality" aspects of the product. Each of these quality characteristics is categorized in accordance with its importance to the customer or user. The quality engineer again in this case plans his product appraisal system of tests and inspections to measure and control these characteristics.

In the failure flow method the defects are considered as the elements by which the screening procedure effectiveness is measured. Each significant test or flight anomaly is carefully diagnosed and it is determined at which level of hardware testing the defect should have been detected if the screening procedure has been perfect. An analysis is conducted of that step in the testing process in which the defect was generated and in which it was finally detected. This technique is perhaps a logical extension of a well-performed failure analysis system. The analysis method forces a review of all levels of the screening procedure and analyzes the reasons for the failure to detect the defect. Proper application of this technique is a way of passing test results on to subsequent programs to insure a continuous building of knowledge. Hardware reliability in these successive programs can be improved by the intelligent application of this information. The same concept can be applied to the application of early test results in the planning and development of later program tests on a similar program.

Effective test planning can, in itself, offer significant cost and schedule savings and improve the cost effectiveness of the entire reliability test program. Careful advance planning of test program elements based on analysis of what is really being sought as a test objective will often point to areas where information from early tests can be used to supplement or even eliminate later tests which are usually more expensive.

Reliability test program elements must also be planned in consonance with other non-reliability type tests. Electronic equipment qualification testing, as an example, usually subjects test samples to overstress conditions relative to known use environments. Failures from qualification tests and subsequent corrective redesigns can be checked and verified by reliability overstress tests or hardware burn-in tests only if the tests are properly time sequenced. Similarly, proper maintenance of failure and time logs on all non-reliability tests offers advance data for preliminary verification of reliability estimates and can also point to weaknesses that warrant detailed monitoring during later reliability tests.

Test planning can have a significant effect on test equipment costs. Proper sequencing of tests may permit reuse of test equipment, instrumentation, test chambers, etc. Qualification testing, as an example, generally requires the same type of test apparatus as overstress and reliability demonstration testing. Concurrent scheduling of any two of these elements could result in inflated test costs. Although this point might appear obvious, financial records reveal that many test programs have contributed heavily to cost overruns because of the necessity to purchase redundant or duplicate test equipment due to ineffective scheduling of related test elements.

CONCLUSIONS

Since no two development programs are identical, it would be a mistake to imply that one could generate a boilerplate test program that would satisfy all requirements. Whatever reliability test program is established must be related to the system reliability requirements, the number of levels of subcontracting involved, the severity of specification and contract control and the major analytical element of the reliability control program. Every reliability test should be carefully pre-planned keeping in mind the desired test outputs and the relationships between these outputs and analytical efforts. Developmental tests should be designed to contribute to reliability growth by proper feedback of test data and failure analysis to a corrective design iteration process. Attention to detail is required to insure that every test failure is analyzed and corrected to prevent recurrence in later tests when delays become more costly. A successive building block approach to reliability testing should be taken starting from component testing and extending through developmental demonstration and production acceptance. A systematic approach to demonstration should be emphasized to insure that maximum statistical confidence is developed at minimum cost. Test environments should be tailored to the expected use conditions where these conditions are known or can be predicted. Safety margin concepts should be utilized and reflected in test planning phases to minimize program risk.

Integrated test planning and control must be defined early to insure proper visibility of not only the reliability oriented test program elements but all other aspects of the system and sub-level test programs. A well thought-out and carefully pre-planned program of reliability testing will normally provide a sizeable return on the investment measureable in terms of improved product effectiveness.

REFERENCES

1. W. H. Douglas and G. W. Hewett, A Survey of Spacecraft Testing as Applied to Long Duration Space Missions, AIAA Test Effectiveness Conference, Palo Alto, California, 1970
2. J. J. Bussolini and S. A. Weisberg, The Systems Approach to Reliability Demonstration, Annals of Assurance Sciences 8th R & M Conference, Denver, Colorado, July 1969
3. J. J. Bussolini, Integrated Reliability Testing, U. S. Army Test and Evaluation Command, Commanders Conference, May 1967
4. J. J. Bussolini, Achieving Design Reliability Through Failure Analysis, IEEE Failure Analysis Conference, Philadelphia, Pa., 1968
5. J. J. Bussolini, Reliability Testing - Technique or Technology?, 15th Annual Technical Meeting, IES, Anaheim, California, 1969
6. J. J. Bussolini and G. Friedenreich, Improving Avionic Equipment Through Test and Failure Analysis, IEEE Failure Analysis Conference, Philadelphia, Pa., 1969
7. O. W. Chen, Integrated Test Program for a Weapon System, AIAA Test Effectiveness Conference, Palo Alto, California, 1970

OPERATIONAL CONSIDERATIONS AND SYSTEMS RELIABILITY

by B. E. Baker, MA

Chief Research Officer
HQ Strike Command
RAF High Wycombe
Buckinghamshire, England

SUMMARY

In the past military users have given only low priority to reliability and have therefore received equipment which is unsatisfactory in this respect. They now appreciate that it is necessary to specify reliability and maintainability in quantitative terms and to cover these requirements contractually. The problem of deciding what figures to specify is discussed. An example is given of trade-offs between reliability and maintainability and performance parameters. The need for a formal reliability programme is stressed and parts of this are discussed in detail. The value of reliability testing at the end of development is illustrated by a costed example.

The need for reliability

1. I am going to discuss the reliability of aircraft and avionic systems from the point of view of the military user. When we consider the characteristics of a military aircraft reliability is not the first characteristic which comes to mind. The operational performance characteristics speed, range, endurance, weapon load and sensor performance predominate, and reliability - if it is considered at all - comes last. Yet when we look at the costs of ownership of a military aircraft we find that the cost of unreliability dominates all other costs. The running cost of a military aircraft over a ten year life is typically three times the initial cost of the aircraft, and the major part of the running cost is the cost of maintenance. Similarly, if you examine the personnel of an Air Force you will find that the operational personnel are heavily outnumbered by the engineering, supply and administrative personnel.

2. The reason for this is that due to rapid technological advances - especially in avionics - and the need to keep ahead of potential enemies in exploiting these, the complexity of aircraft has increased very rapidly. There has been a steady improvement in component reliability, but at a slower rate than the increase in complexity. So system and aircraft reliability has fallen to the point where military aircraft can no longer be relied on to perform as and when they are required. Furthermore they are so expensive that it is no longer possible to get around this problem by buying more aircraft than are really needed. So the operator has come to realise that he needs reliability as well as performance. He is therefore willing to pay for it, within reason. He is even beginning to admit that a little performance may have to be sacrificed in order to obtain satisfactory reliability.

Specifying reliability

3. The problem is twofold: how to decide what reliability to specify and how to ensure that this reliability is achieved. In the past the lack of emphasis on reliability and the difficulty in deciding what to ask for have led to phrases in Staff Requirements such as, "The highest possible reliability shall be provided". Such a statement is, of course, valueless in a Contract. Moreover, although the designer may conscientiously strive to achieve a reliable design, if he is faced with the choice between degrading an unspecified reliability figure and failing to achieve a quantitatively specified performance figure, there is little doubt which course he will choose. This failure to specify reliability in a quantitative manner and to include it as a mandatory item in Contracts has led to the production of equipment which is unsatisfactory operationally, since it fails to perform when required, and also imposes a heavy servicing load.

4. It is therefore necessary to write quantitative specifications for reliability and maintainability of equipment, and this is now done by all three Services in the UK. The next step is to make these requirements a mandatory part of the Contract. We have been less successful in this, but progress is now being made with incentive schemes to cover both performance and reliability achievement.

Feasibility study

5. How, then, do we decide what figures to specify? In the UK the development process starts with a Staff Target which describes in general terms what equipment is required and what task it has to perform. At this stage we do not put in quantitative reliability requirements. The Staff Target forms the basis for a Feasibility Study by one or more Contractors. They examine the various possible technical solutions and, as part of this examination, they are asked to make predictions of the reliability of each solution. At this stage no equipment has been built so the reliability predictions can only be crude. However, predictions will differ for solutions of different complexity, and this helps us to assess whether the more complex solutions are worthwhile. The feasibility study reports are vetted by our technical experts and one solution is recommended for adoption. This comparison of different solutions may be straightforward, but on occasion it can be quite complex.

Trade offs

6. Consider for instance an aircraft required to provide airborne early warning. The radar equipment characteristics will be determined by the nature of the threat and the capabilities of the fighters which will intercept it. The main difficulty is to decide what size of aircraft to choose to carry the equipment. The larger the aircraft the more endurance it will have and the longer it will stay on patrol. On the other hand it will cost more and will have a greater failure rate than a smaller aircraft. The greater failure rate will mean a greater probability of failure in flight and a longer time spent on repairs on the ground, so there may well be a limit to the size of aircraft which is desirable. There is certainly a trade-off between endurance and reliability.

7. How do we determine this trade-off? The answer is a cost-effectiveness study, or rather a cost study at constant effectiveness. We must first enquire what is to be a typical task. This could be to maintain one serviceable aircraft continuously on patrol with high confidence at a certain distance from base for many days. For each possible size of aircraft we have to determine the number of aircraft required to perform this task. This is a very difficult problem to solve analytically but it is very easy to tackle by a Monte Carlo computer simulation. The simulation would represent the flying and servicing activities for each of the aircraft. For each aircraft the main inputs would be transit speed, endurance on patrol, probability of a mission failure, downing failure rate and average repair time. Assumptions would have to be made for such items as the delay in manning an aircraft to replace one which fails during its mission, the distribution of times to mission failure within a sortie, etc. The output would be the number of aircraft of each type to carry out the tasks with the specified level of confidence. A simplified flow chart for such a simulation is at Figure 1, and some typical results are at Figure 2.

Costing

8. To work out the cost of each solution whole life costing should be used. The cost elements for this are the development costs, capital costs of aircraft, initial buy of spares and ground equipments and the running cost of the fleet throughout its life. The running cost includes such items as fuel and lubricants, maintenance and aircrew personnel and the cost of factory overhauls of airframe, engines and equipment.

9. At the stage of development which I am discussing these costs will not be known accurately. The feasibility study will have produced estimates of the remaining costs of development, and of the unit cost of the aircraft. The other costs are estimated in terms of the unit cost since experience has shown that there are reasonably constant relationships between the unit cost and running cost and between unit cost and initial buy of spares. Both the effectiveness and cost figures are crude at this stage, so small differences in total costs are not meaningful. However, the less worthwhile options are usually identified by this type of study.

10. The essential point is to ensure that reliability and maintainability are treated quantitatively from the start of the equipment design, and that the costs of unreliability or poor maintainability are revealed by their effect on the whole life costing of the aircraft. The US Air Force Logistics Command is following this approach in Project ABLE, in which a series of equations have been developed to allow the comparative costing of different levels of reliability to be made at an early stage in design.

Staff Requirement

11. We have now come to the point at which the technical approach has been chosen and we are about to start full development. At this stage a Staff Requirement is written. This specifies in detail the required operational characteristics and also the required reliability and maintainability figures. These figures will be derived largely from the estimates produced in the feasibility study, after various checks have been applied. They will have been checked for technical feasibility by the technical authority which monitored the feasibility study. Other checks will consider whether the proposed reliability and maintainability figures are acceptable operationally and for maintenance in service. It may be worth calling for considerable effort on one vital part of the equipment. It is also necessary to state the maintenance policy at this stage, in particular whether manual, automated or built-in test equipment will be used. The echelons at which repair will be done must also be stated. Both these factors can affect the design.

Reliability programme

12. At least as important as the actual figures specified for reliability and maintainability is the requirement for a reliability programme which is also called for in the Staff Requirement. The sort of programme we use is published by the British Standards Institution in Specification BS 4200, Part 5. This includes reliability predictions for each part of the equipment, a failure mode and consequence analysis, testing of parts of unknown reliability or new design, testing of sub-units and finally a long reliability test of the complete equipment in an environment at least as severe as will be met in service. The reliability prediction, for avionic equipment, is done by means of a parts count. This pre-supposes the existence of a data bank giving figures for the reliability of all types of part under specified environmental conditions. The preparation of such a data bank is in itself a difficult and expensive task and is a subject on which many papers have been written. I will therefore not elaborate this point here, but merely remark that such data banks do exist (eg, Mil Handbook 217A).

Failure consequence analysis

13. I want to spend a little more time in discussing the failure mode and consequence analysis. In this analysis the possible modes of failure of each part are considered and the seriousness of each is assessed. The seriousness of a part failure depends on its effect on the system to which it belongs. If it causes a system failure four levels of effect can be observed. Firstly the safety of the aircraft may be affected. This is the most serious type of failure and in general it is designed out. The part or the system is re-designed until the risk is reduced to some very small, acceptable level. This will often involve the use of redundancy. Examples are dual or triple hydraulics or flying control systems.

14. The second level is the system failure which, though not prejudicing safety, does affect the performance of the aircraft's mission. The mission failure may cause either abandonment of the mission or the use of less effective reversionary modes of operation. An example of this is the failure of a navigation sensor. It may or may not be possible to continue the mission with some less accurate method of navigation. So with this type of failure the effectiveness of the mission is reduced either partially or completely.

15. The third level is the failure of a system which is not used in all types of mission. This reduces the flexibility of use of the aircraft and its importance varies according to the type of mission required at the time of failure.

16. The fourth level is a failure of a system which is covered by redundancy. This can increase the seriousness of a subsequent failure but may itself have no effect other than demanding repair at the next opportunity.

17. Next we consider component failures which degrade the performance of the systems they belong to without making the systems completely useless. As for complete system failure the seriousness of this depends on circumstances; whether the system is in use, whether degraded performance is tolerable, etc.

18. Finally, each component failure demands repair work, but the urgency of this can vary. We divide these into 'downing' failures which must be repaired before the next sortie, and others. However, this is not an absolute definition. The demarkation line can be drawn in different places at different times and by different people, depending on circumstances and degree of risk which is acceptable.

19. I have gone into the possible effects of a part failure in some detail in order to illustrate the difficulty of assessing the seriousness of such a failure, particularly while the system is still in development. Such an assessment has to be made in the context of one or more typical missions which show both the essentiality of each system to the mission, and also the time during which it is at risk. This allows a quantitative analysis to be done.

Re-design or modification

20. The failure consequence analysis or parts testing may suggest that the re-design of part of the equipment would be worthwhile. However, such a re-design would inevitably involve additional cost. To justify this we carry out a cost benefit analysis in which the benefits of higher reliability in service are balanced against the cost of the re-design. I shall be giving an example of this type of analysis later.

21. Re-design not only costs money, but it takes time and may well delay the in-service date for the equipment. Operational staffs are usually very averse to any delay. However, unreliability can also cause delay. There have been cases when unreliability has remained undetected until the acceptance trials of the equipment and has caused the abandonment of the trials until modifications have been produced. Re-design at this stage is clearly more expensive and causes more delay than if it is done during development. However, this argument is hard to put over during the development stage since the delay for re-design is certain, whereas that caused by unreliability is uncertain. Operators tend to be optimistic about this and frequently a compromise results, whereby the re-design is started but the equipment comes into service unmodified and is modified later.

Reliability endurance test

22. The value of a long and thorough reliability endurance test of the complete equipment at the end of development cannot be over-emphasised. This should be done in an environmental chamber which allows vibration, temperature cycling and humidity cycling to be applied simultaneously. The point of such testing is not to prove with a high degree of confidence that a certain reliability figure has been achieved; it is intended solely to detect and eliminate weak points in the design. There is therefore no need to reproduce exactly the stresses to which the equipment will be subjected in the field. It is probably desirable to overstress the equipment slightly since this will reveal potential weaknesses quickly.

23. Even if an equipment is designed with careful attention to reliability, a great number of design weaknesses will not be detected unless such testing is done and the equipment will not achieve its predicted reliability. A very good example of this was discussed in a paper to the IEE Conference on Reliability in Electronics held in December 1969. The paper - by JE Green and PH Mead - was entitled, "Experience gained from reliability tests on an airborne radar". The radar had been developed to the point at which performance tests had been satisfactorily completed and the design would have been accepted for production. However, at this point the aircraft for which it was intended was cancelled. The Contractor was given a further contract to carry out reliability tests and modifications. The result was dramatic. The failure rate, which was initially five times the predicted rate, was reduced to a figure very close to the predicted rate. A further interesting result was that the rate of discovery of design failures followed a negative exponential law with a time constant of about 400 hours. This result allows one to estimate the desirable duration of such tests.

24. Now although this five-fold decrease in failure rate was impressive, the testing was expensive. Moreover, it would have been necessary to repeat the testing on production models of the equipment to ensure that the change to production methods of manufacturing had not had an adverse effect on the reliability.

25. The total expense of this testing including test gear and the extra equipments produced for testing was estimated at just over £1 M. Furthermore, it was argued that the faults which had been eliminated would have been discovered during Service use at no cost and would have been cured in the normal way by modification action. It was therefore necessary to undertake a study to discover whether or not such testing could be justified in cost-effectiveness terms.

Cost benefit analysis

26. The first phase of this study was the examination of the reliability history of an in-service airborne radar, to see the extent of the reliability improvement in service, and the time taken to achieve it. It was found that a five-fold improvement in failure rate was demonstrated, but that it took the first five years of the in-service life of the aircraft to achieve it. Note that the improvement is similar in magnitude to that achieved in the reliability testing.

27. We therefore postulated two cases: one in which the reliability testing was carried out and the equipment entered service with the high reliability achieved at the end of this test. In the second case no testing was done; the failure rate on entering service was five times as high, and reduced to the same figure as the first case at the end of the fifth year of service.

28. In the 'no test' case there are certain additional costs which are indisputable. The higher failure rate leads to a greater repair bill for labour and parts. Additional equipments are needed for the repair pipeline and there will be a higher transport cost. Additional test equipment may be required. The additional technicians will require training. There will be a cost for the production of modification kits and their incorporation in the equipment. The cost of designing the modifications is not an additional cost since it is incurred in both cases.

29. The above additional costs can be derived from Service data and are non-contentious. However, there is a further cost which is harder to argue. This is the operational penalty of the lower reliability. There will be an operational task to be met by the aircraft - both in peace and war. The lower reliability will affect this task achievement in two ways. Firstly it will reduce the number of successful missions flown. This will create a need for additional sorties. Secondly it will increase the time on the ground for repairs and will therefore reduce the utilisation of the aircraft. These effects combine to produce a need to operate more aircraft. It may be argued that instead of operating more aircraft the existing aircraft could be used more intensively, so that the costs involved would only be the direct costs of flying more sorties, ie, fuel, maintenance, etc. This, in turn, argues that the optimum balance between numbers of aircraft and numbers of men and other resources has not been achieved. In some cases this may be true, but in principle if the right balance has been achieved then the cost of flying extra sorties - either by providing additional aircraft or by more intensive use of existing aircraft - should be equal. A further argument to support the use of additional aircraft is that in wartime additional sorties spread over a longer time scale may not have the same effect as the right number of successful sorties flown at the required time. This is certainly true when speed of response is critical or when penetration of the enemy defences is achieved by saturation.

30. If additional aircraft have to be bought to provide the greater number to be operated, then the cost of this becomes very large. However, since the need for extra aircraft arises only in the first few years of service, it can usually be met by operating aircraft which have been bought as the reserve to cover wastage. The additional flying will itself generate additional wastage and this must be costed.

31. The importance of these operational considerations is illustrated by the results of this study, which assumed a fleet of 100 aircraft. This fleet was built up gradually over three years, which tended to reduce the effect of the higher unreliability in the earlier years.

32. The additional costs of the 'no test' case were as follows:

	£ K
Cost of operating larger fleet	1,200
Additional wastage	320
Modifications	207
Spare equipments	100
Maintenance labour	47
Training	4
Transport	2
TOTAL	£1,880 K or £1.88 M

Luckily this is considerably greater than the £1.0M for the reliability testing. Note that without the costing of the operational penalties in terms of operating a larger fleet, the additional costs are drastically reduced and the testing is no longer justified.

33. A further point must be made which applies to all cost benefit analyses of this type. The costs of unreliability are directly proportional to fleet size, whereas the costs of reliability testing are not. Production reliability test costs will not scale directly with fleet size and development test costs will normally be independent of fleet size. Thus much greater overall benefits will be achieved for larger fleet sizes. For small fleets a reliability test programme of this size may not be justified.

Conclusions

34.

- a. In the past the achievement of high reliability has been subordinated to the achievement of high performance. This has led to the production of equipment which has been unsatisfactory in service.
- b. To counter this tendency, reliability and maintainability requirements must be specified in quantitative terms, and these requirements must be covered contractually.
- c. Reliability activities must proceed concurrently with equipment development, and these must form part of the development plan.
- d. Reliability testing at the end of development is of particular importance.
- e. Reliability work can be shown to be cost effective.

Figure 1 to
Paper 12 by
BE Baker, MA

PATROL AIRCRAFT SIMULATION
FLOW CHART OF INDIVIDUAL AIRCRAFT CYCLE

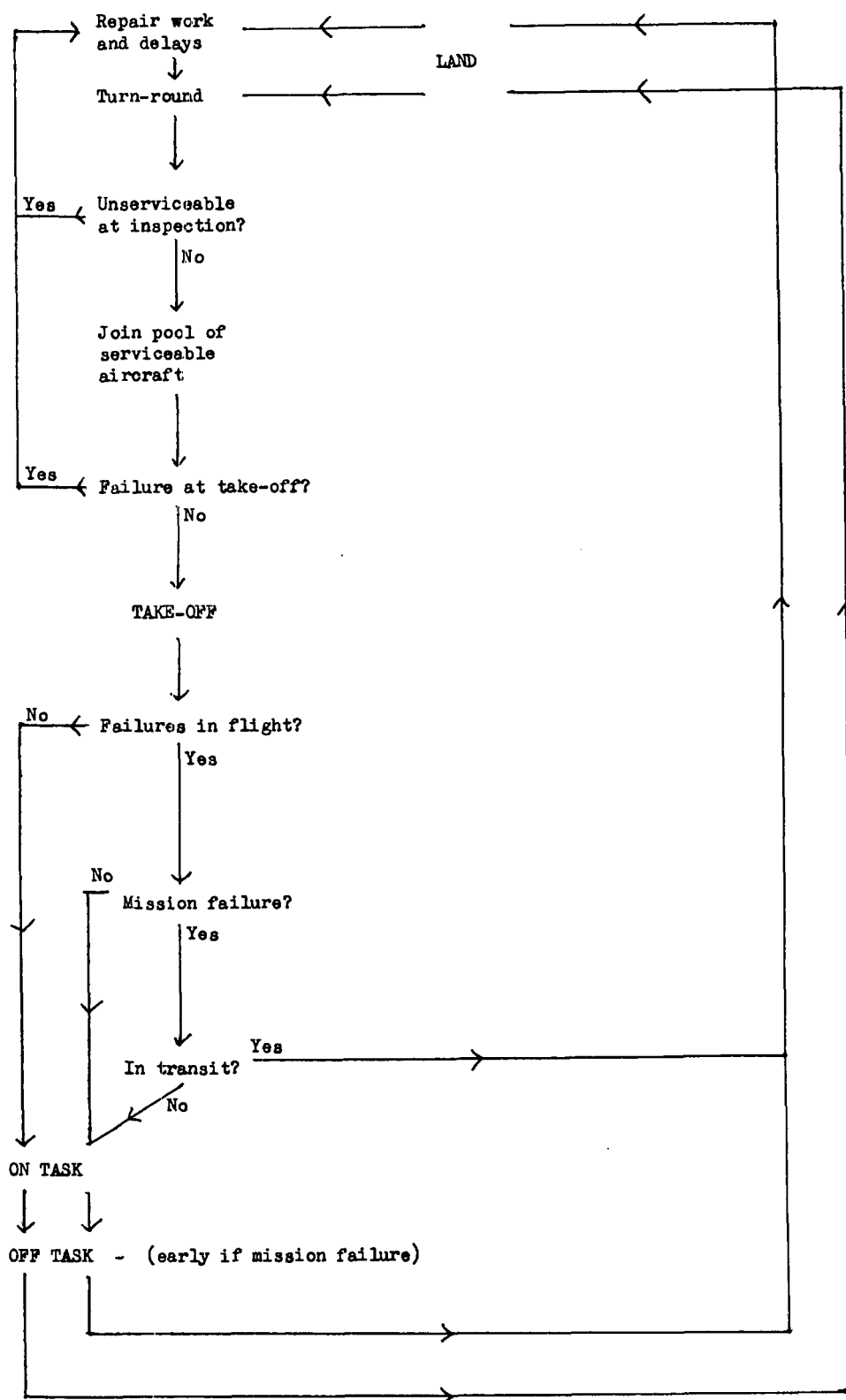
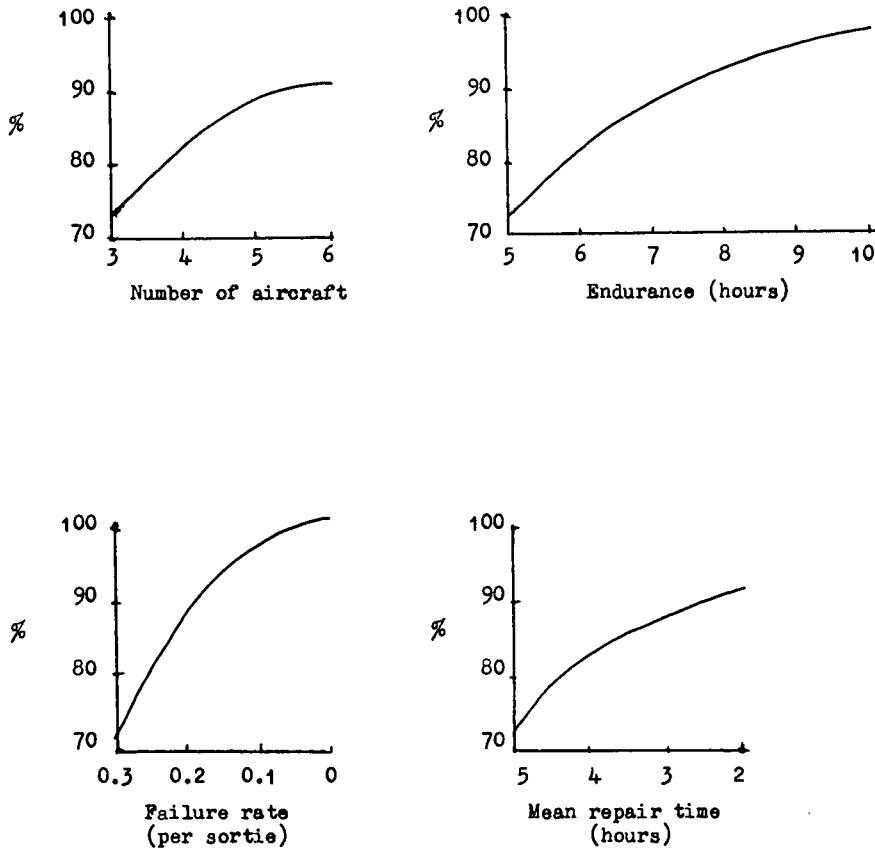


Figure 2 to
Paper 12 by
BE Baker, MA

TYPICAL RESULTS OF SENSITIVITY TESTS
ON PATROL AIRCRAFT SIMULATION



On these graphs the ordinate represents the percentage time the patrol is maintained, ie, that one aircraft is on patrol in a serviceable condition.

In each graph just one parameter is varied. The starting point at the left-hand side is the same in each case; it shows the patrol performance of 3 aircraft having 5 hours' endurance, 0.3 failure rate and 5 hour mean repair time.

These graphs demonstrate how one parameter can be traded-off against another.

NATIONAL DISTRIBUTION CENTRES FOR UNCLASSIFIED AGARD PUBLICATIONS

Unclassified AGARD publications are distributed to NATO Member Nations
through the unclassified National Distribution Centres listed below

BELGIUM

General J.DELHAYE
Coordinateur AGARD - V.S.L.
Etat-Major Forces Aériennes
Caserne Prince Baudouin
Place Dailly, Bruxelles 3

CANADA

Director of Scientific Information Services
Defence Research Board
Department of National Defence - 'A' Building
Ottawa, Ontario

DENMARK

Danish Defence Research Board
Østerbrogades Kaserne
Copenhagen Ø

FRANCE

O.N.E.R.A. (Direction)
29, Avenue de la Division Leclerc
92, Châtillon-sous-Bagneux

GERMANY

Zentralstelle für Luftfahrtokumentation
und Information
Maria-Theresia Str. 21
8 München 27
Attn: Dr Ing. H.J.RAUTENBERG

GREECE

Hellenic Armed Forces Command
D Branch, Athens

ICELAND

Director of Aviation
c/o Flugrad
Reykjavik

ITALY

Aeronautica Militare
Ufficio del Delegato Nazionale all'AGARD
3, Piazzale Adenauer
Roma/EUR

LUXEMBOURG

Obtainable through BELGIUM

NETHERLANDS

Netherlands Delegation to AGARD
National Aerospace Laboratory, NLR
Attn: Mr A.H.GEUDEKER
P.O. Box 126
Delft

NORWAY

Norwegian Defense Research Establishment
Main Library, c/o Mr P.L.EKERN
P.O. Box 25
N-2007 Kjeller

PORTUGAL

Direccao do Servico de Material
da Forca Aerea
Rua de Escola Politecnica 42
Lisboa
Attn: Brig. General Jose de Sousa OLIVEIRA

TURKEY

Turkish General Staff (ARGE)
Ankara

UNITED KINGDOM

Ministry of Technology Reports Centre
Station Square House
St. Mary Cray
Orpington, Kent BR5 3RE

UNITED STATES

National Aeronautics and Space Administration (NASA)
Langley Field, Virginia 23365
Attn: Report Distribution and Storage Unit

* * *

If copies of the original publication are not available at these centres, the following may be purchased from:

Microfiche or Photocopy

National Technical
Information Service (NTIS)
5285 Port Royal Road
Springfield
Virginia 22151, USA

Microfiche

ESRO/ELDO Space
Documentation Service
European Space
Research Organization
114, Avenue de Neuilly
92, Neuilly-sur-Seine, France

Microfiche

Ministry of Technology
Reports Centre
Station Square House
St. Mary Cray
Orpington, Kent BR5 3RE
England

The request for microfiche or photocopy of an AGARD document should include the AGARD serial number, title, author or editor, and publication date. Requests to NTIS should include the NASA accession report number.

Full bibliographical references and abstracts of the newly issued AGARD publications are given in the following bi-monthly abstract journals with indexes:

Scientific and Technical Aerospace Reports (STAR)
published by NASA,
Scientific and Technical Information Facility,
P.O. Box 33, College Park,
Maryland 20740, USA

United States Government Research and Development
Report Index (USGDRI), published by the
Clearinghouse for Federal Scientific and Technical
Information, Springfield, Virginia 22151, USA

