46p

[redacted]

REPORT NO. AE610363

X63-80392

CLASSIFICATION CHANGE

TO - UNCLASSIFIED [redacted]

By authority of [redacted] E.O. 11652

Changed by [redacted] Date 8-27-73

APOLLO

FINAL STUDY REPORT

VOLUME V IMPLEMENTATION PLAN

BOOK 2 | RELIABILITY

(NASA-CR-136948) APOLLO. VOLUME 5: IMPLEMENTATION PLAN. BOOK 2: RELIABILITY Final Study Report (General Dynamics/Convair) 46 p

N74-71732

Unclas

00/99 31136

[redacted]

GIIIIIIIID

CONVAIR (ASTRONAUTICS) DIVISION OF GENERAL DYNAMICS CORPORATION AND AVCO CORPORATION

[redacted]

[redacted]

Code - None

~~SECURITY NOTICE~~

~~This document contains information affecting the national defense of the United States within the meaning of the Espionage Laws, Title 18, U.S.C., Sections 793 and 794. Its transmission or the revelation of its contents in any manner to an unauthorized person is prohibited by law.~~

NOTICE OF EXISTENCE OF PROPRIETARY INFORMATION

This report is furnished to the Space Task Group, NASA, under the terms of Contract NAS 5-304, and shall not be released outside the Government (except to foreign Governments, subject to these same limitations), nor be disclosed, used, or duplicated, for procurement or manufacturing purposes, without the permission of Convair-Astronautics, a Division of General Dynamics Corporation, and of Research and Advanced Development Division of AVCO Corporation. This legend shall be marked on any reproduction hereof in whole or in part.

CASE FILE COPY

~~CONFIDENTIAL~~

APOLLO
FINAL STUDY REPORT

Report No. AE61-0363

15 May 1961

Contract NAS 5-304

Volume V
IMPLEMENTATION PLAN
Book 2
RELIABILITY

Prepared by:

CONVAIR (ASTRONAUTICS) DIVISION
GENERAL DYNAMICS CORPORATION
and
AVCO CORPORATION

[redacted]

RDF61-026

[redacted]

CONFIDENTIAL

VOLUME I	SUMMARY
VOLUME II	SELECTED VEHICLE DESIGN
VOLUME III	SUPPORTING DESIGN ANALYSES
BOOK 1	FLIGHT MECHANICS
BOOK 2	HEAT CONTROL SYSTEMS
BOOK 3	STRUCTURAL ANALYSES AND MATERIALS
BOOK 4	PROPULSION AND AUXILIARY POWER
BOOK 5	TRACKING, COMMUNICATIONS AND DATA SYSTEMS
BOOK 6	GUIDANCE AND CONTROL
BOOK 7	AEROSPACE MEDICINE AND RADIATION
BOOK 8	ENVIRONMENTAL CONTROL AND LIFE SUPPORT
BOOK 9	HUMAN FACTORS
BOOK 10	RELATED CONFIGURATION STUDIES
VOLUME IV	GROWTH AND ADVANCED CONCEPTS
VOLUME V	IMPLEMENTATION PLAN
BOOK 1	SYSTEMS ANALYSIS, SCHEDULES AND COSTS
BOOK 2	RELIABILITY
BOOK 3	DEVELOPMENT PROGRAM
BOOK 4	MANUFACTURING PLAN
BOOK 5	SUPPORT OPERATIONS

TABLE OF CONTENTS

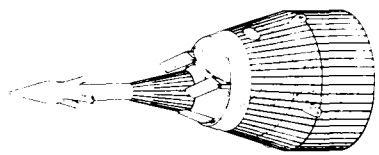
Section		Page
1	INTRODUCTION	1
2	MISSION RELIABILITY REQUIREMENTS AND APPORTIONMENTS	3
2.1	GENERAL	3
2.2	ANALYTICAL APPROACH AND METHODS	3
3	APOLLO SYSTEM RELIABILITY	7
3.1	STRUCTURES RELIABILITY	7
3.2	SUBSYSTEM RELIABILITY	7
3.2.1	Propulsion	7
3.2.2	Auxiliary Power	8
3.2.3	Electronics	9
3.2.4	Abort, Landing, and Recovery	15
3.2.5	Life Support	16
4	RELIABILITY PROGRAM PLAN	17
4.1	ROLE OF RELIABILITY	17
4.1.1	Planning and Milestones	17
4.2	RELATIONSHIP OF RELIABILITY TO SYSTEMS DESIGN, MANUFACTURING, AND TEST	18
4.3	COMPONENTS TEST	21
4.4	FLIGHT TEST	21
5	MATHEMATICAL MODELS	23
6	DATA SYSTEM	25
7	MAINTAINABILITY	27
8	PRODUCIBILITY	29
9	QUALITY CONTROL	31
10	RELIABILITY REQUIREMENTS DOCUMENTATION	33
11	RELIABILITY PROGRAM MANAGEMENT	35
	REFERENCE	37

LIST OF ILLUSTRATIONS

Figure		Page
1	Possible Paths of VHF Operation	12
2	Systems Engineering Creative Process; Flow Diagram	18
3	Systems Design Engineering; Information Flow Diagram	19
4	Detail Design; Flow Diagram	20
5	Fabrication and Test; Flow Diagram	20

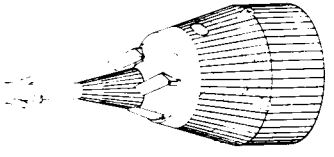
LIST OF TABLES

Table		Page
1	Reliability Goals and Apportionments	3
2	Preliminary Predictions of Communication Subsystem Reliability	10
3	Sampling Plan for the Combined Reliability and Production (CRP) Test Program	21



1 INTRODUCTION

This book describes the reliability effort for the Apollo program. The fact that Apollo vehicles will be manned makes it important that a high level of confidence be achieved in the probability of successful mission completion. In order to develop this confidence level, it would be ideal to perform a considerable number of flight tests. However, the extremely high cost of the booster and the Apollo vehicle precludes an extensive flight test program and it becomes necessary to achieve high mission reliability through the utilization of a systems approach to analytical reliability measurement and improvement during the predesign and later design stages. At the onset of the Apollo study program, preliminary system reliability requirements were established in concurrence with initial system performance guidelines to meet the overall mission objectives. During this effort, detailed design trade-off studies were conducted to integrate reliability goals without jeopardizing performance objectives. Reliability estimates, using applicable methods and actual or extrapolated data on physically or functionally similar systems, subsystems, and equipment, were used. The resulting trade-offs for improved reliability are therefore considered to be valid. Redundancy was used where practical, and the crew was evaluated as a redundant sensor, computer, and control element in guidance, flight control, energy utilization and life support systems.



2 MISSION RELIABILITY REQUIREMENTS AND APPORTIONMENTS

2.1 GENERAL. The Apollo design mission of orbiting the moon and returning to earth is scheduled for 1967. The preliminary mission reliability objective of 0.878 was established on the basis of analysis of each major subsystem. Table 1 summarizes the reliability goals and apportionments for the Apollo vehicle. The analysis is described in section 3.

Table 1. Reliability Goals and Apportionments

Subsystem Description	Major Component Reliability	Subsystem Reliability
Abort		0.992
Auxiliary Power		0.976
Electric	0.998	
Hydraulic	0.990	
Pneumatic	0.985	
Controls		0.971
Guidance	0.988	
Attitude Control	0.990	
Velocity Control	0.990	
Communications		0.985
Voice Link	0.995	
Tracking	0.993	
Landing and Recovery		0.985
Life Support		0.995
Crew Support		0.995
Propulsion		0.990
Structure		0.990
Overall Lunar Mission Reliability		0.878

2.2 ANALYTICAL APPROACH AND METHODS. The following assumptions, based on engineering design data, historical reliability data, extrapolation of normal growth curves, analysis of environment interaction, analysis of human interaction and criticality determination were made in order to develop reliability figures for Apollo:

a. Reliability experience data on major components can be extrapolated using historical reliability data on the same or similar components and a fitted exponential growth curve; new developments lower the curve during the development and early operational period, after which it would rapidly, asymptotically approach the original curve.

b. Reliability growth of major subsystems is limited by the occurrence of random failures at the following values:

Simple subsystem	0.992
Medium complexity subsystem	0.985
High complexity subsystem	0.971

c. For ease of handling in the preliminary analysis, the reliability of a subsystem is the product of the major component reliabilities, a weighting factor for criticality, and other factors introduced by the crew interaction. These are:

1) Redundancy factor for crew as control sensor element;

2) Redundancy factor for crew as control computer and decision element;

3) Redundancy factor for crew as control operation element;

4) Redundancy factor for crew as maintenance element; and

5) Unreliability factor for crew causing malfunction or failure.

Analysis of reliability in this program was accomplished in these steps:

a. Each subsystem was examined to determine its function, operation, material flow, signal flow, control flow, major components, criticality of malfunctions and off-tolerance performance.

b. Major component reliability was derived by extrapolating applicable reliability experience on same or similar components for mid-1964, mid-1965 and mid-1967, corresponding to initial test flight program, sub-orbital and orbital test flights, and lunar flights, respectively.

c. Effects of environments to which the major component will be subjected in the lunar mission were evaluated for effects on component reliability.

d. Subsystem reliability was determined using the product rule, for the dates of mid-1964, mid-1965, and mid-1967.

e. Effects of the crew interaction on subsystem reliability was analyzed by deriving the following factors:

1) Man as a cause of subsystem malfunction or failure;

2) Man as a redundant control computer and decision element;

3) Man as a redundant control sensor element;

4) Man as a redundant control operation element; and

5) Man as a maintenance element.

f. Total subsystem reliability was determined by combining the results of (d) and (e) above.

g. Mission reliability was determined by analyzing the overall system reliability throughout the mission, by combining the reliabilities of the operating subsystems through the different phases of the mission and multiplying by weighting factors based on the operating phase duration.

Equations used in the reliability analysis are:

Growth curve fit $\quad R = 1 - e^{-at}$

This curve is used to extrapolate historical reliability data of major components.

Given historical data:

$$\text{reliability} = R_1 \text{ at date } (t_0 + t_1)$$

and

$$\text{reliability} = R_2 \text{ at date } (t_0 + t_2)$$

$$R_2 > R_1 \; ; \; t_2 > t_1$$

Values for at_1 and at_2 can be found in standard exponential tables. To determine the value of a, we start from the identity:

$$(at_2)t_1 = (at_1)\, t_2.$$

Solving for t_1, $t_1 = \dfrac{at_1}{at_2}\, t_2$

and $\quad \Delta t = t_2 - t_1 = t_2 - \dfrac{at_1}{at_2}\, t_2 = t_2 \left(1 - \dfrac{at_1}{at_2}\right)$

Solving for t_2, $t_2 = \dfrac{\Delta t}{1 - \dfrac{at_1}{at_2}}$

Therefore, $\quad a = \dfrac{(at_2)}{t_2}$.

Date for R_2 is $(t_2 + t_0)$, and the

Date for $R = 0$; $t_0 = \left(t_2 + t_0\right) - t_2$

therefore the reliability at any date $\left(t_0 + t_3\right)$

is $\quad R_3 = e^{-a(t_0 + t_3)}$.

Any subsystem consists of major elements for which a reliability value can be calculated for specific dates. The reliability of the subsystem is equal to the product of the major component reliabilities.

$R_{A,\,B,\,C,\,D\,..N}$ = reliability of major components

R_{SS} = reliability of subsystem

$$R_{SS} = R_A \times R_B \times R_c \times R_D \ldots R_N$$

For the case of a completely redundant system of two major operational components where only one is required to operate adequately and where the malfunction of one component does not affect the performance of the other, the following equation applies:

$$R = 1-(1-R_{1A})\ (1 - R_{1B}),$$

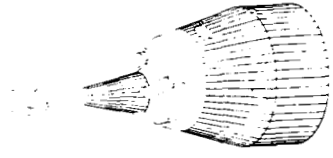
where R_{1A} and R_{1B} are the reliabilities of each component.

For the case of duplicate third components redundant to each other in a chain of four units:

$$R = R_1 \times R_2 \times \left[1 - (1-R_{3A})\ (1-R_{3B})\right] R_4.$$

For the case of a system using a chain of four major components (R_1, R_2, R_3 and R_4) with a redundancy capability, R_5, of the human operator to perform the functions of R_2 and R_3, and with the maintainability capability of the human to repair R_2, R_3, R_4, and R_6, and if we assign a probability of success for both R_5 and R_6, the applicable equation reads as follows:

$$R = R_1\left[1 - \left\{1 - (1-R_2R_3)\ (1-R_5)\right\} R_4\right]\left(1 - R_6\right).$$



3 APOLLO SYSTEM RELIABILITY

3.1 STRUCTURES RELIABILITY. The three main structures of the vehicle are the main body (mission module), the re-entry vehicle (command module), and the abort tower.

The recommended design is a pressure-stabilized structure which supports the command module and provides a living area with the equipment necessary for the lunar mission. It also supports the attitude, mid-course, and main propulsion engines. The structure is basically a shell with hat section stiffeners welded to titanium sheet material. The command module, occupied by the crew primarily during the boost and re-entry phases of flight, is designed to support three men, control and display equipment, exterior flap controls for re-entry, and the abort tower. The module is constructed essentially of honeycomb stainless steel with insulation and an ablation material on the heat shield for re-entry. The abort tower is jettisoned after first-stage boost. It supports solid-fuel rockets used to safely abort the command module in the event of a major system failure during first-stage boost or before launch. The reliability of these three structures is considered most important, thus special precautions were taken to design a reliable structure with redundancy where possible. This redundancy is provided by using multiple load paths in the structure to ensure system integrity in case of a failure in adjacent structures. Other means used to provide a reliable structure are: 1) the use of materials which have adequate ductility and toughness, which avoids notch sensitivity; 2) the avoidance of stress raisers in design such as notches, holes, sharp radii, or abrupt changes in area; and 3) the avoidance of dissimilar metals which could cause stress corrosion through galvanic action. In addition to these design provisions, it is essential that a high level of production quality control be required and that periodic inspection of the structure be provided for in the field.

The overall reliability of the Apollo structure will probably be high since similar type structures are used successfully in operational missiles. The reliability of the overall Apollo structure is estimated to be 0.983 by mid-1964, 0.985 by mid-1965, and 0.987 by mid-1967.

The reliability of the structure can be further increased by providing for repair of punctures by small meteorites. With this provision and other possible maintenance by the crew, the reliability of the structure is estimated to be 0.985 by mid-1964, 0.987 by mid-1965, and 0.990 by mid-1967.

The command module has atmospheric controls, primary controls and displays for use during take-off, re-entry, post-landing survival, and recovery. Also included are batteries, survival kit, medical kit, flares, lights, dye marker, balloons and communication equipment and multi-directional couch restraints. On the exterior are the antennas, parachutes, inflatable flotation bags, and impact bags.

After re-entry the crew has the capability of releasing the main chute manually as well as releasing the auxiliary chute should the main chute be defective.

Impact attenuation is provided by crushable structures of demonstrable reliability.

Ground landing is to be handled by the parachutes, crushable structure, and impact bags. Water landing will involve the same components plus flotation bags to maintain the optimum attitude.

Post-landing survival reliability is provided by survival kits, medical kits, food and water for three days, and batteries for communication and downrange tracking. Recovery will be by downrange vessels which have locked on to the re-entering vehicle by means of the tracking network.

For purposes of preliminary reliability goals, data were extrapolated from like systems and components using the product rule to arrive at the reliability for 1964. This was estimated to be 0.950. By applying the normal growth curve to this estimate and assuming an intensive effort to increase reliability, the reliabilities for 1965 and 1967 are 0.970 and 0.985, respectively.

3.2 SUBSYSTEM RELIABILITY

3.2.1 Propulsion. The Apollo main propulsion system provides the power for exiting from a lunar orbit and to abort the mission in the post-atmospheric phase, in the event of an emergency. The proposed propulsion system uses Pratt and Whitney XLR-115 engines with 15,000-pounds thrust. Major components include thrust chambers, injectors and igniters, propellant start valves, main propellant valves, fuel and oxygen fill-and-drain valves, boiloff valves, disconnects, and associated plumbing. The propellant tanks are toroidal in shape and are pressurized with helium gas to provide the necessary NPSH for the propellant pumps.

The estimated flight reliability of a turbo pump-fed system (the MA-3) was determined by fitting an asymptotic growth curve to previous flight

data. The estimated static test reliability of a pump-fed system was determined by the actual reliability of the last 100 static firings. Data for a pressure-fed system were obtained from static test data and from extrapolated manned flight data.

The propulsion system reliability was estimated to be 0.93 and 0.98 respectively for the flight and static test data on the pump-fed system. The reliability for the pressure-fed system was estimated to be 0.97.

Since the MA-3 propulsion system consists of a booster engine with two thrust chambers, two vernier engines, and a sustainer engine, another adjustment must be made in their reliability data to make it comparable to the single thrust-chamber Aerojet engine. This adjustment would raise the reliability for a single MA-3 engine.

It was concluded that the reliability data for the two systems were not significantly different in magnitude, considering the differences in ground rules, to justify a clear choice in the type of system based on these data. Since it was shown by these data that either system would obtain a high reliability, the turbo pump system was chosen because of its better performance and reduced weight advantages.

Due to the importance of successful operations of the main propulsion system, a further increase in reliability was considered necessary, and thus a system trade-off was effected to provide for a completely redundant propulsion system, except for the propellant tank itself. This engine would be required to fire along with the other engine if a mission abort was required in the post-atmosphere area to provide sufficient thrust, but the second engine would be redundant for the insertion and exit from lunar orbit, which would better provide for the crew's safe retrun. An analysis of this is given in Book 4 of Vol III.

The proposed Pratt and Whitney engine is currently being used on the Centaur program. At the expected time of the first flight requirements on this propulsion system, this engine will have accumulated considerable flight experience. In addition, it is recommended that if this engine is used, Pratt and Whitney company should be allowed to conduct a proposed reliability test program in addition to the Centaur reliability tests to demonstrate a reliability of 0.975 with a 90 percent confidence by April 1963. If this reliability level is obtained, the redundant engine should make the propulsion system most desirable.

The overall reliability for the propulsion system in meeting the lunar trajectory requirements is estimated to be 0.975 by mid-1964, 0.985 by mid-1965, and 0.990 by mid-1967.

The vehicle crew will probably not be able to add significantly to the reliability of the propulsion system because the main engine will be controlled automatically for both insertion into and exit from lunar orbit and/or for abort.

3.2.1.1 Attitude Control Propulsion. The function of the attitude control subsystem is to provide pitch, roll, and yaw control for the Apollo vehicle throughout its mission duration. It consists of 12 fixed nozzles (two clusters of four and two clusters of two) distributed around the periphery of the mission-module aft adapter ring. The system utilizes fuel tanks, oxidizer tanks, nozzles, and interconnecting components (valves, solenoids, controls, and plumbing). Some redundancy is provided in the propellant supply system. A degree of manually controlled operation is possible.

Reliability figures on similar present-day subsystems is 0.90; however, with continued flight test programs this will increase to 0.98 by 1964, 0.985 by 1965 and 0.990 by 1967.

3.2.1.2 Midcourse Velocity Correction. The function of this subsystem is to effect midcourse velocity corrections. The four engines fire in pairs or simultaneously, depending on the maneuver required. The propellant system is common to the attitude control system. The reliability of similar existing systems is 0.90; however, this will increase to 0.98 by 1964, 0.985 by 1965 and 0.99 by 1967.

3.2.2 Auxiliary Power

3.2.2.1 Electrical. The major components of these subsystems are the O_2/H_2 fuel cell, two 28-VDC batteries, solar cells, voltage regulators, radiator, heat exchanger, power changeover switch, and cabling.

Components of the electrical subsystems are of proven design and many are off-the-shelf items with high reliability and long use history. The environments to which these components will be subjected will have little effect on their reliability. In manned flights, subsystem reliability will be increased slightly since the voltage sensors will have mechanical overrides in the event of failure in the primary subsystem.

Preliminary subsystem reliability was derived by extrapolating data of similar systems, using the product rule and sound engineering judgment.

The reliability estimated for 1964 is 0.988. Applying the normal learning curve to these data, reliability is estimated at 0.995 by 1965 and 0.998 by 1967.

3.2.2.2 Hydraulic. The Apollo hydraulic system actuates four flaps on the command module. The flaps function as aerodynamic flight-control surfaces during and after re-entry. The flaps are operated by hydraulic actuator assemblies controlled by means of conventional electromechanical servo valves attached to the actuators. Signals to the servo valves will be received from the Apollo guidance and control system.

The proposed hydraulic system will consist of four hydraulic actuator assemblies (one for each flap), an accumulator, a reservoir, four valves, a filter, and a piston-type hydraulic pump driven by an electric motor.

The pump supplies fluid to the accumulator against a pneumatic pressure head. When a pulse of power is needed for the flaps the accumulator supplies the necessary pressurized fluid. Between power pulses the pump replenishes the accumulator for the next cycle of operation.

Reliability of the individual components and subsystems should match that of components used successfully on similar systems. Based on existing reliability data, an estimated reliability of 0.98 is expected for mid-1964, 0.985 for mid-1965, and 0.99 for mid-1967 for the Apollo vehicle.

The presence of man onboard will not be significant in the operation or maintainence of the hydraulic system.

3.2.2.3 Pneumatic. The pneumatic subsystem provides regulated helium from storage bottles for propellant tank pressurization, attitude controls, propellant expulsion, and engine control pressure. It is anticipated that hydrogen gas bled from the engine will be used for fuel tank pressurization after engine start to reduce helium requirements. The pneumatic subsystem makes use of existing components, or modifications thereof. Consequently, component reliability data are available from current missile programs.

The major functions of the subsystem components, listed in the order of their mission criticality, are:

a. Engine-start propellant-tanks pressure regulation;

b. Propellant-tanks pressure-regulation and venting;

c. Propellant-tanks helium-to-hydrogen pressurization changeover;

d. Engine-controls and attitude-controls propellant expulsion regulation; and

e. Helium storage.

Experience indicates a reliability of 0.913 for a similar 1960 pneumatic subsystem which has narrower tolerances and higher performance re-requirements for regulation and venting. Therefore, it can be expected that the reliability of the Apollo pneumatic subsystem will be 0.975 in mid-1964, 0.982 in mid-1965, and 0.985 in mid-1967.

Not included in these reliabilities are the effects of zero g and of man on the failure rate, either as a redundant control operation element or as a maintenance element. These effects will be reflected in the subsystem reliability when more information becomes available during Apollo design.

3.2.3 Electronics

3.2.3.1 General. Preliminary predictions of the reliability of various electronic subsystems are summarized in Table 2. These statistical predictions represent probabilities of survival for the various equipment items during the required operating time. The predictions are based on present tentative circuitry in some cases and on circuitry of similar existing equipment in other cases. The failure rates are from standard failure rate sources such as RCA TR 59-416-1, "Reliability Stress Analysis For Electronic Equipment" and are based on presently expected levels of thermal and electrical stresses. The reliability predictions are derived from the failure rates according to the relationship:

$$R = e^{-\lambda t}$$

with

λ = failure rates in failures per hour

t = required operating time in hours.

Where an identical standby unit is provided, to be switched on after the first unit has failed, the reliability of this series redundancy configuration is given by:

$$R = R_1 + \lambda t R_1, \text{ where } R_1 = e^{-\lambda t}.$$

The reliability of a series grouping of equipment or circuits is given by the product of the individual reliabilities, taking into account any redundancy.

Table 2. Preliminary Predictions of Communication Subsystem Reliability

Circuit	Failure Rate (%/1000 Hours)	Required Operating Time (Hours)	Reliability (No Redundancy)	Reliability (Redundant Circuit)
Prime Communication & Tracking				
Receiver (including noise ranging and BPF)	17.8	360	0.938	0.998
2-KMC Transmitter	3	360	0.989	0.9999
Power Amplifier	8.1	360	0.971	0.999
C-Band Beacon	72	2	0.999	*
Total circuit reliability (with present redundancy): $R_C = 0.996$				
Telemetry				
Commutation	32	360	0.9999**	
Data Selection	8.4	360	0.970	0.999*
A/D Converter	13.9	360	0.951	0.999*
Up Telemetry Unit	9	360	0.968	0.999*
Tape Recorder	10	360	0.964	0.999
Shift Register	1	360	0.996	0.9999*
Total circuit reliability (with present redundancy): $R_T = 0.888$				
Rescue Communications				
HF Transmitter/Receiver	7.6	72	0.994	0.9998*
VHF Transmitter/Receiver	18	72	0.987	0.9997*
UHF/HF Beacon	1	72	0.999	*
Total present circuit reliability: $R_R = 0.979$				
Re-entry Navigation				
DME Equipment	35	0.25	0.9998	*
VOR Converter/Indicator	2	0.25	0.9999+	*
Marker Beacon Receiver	6	0.25	0.9999+	*
Total circuit reliability: $R_N = 0.9998$				

Table 2. Preliminary Predictions of Communication Subsystem Reliability (Continued)

Circuit		Failure Rate (%/1000 Hours)	Required Operating Time (Hours)	Reliability (No Redundancy)	Reliability (Redundant Circuit)
Spacecraft Electronic Subsystem (with present redundancy)					
Prime Communications & Tracking	$R_C = 0.996$				
Telemetry	$R_T = 0.888$				
Rescue Communications	$R_R = 0.979$				
Re-entry Navigation	$R_N = 0.9998$				
Total Subsystem Reliability:	$R = 0.865$				

* Redundancy not provided at present
** Probability that no more than two channels will fail.

Each prediction in Table 2 represents the theoretical limit of reliability of that equipment or circuit; the prediction assumes complete debugging of possible design weaknesses, taking into account every aspect of the intended environment. Complete debugging of each production unit with respect to workmanship and possible marginal parts is also assumed. The extent to which this theoretical limit is approached should be determined by testing prior to flight.

Some equipment will be used in many phases of the program. Therefore, the reliability of each spacecraft equipment has been calculated according to the maximum required operating time of that equipment, which represents a worst-case reliability prediction.

The spacecraft reliability requirement at present for operating properly for the duration of the mission is 0.91. The spacecraft electronic subsystem reliability requirement may be approximated by:

$$\sqrt[6]{0.91}$$

or 0.985, since there are six subsystems. During the course of the program it should be determined whether certain subsystems could be allocated a greater or lesser portion of the overall requirement. For the present, however, this preliminary allocation is useful.

Within the spacecraft electronic subsystem, tentative goals have been allocated as follows:

Prime communications and tracking	0.993
Telemetry	0.993
Rescue communications	0.999
Reliability product:	0.985

These goals serve as guides in meeting the overall requirement of 0.985. The goals will be revised, as necessary, during the development program to reflect more precise trade-offs as to mission objectives and relative weights, performance, and power requirements of subsystem equipment.

From Table 2, it is seen that the preliminary reliability prediction for the total spacecraft electronics, for the design mission requirement, is 0.865. If redundant circuits are used, the electronic subsystem reliability estimate would be given by the product of the redundant reliabilities shown in the right-hand column of Table 2, which is 0.991. This reliability includes prime communications and tracking, telemetry, rescue communications, and re-entry navigation.

Calculations of the suggested redundancies indicate that the reliability requirement can be met by the proposed subsystem, using additional re-

dundancy. Where weight and space requirement indicate that redundancy must be kept at a minimum, consistent with the reliability requirement, redundancy of individual, critical circuits should be considered in contrast to redundant standby equipment. Standard restrictions on methods of providing reliability for space electronic components must be re-assessed for equipment in a manned spacecraft. The reliability requirement for Apollo must be met without benefit of normal onboard repair and for mission times of one or two weeks, during which time crew members may have considerable free time. The feasibility of the crew's performing minimal onboard troubleshooting and repair should be considered whenever it can be achieved at no cost, since inherent reliability is greatly enhanced.

3.2.3.2 Communication

3.2.3.2.1 Vehicle Subsystems. Independent selection of one of two transmitters, one of two receivers, and one of two power amplifiers provides for the possible paths of UHF operation shown schematically in Figure 1. Therefore, each of these equipments is provided with series redundancy. The reliability prediction for each is calculated and illustrated for the UHF transmitter:

$$R_1 = e^{-(3)\,(360)\,10^{-5}} = e^{-0.011} = 0.989$$

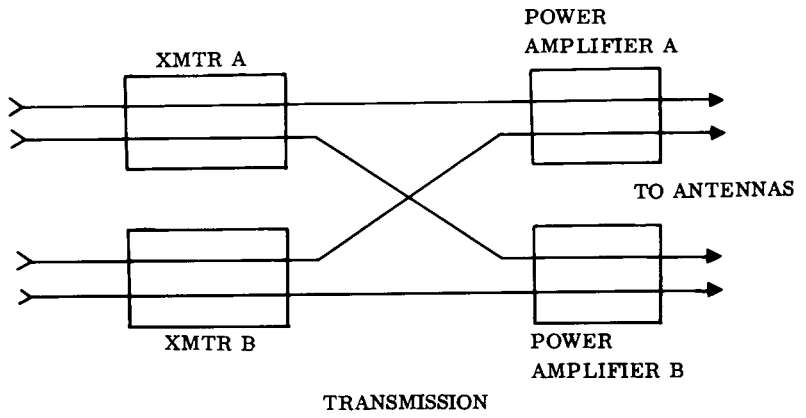
and, with series redundancy,

$$R = 0.989 + (0.011)\,(0.989) = 0.9998.$$

For each receiver, the noise-ranging circuitry is included in the failure-rate estimate because the present block diagram indicates that some failure modes of a noise-ranging circuit could cause the receiver packaged with it to be inoperative. For each type of equipment, the failure-rate estimate includes the manually operated switches used for selecting the equipments.

It is seen from Table 2 that the spacecraft prime communications and tracking equipment meets its present reliability goal of 0.993. This might be improved by providing cross switching of the ranging circuitry between transponders.

3.2.3.2.2 Ground Station Equipment. Two types of availability predictions can be made when sufficient information is available on the ground stations (discussed in a later section). From experience to date on similar ground equipment, an order of magnitude guess of achievable interval



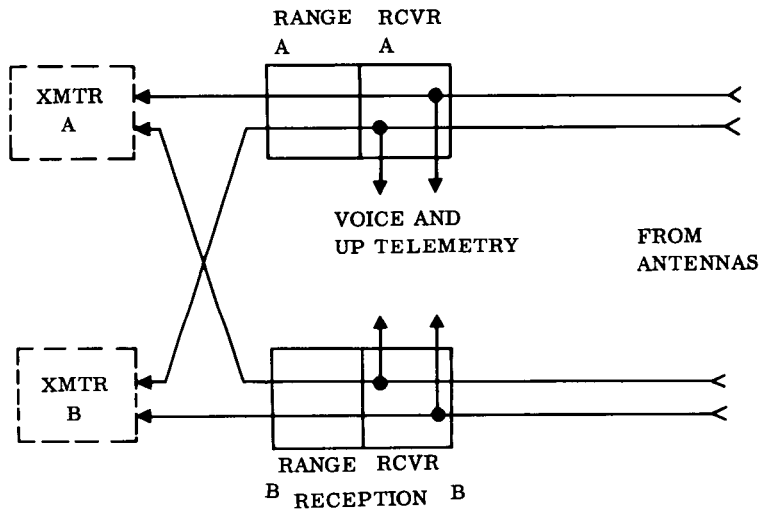


Figure 1. Possible Paths of VHF Operation

4) planned stocking of spare parts. A comprehensive field reliability availability for a three-station ground system would be from 90 to 95 percent.

Most previous experience has been with Earth orbits, involving relatively short durations followed by nonoperational periods sufficiently long for most repairs. For lunar missions, however, since failures would occur during passes eight-hours long, most repair time would interrupt operational time. Therefore, ground station availabilities can be expected to be lower for lunar missions than for Earth orbits.

It is necessary that quantitative estimates of mean times between failures and mean times to repair be made for all ground equipment early in the program to allow time for optimum reliability improvements to be designed into the ground complex where needed. For such estimates to be valid, it is essential that a comprehensive field reliability reporting system be started for the ground stations immediately, even though the final configuration of a given station may not be operational for several years. This reporting system should include operating time, failure data, and repair data. Much of the failure data and mean time to repair data can be extrapolated from present configurations. This data, in conjunction with standard prediction techniques, can give approximate availability numbers early in the program. These figures will take into account the number of stations and the amount of overlapping coverage involved, and the antenna redundancy provided for DSIF stations.

Although a ground system reliability requirement has not yet been established, this should be done as soon as possible in order to assure that the ground system availability will be in keeping with the overall program objectives and with the high reliability requirements of the spacecraft equipment. A statement of the maximum allowable period of time for interruption of ground equipment by repairs, should be included in this requirement.

As discussed previously, normal operations could continue even if noise-ranging was inoperative. Therefore, it would be desirable for ground stations to have the capability to bypass their noise-ranging equipment so that tracking and communications could continue while it was being repaired.

From failure data, repair data, and theoretical failure predictions, a detailed reliability program can be planned to assure that the ground system will meet its availability requirement. The major approaches of this program will be: 1) scheduled preventive maintenance during nonoperational periods, 2) redundancy of critical circuitry, 3) optimum packaging of critical circuitry for ease of repair by such means as plug-in modules, and reporting program will continuously update the availability figures, providing a check on whether the equipment is achieving its availability requirement. A month by month plot of availability will indicate when debugging is complete, at which time it can be determined whether further redesign is necessary.

3.2.3.2.3 One-Way Links

3.2.3.2.3.1 Ground to Space Communications. At present, it appears that an interruption in ground equipment operation, until completion of repairs or until another station takes over, can be tolerated. Therefore, the preliminary reliability prediction for the ground-to-space prime communication link does not include the ground equipment. The spacecraft UHF receiver, including noise-ranging circuitry and a band pass filter, has a predicted reliability of 0.998. When sufficient information is available on the ground equipment, this figure will be qualified by the statement that the link will be available, until failure, for an expected percentage of time as given by the interval availability figure for the ground transmission equipment.

3.2.3.2.3.2 Space to Ground Communications. The preliminary reliability prediction for the space-to-ground link does not include the ground equipment. From Table 2, it is seen that the product of the prime communication transmitter redundant reliability and the power amplifier redundant reliability is 0.999 which, therefore, is the preliminary prediction for the prime communication space-to-ground link. This prediction will later be qualified by the interval availability estimate for the ground receiving system.

3.2.3.2.4 Rescue Communications. From Table 2, the rescue equipment reliability is seen to reduce the overall reliability prediction more than the prime communications equipment does. At present, the rescue equipment reliability is calculated for a required operating time of 72 hours for each of two transmitters, each of two receivers, and for the beacon.

To improve the reliability of the rescue equipment, the optimum approach from the standpoint of reliability would be the use of standby redundant units for each transceiver, although not for the beacon. From Table 2, these standby units would increase the reliability of the rescue equipment to a figure given by the product of the individual reliabilities (0.999), including redundancy, where used.

3.2.3.2.5 Early Flight Communications. It is expected that for Earth orbits there will be a maximum average communication equipment opera-

tion of 20 minutes per each 94-minute orbit. For a possible one month mission this would be about 150 hours of operational time for communication equipment. From Table 2 it is seen that the prime communication equipment for early flights would have a reliability given by the product of the separate redundant reliabilities (0.9998) if series redundancy were provided for the transmitters and for the receiver.

3.2.3.3 Tracking

3.2.3.3.1 Vehicle Subsystems. The minimal spacecraft requirement to ensure availability of tracking data to the crew is operation of the communication system and ranging circuitry; if the onboard telemetry equipment were operative, tracking data could be transmitted from the ground via the voice link, which is independent of the telemetry equipment. Therefore, the reliability prediction for the spacecraft noise-ranging equipment is given by the prediction for the spacecraft prime communication system, including ranging circuitry.

3.2.3.3.2 Ground Equipment. The availability figure for the pseudo noise-ranging ground equipment will be approximately that for the communication ground system. (Refer to Reference 1 for a complete definition of the term "availability.") When sufficient information is available on ground equipment circuitry, and on the number and locations of tracking stations, two types of availability predictions can be made for the tracking ground equipment. Pointwise availability is the probability that the equipment will operate satisfactorily at a specified instant of time. This figure will be useful if it is determined that there are one or more points during the mission for which a minimum reliability requirement should be specified for ground equipment. Interval availability is the expected percent of satisfactory operation during any specified operating period. This figure will be broken down into the major phases of any mission, as for example: launch to injection, midcourse, re-entry, and abort.

3.2.3.3.3 Special Considerations. If noise-pseudo-ranging became inoperative, angle tracking would still make communication possible. Therefore, a switching means to bypass the spacecraft noise-ranging circuitry, in the event it failed, is being considered. At present, it appears that if noise ranging were inoperative, the mission could still be successful, based on the expected accuracy of onboard navigation. The proposed switching means would include an individual power disconnect for the ranging circuitry, in case the failure mode were a power short.

To date, no distinction has been made between the reliability requirements for the ranging equipment and for the communication equipment. However, since it now appears the mission could be successful without noise ranging, an effort should be made early in the program to allocate separate reliability goals for these two functions. If the two goals are substantially different, requiring different degrees of redundancy, then this difference should be considered in subsystem trade-offs involving weight, space, performance, and reliability.

The methods for improving tracking equipment reliabilities are, in general, those discussed for the communication system. However, the C-band tracking airborne package could require a special reliability solution if it uses a magnetron. With a failure rate of 40%/1000 hours, this part would probably constitute the major portion of the failure rate of the airborne package. Therefore, the feasibility of carrying an onboard spare magnetron should be considered early enough in the program so that the equipment could be designed for easy magnetron replacement. At present, it appears there will be no other individual parts in the spacecraft electronics (with the possible exception of the Klystron tubes) for which onboard spares would be justified.

In addition to the possibility of bypassing the noise-ranging circuitry, the feasibility of cross switching the noise-ranging circuits from one transponder to the other is being considered to maximize effectiveness of the redundancy provided for the spacecraft transponder.

3.2.3.4 Telemetry. The preliminary reliability prediction for the spacecraft telemetry system is a 0.888 probability of survival for the maximum required operating time of 360 hours. This prediction allows for the loss of no more than two individual channels. Redundancy is needed to meet the present reliability goal of 0.993.

For purposes of the prediction, the circuitry was divided roughly into four parts: commutation, tape recorders, up-telemetry unit, and critical circuitry. The critical circuitry, in which one failure anywhere could cause complete loss of telemetry, includes the analog-to-digital converter, the data selection circuits, and the output shift register.

The commutation circuitry has an estimated failure rate of 32%/1000 hours and involves about 200 channels, a failure in any one of which would not affect the others. From:

$$P = \sum_{i=o}^{i=n} \frac{(e^{-\lambda t})(\lambda t)^i}{i!}$$ where n = failures,

(values for which are tabulated in "Poisson's Exponential Binomial Limits," by E. C. Molina) it is seen that the probability of no more than two channels failing in this circuitry in 360 hours is 0.9999+. Assuming that failure of two channels would be tolerable, this portion of the telemetry unit is a negligible reliability risk. Also, redundancy can be provided for the most essential channels.

Lacking detailed information on the tape recorders, a failure rate of 10%/1000 hours is assumed for purposes of the preliminary estimate. This figure will be revised as more information becomes available. Series redundancy is provided for the tape recorders, since if one recorder failed the other could handle the required data.

Although the tape recorders and the up-telemetry unit are included in the telemetry reliability prediction, they are not vitally essential to the telemetry system. The loss of both tape recorders would mean the loss of telemetry data obtained during the times transmission is not possible. At present, it appears this would not endanger the success of the mission. Similarly, the loss of the up-telemetry unit would not affect the rest of the telemetry system, and the mission could still be successful because vital up-telemetry data could be transmitted to the crew by the voice link.

At present, it appears feasible to provide individual backup units for some sections of the circuitry. These standby units could be switched-in manually or by up-telemetry command. If redundancy were thus provided separately for the analog-to-digital converter, the up-telemetry unit, the data selection circuits, and the shift register, then from Table 2 the telemetry equipment reliability prediction is given by the product of the redundant reliabilities of the individual circuits (0.996), which meets the present goal of 0.993.

3.2.3.4.1 Ground Data Handling. In determining the availability estimates for ground equipment for communications and tracking, equipment providing data handling functions essential to tracking must be included in the calculations. It should be noted that, in general, the ground data handling is not essential to the means of communication, but only to the content of the communications.

At present, it appears that interruptions of ground data handling for repairs, and the consequent interruption of telemetry reduction and computation of up-telemetry information, will not endanger the success of the mission.

In order that ground equipment availabilities be consistent with the objectives of the program, however, ground data handling equipment must be analyzed as to an order of priority of its functions. Then, equipment design must allow for the required redundancy of circuitry for the most essential functions. Also, the reliability of these functions should not be dependent on equipment which operates primarily on less essential data.

3.2.3.5 Guidance. The guidance system operates continuously for launch, injection, lunar and earth approaches, and re-entry. Onboard measurements and external tracking provide the necessary data for corrections.

Major components of the system are: 1) the instrument platform which includes the combined planet and star tracker and the infrared horizon scanner, 2) digital computer, 3) ground tracking and trajectory calculations, 4) radar altimeter, 5) sun tracker, 6) sextant, 7) backup inertial reference 8) associated controls and displays, and 9) autopilot, including rate gyros.

Redundancy is provided in the system by the sextant, earth-based tracking, and the backup inertial reference. The sextant provides a secondary method for obtaining position fixes on board. The backup inertial reference is a simple strapped-down guidance system which permits safe return to earth if the instrument platform fails. The reliability of the computer is enhanced by the use of error detection and correction codes.

Basically, the onboard system uses inertial guidance principles; reliability data based on past experience is limited. Based on preliminary estimates of the reliability of individual components, the total subsystem reliability for 1964, 1965, and 1967 was assumed to be 0.965 0.975, and 0.988, respectively.

3.2.4 Abort, Landing, and Recovery. Preliminary component reliability for these subsystems was derived by using the reliabilities of like and similar components, and by extrapolating and applying the product rule. The reliability was found to be 0.988 in 1964. Applying the normal growth curve for the known components in similar subsystems, preliminary reliabilities for 1965 and 1967 can be assumed to be 0.992 and 0.995, respectively. By having a crew in the system loop, reliability can be increased by allowing them to analyze launch conditions from engine ignition to an altitude where a lesser mission could be effected. Using this crew function as a redundant element, plus extrapolation of data from like subsystems, the normal growth-curve estimated reliability for the abort subsystem is assumed to be 0.985 in 1964, 0.990 in 1965 and 0.992 in 1967.

3.2.5 Life Support

3.2.5.1 Ecological Systems. The life support subsystems consist of 540 pounds of water and 93 pounds of dehydrated, hydrated, and concentrated foods; food storage, preparation, and dispensing units; and water storage, transfer, and dispensing units. The atmospheric control system has oxygen and nitrogen distribution, pressurization, circulation fans, purification systems, humidity controls, temperature controls and all necessary valves, regulators and tubing, plus the tankage for storage of O_2 and N_2. The thermal control system includes pumps, heat exchangers, a heat transport fluid, pipes, and necessary valves and controls. Radiation protection is in the form of water-filled garments. Noise insulation is used to limit noise during launch and re-entry. Orbital noise levels are in the 50-60 db range to provide a customized sound background. These features provide the crew with a shirt-sleeve environment.

All critical elements of the life support subsystem include redundant control elements.

Components used in the life support system have been assigned reliability numbers by taking data available on similar components. Reliability in the more severe environment must be assured. Using the product rule, component reliability has been devised to be 0.985 for 1964. Applying a normal growth curve, as extrapolated from other like components, a reliability of 0.988 can be assumed for 1965 and 0.992 for 1967.

3.2.5.2 Crew Support. Pressure suits, multi-directional restraint for boost and re-entry, and sanitation facilities comprise the main subsystems for crew support. Their purposes are to maintain the crew in the event of a cabin leak or meteorite penetration, absorb g loading during take-off and re-entry and provide means for collection and storage of waste.

The waste collection unit is a toilet for the collection and packaging of urine and feces. It consists of a stool, collection bags, mechanical apparatus for holding and closing the collection bags, and a hand-operated air pump used to create airflow from the top of the collection packages to the bottom, thus preventing fecal matter from floating out of the collection packages before they are closed. The urine collection device consists of suitable fittings integral with the feces collection unit, together with plastic bags for urine collection and transfer. A 10-cubic-foot freezer unit is provided for the storage of waste (discarded sponges, feces, etc.,) food, and biological specimens in separate compartments.

The emergency water recovery unit provides for recovery of waste water by vapor compression.

Crew protection against harmful radiation is supplied by water-filled garments. The critical aspect of radiation protection by this device is that actuation depends upon crew knowledge of the radiation hazard. This knowledge is supplied by a radiation warning system. Therefore, reliability of the radiation warning system is of primary importance with respect to crew protection.

Crew support and restraint will be provided by contour seats, while full-pressure suits will be provided as emergency backup to the environmental control system. The pressure suits will provide the crew with a habitable atmosphere in the event of environmental control system failure resulting from meteorite penetration or other causes.

The Apollo mission environments are not likely to affect the components to any great extent except in the case of class-III solar flares, in which event the crew could be seriously injured if subjected to the radiation for any length of time. The subsystems involved are redundant. The vehicle is pressurized but pressure suits are also provided, extra water storage is provided, and vehicle radiation protection is augmented by water-filled personal garments. For many components within the crew support subsystems, man's presence allows a maintenance aspect. The crew can evaluate components such as water purification, storage, food supplies, waste collection, etc. In the event of an out-of-tolerance malfunction, corrective action could be taken. This improves reliability for the subsystem as a whole.

By taking existing data of similar subsystems for use in similar environments, and by applying the crew support subsystem for the year 1964, a preliminary reliability of 0.990 by 1965 and 0.995 by 1967 can be assumed.

4 RELIABILITY PROGRAM PLAN

4.1 ROLE OF RELIABILITY. Reliability is defined as the probability that a product, whether a detailed part or an entire system, will perform its intended function, for the specified time, under the specified conditions. Reliability assessment and improvement for Apollo begins with formulation of the basic system requirements and proceeds through system design, detailed design, prototype production, development testing, operational production, and field use. Considering the fact that men and machines are important elements of the system, the human reliability is as important as the machine reliability.

The drive to complete primary assignments (on-schedule delivery, etc) has always caused a conflict in trying to achieve high reliability in design and production. A comprehensive reliability program must be applied by a departmental management distinctly separate from engineering and production departmental managements. Thus, the product reliability management elements cannot be compromised in their "check and balance" functions.

Integration of reliability for the Apollo requires consideration of the following functional areas:

a. Reliability data;

b. Reliability testing;

c. Specifications and standards;

d. Maintainability;

e. Quality assurance;

f. Quality requirements;

g. Producibility;

h. Inspection;

i. Human reliability;

j. Reliability requirements;

k. Reliability control.

Reliability data, maintainability, producibility, human reliability, reliability documentation, and reliability control are areas in which the most significant developments are expected. They are described in some detail in later paragraphs.

4.1.1 Planning and Milestones. Each product proceeds from a "mission requirement" concept through all the intermediate processes to its end use in its design environment. Some common milestones widely accepted today are system design complete, detail design complete, design review complete, engineering release complete, prototype production complete, prototype testing complete, design proof testing complete, qualification (preproduction) testing complete, start of production, acceptance testing complete, start of delivery, and beginning of operations.

Since the process of proceeding from product concept to end use is step by step, the reliability of the end product in its design environment must develop in the same manner and should be so planned. Each step in each area should contribute something positive to the process or it should be eliminated. Tests should provide answers where none are known, or demonstrate that the product is ready for the next step. These two purposes should never be intermingled in a test program.

A successful reliability assessment and improvement program demands complete preplanning and should have reliability milestones established at each significant step in the progression from concept to end use. Several additional steps are usually desirable, such as programing for design reliability assessment, reliability testing, end-use reliability measurement, and service-life reliability measurement.

In developing the planning for the Apollo program, reliability goals, in numeric form, should be established for each milestone and compared with the most accurate measurements available at the milestone point. This serves two important purposes: 1) items with lagging reliability improvement are brought to light for increased emphasis, and 2) assessment of overall reliability activities indicates program status and effectiveness.

Initially, data must be gathered from various sources on identical, similar, or functionally identical items to establish reliability goals and to support system and detail design efforts. Subsequently, as test data begins to accumulate, a continuous, iterative process can be applied to obtain realistic reliability assessments. Milestones then become specific points in the overall program where significant reliability data becomes available and warrants thorough analysis and review. Such reviews provide a basis for management decisions to shift emphasis from one item to another or from one program area to another. Also, at this point in time, the milestone activities provide management tools to determine where the program stands in terms of the rate of reliability growth and level of reliability.

4.2 RELATIONSHIP OF RELIABILITY TO SYSTEMS DESIGN, MANUFACTURING, AND TEST. The effectiveness of a reliability program may be measured by its contribution to systems engineering. Systems engineering consists of defining an objective, designing equipment systems to accomplish the objective, and demonstrating that the objectives have been met. A reliability program as a part of the systems engineering process defines reliability goals, enters into the design of equipment systems, and demonstrates that its objectives have been met.

The creative process of systems engineering is analogous to a closed-loop control system and can be diagramed as in Figure 2. This applies to many levels of systems engineering, from weapon systems to minor subsystems. There are many feedbacks in the process, but the prime feedback is from testing activities.

The effectiveness of the reliability program is strongly affected by the manner in which the overall system engineering effort is conducted. So much information becomes available that it is necessary to establish a system of channels for the information flow and filters to suppress misinformation. The main flow channels take the form of system specifications which delineate requirements for the next lower level of systems and subsystems. Delineation of the subsystem problems is a partial solution of the system problems.

The problem of filtering the mass of information fed back from testing and other sources is a matter of applying sound analysis and judgment to the data and passing only that which will contribute to attainment of system engineering objectives. As seen in the Figure, these feedbacks are used to re-specify the requirements if a steady state error remains after the system "settled out". Reliability analysis distinguishes "transient errors", which will disappear as the system matures, from "steady state" errors, which will not.

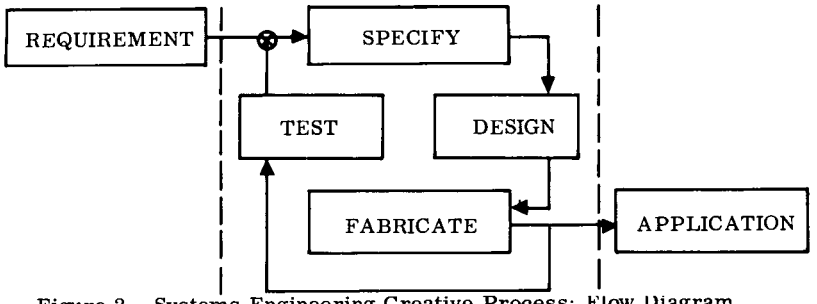


Figure 2. Systems Engineering Creative Process; Flow Diagram

The three blocks in Figure 2 can be further expanded as shown in Figures 3, 4, and 5. Implementation of the reliability program in each of the steps shown in these diagrams is described in the following paragraphs.

Referring to Figure 3, the predesign function is considered to take place between the time of prime contractor selection and the firming up of a model or weapon system specification. The reliability department will participate in establishing a contractual reliability program and will arrive at a preliminary apportionment of reliability goals for the various systems and subsystems.

In the system design phase, reliability engineers will participate in detailed functional analyses of the systems to ensure that proper trade offs are made between reliability, performance, and program costs. Planning of an integrated test program which will produce reliability data along with performance data will take place in this phase. The output will be a set of subsystem specifications in which the reliability requirements for design and testing are spelled out.

In the subsystem design phase, comparative studies of alternative subsystem designs will be conducted and a selection made. Test planning will be expanded. The results of this phase will be in the form of component specifications and design parameters to guide detail design of components. Reliability requirements will be stated in familiar terms. Subsystem trade off studies will be based on optimum de-rating or redundancy to achieve reliability goals.

A reliability engineer will be assigned to each system design team and will participate in all design decisions.

The next major phase is the detailed design which establishes precise instructions for the manufacture of the hardware. This process is illustrated in Figure 4.

Working from component specifications and design parameters generated in the subsystem design phase, final layouts of the equipment are made by design groups. In this phase, some of the equipment is designed in-plant, while other parts are on procurement from suppliers. It is in this phase that reliability is designed into the equipment.

Reliability engineers will work in close association with in-plant designers and the suppliers to ensure reliable designs. Suggestions will be made early enough to be incorporated by the designer before he finalizes his design, thus avoiding late changes.

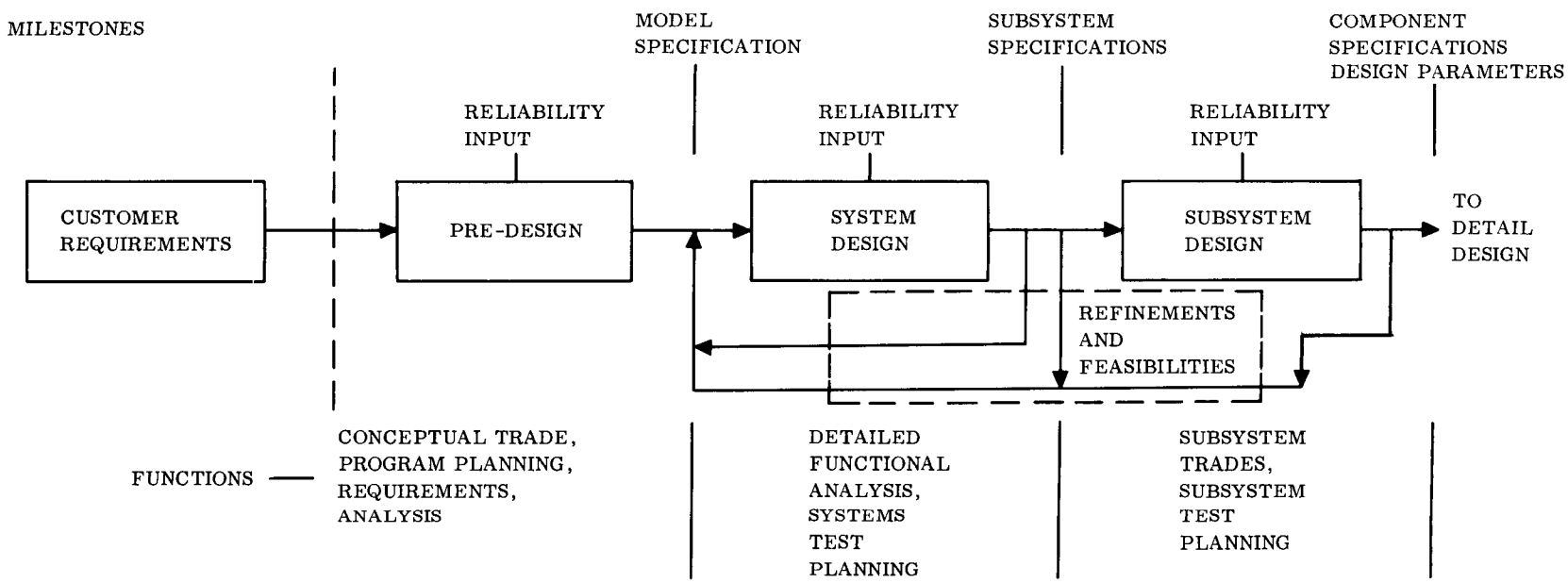


Figure 3. Systems Design Engineering; Information Flow Diagram

In the case of procured items, design approval by the prime contractor will include a required reliability approval.

The next phase involves detail design, preparation of working drawings, and component selection. Many details having an effect on reliability are finalized in this phase. Fits and tolerances, selection of materials and processes, specification of standard parts, lubrication, and corrosion protection are determined.

A final design review covering all reliability aspects will be made before final release of the fabrication drawings. Reliability check lists will be used in examination of detail designs.

To complete the instructions to the manufacturing departments, detailed checkout and proofing procedures are documented to aid in preparing the finished product for operation. These include calibrations, adjustments, and functional check parameters which indicate the tolerances of properly operating equipment.

The final major subdivision of the process of creating a reliable operational system is diagramed in Figure 5. This is the manufacturing and testing phase. Manufacture of prototypes is followed closely or is overlapped by manufacture of production articles.

Quality control checks and tests are performed at each stage of manufacture. Purchased parts are received and checked to standards established by engineering. First articles are given special inspections and tests by the engineering laboratories to determine their acceptability for prototype use. Full qualification testing for production use usually proceeds concurrently with prototype fabrication and test.

It has been customary to fabricate prototypes for static tests, which may be destructive, and for performance testing. The importance of reliability in the proposed system makes it advisable to fabricate an additional prototype for life testing to determine reliability factors. Other critical parts and components should be provided for search-for-critical-weakness testing, which is usually destructive.

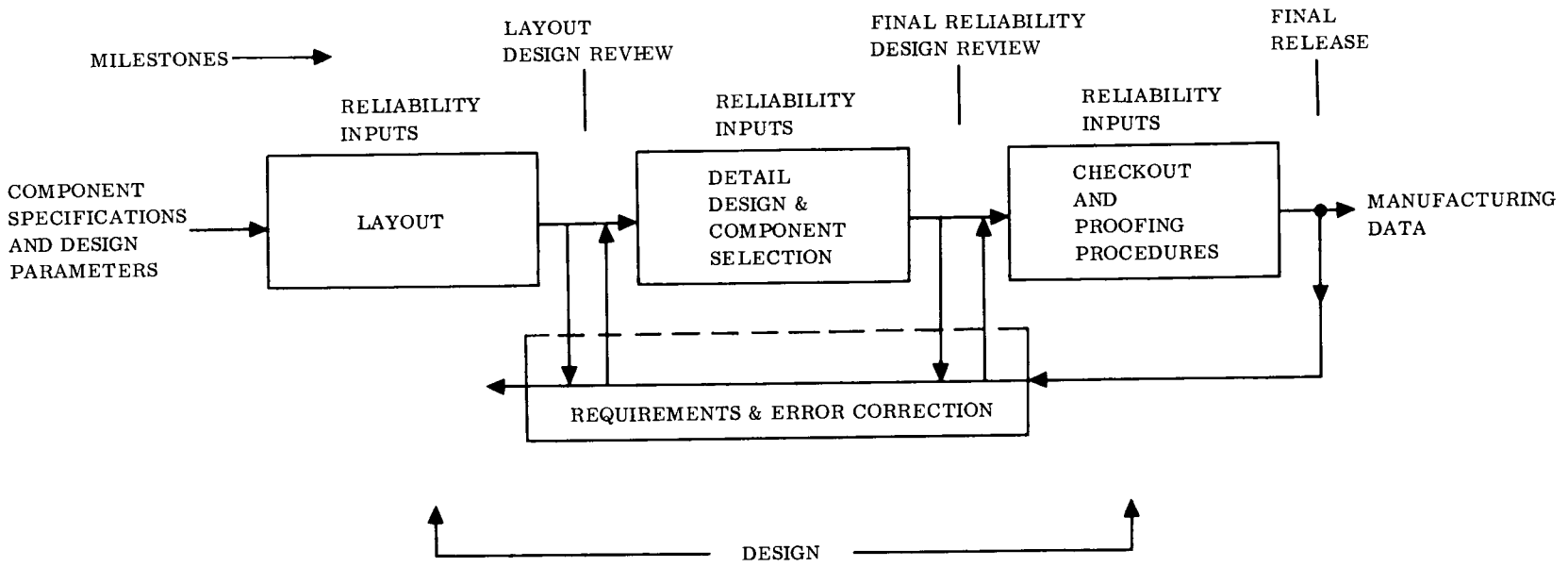


Figure 4. Detail Design; Flow Diagram

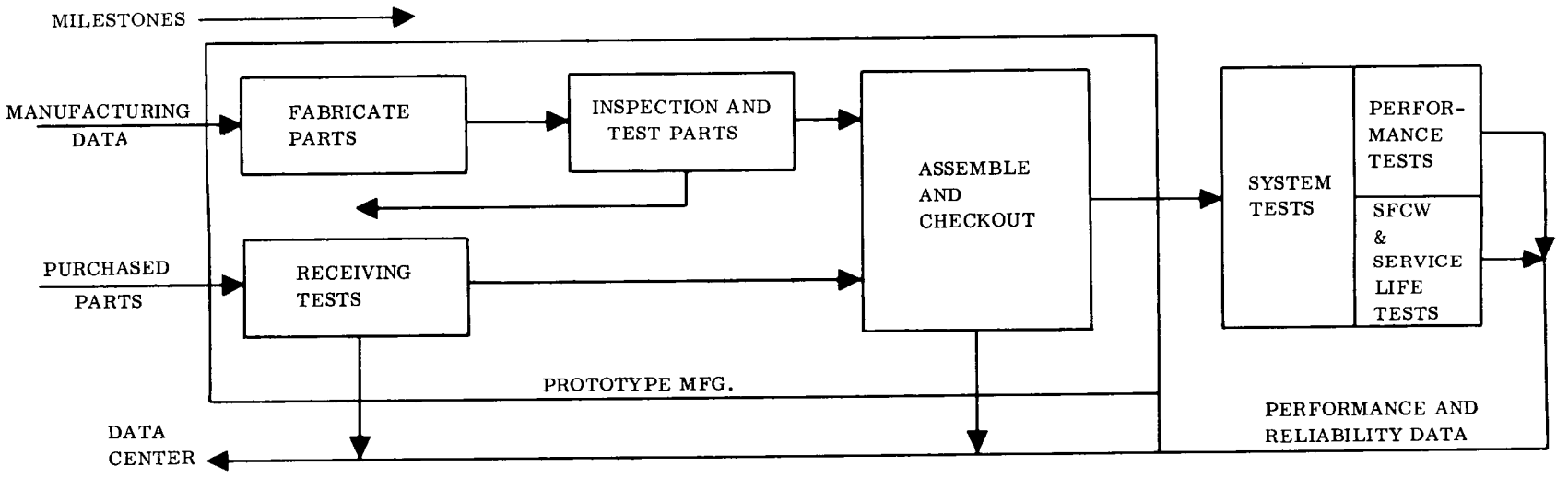


Figure 5. Fabrication and Test; Flow Diagram

Reliability engineers will work closely with quality control and manufacturing personnel throughout the fabrication and checkout phase, gathering data and studying characteristics of the equipment for potential reliability problem area. Information and recommendations are fed back to the cognizant design groups.

Reliability engineers will monitor the performance test programs to obtain reliability information and will direct the life testing and search-for-critical-weakness testing.

The production manufacturing process is similarly conducted as shown in Figure 5. During this phase, emphasis is placed on completing the pre-production test monitoring for reliability information. Where production quantities will not establish an adequate confidence level for the purposes of the program, additional units will be required for reliability tests.

The final step before the system is declared suitable for manned operations is the system evaluation test program conducted by the procuring agency. Further reliability data is gathered in this phase and fed back into design and production at the highest effective level. This process continues, as required, during the operational life of the overall system.

4.3 COMPONENTS TEST. Combined reliability and production component testing for the Apollo program should incorporate three test programs in order to establish central control, reduce cost, and provide an independent evaluation of all critical hardware. This will encompass pre-production tests, product evaluation tests, and reliability search-for-critical-weakness tests.

Environments should be combined to simulate actual service conditions as closely as possible within the laboratory "state-of-the-art". This type of testing during previous reliability programs required less operating time on test specimens, was more economical, and revealed weaknesses that would not otherwise have been detected.

A major critical hardware list should be prepared in coordination with the reliability organization, systems engineering, design and quality control. The components on this list will undergo the combined reliability and production (CRP) test program outlined below.

A minimum of six test specimens for each item on the major critical hardware list should be selected for the CRP test program. This sample size is large enough to reveal any weakness and give a good indication of performance and production variability. Specimens will be selected from production items as shown in Table 3.

The first two production items should be subjected to qualifying tests with combined airborne environments (vibration, temperature, altitude, etc.) on the first unit, and ground environments (transportation, handling, humidity, sand, dust, fungus, etc.) on the second unit. The procedures will be established and the results approved jointly by the reliability organization and the systems engineering section. Satisfactory completion of these tests will permit acceptance of the first 10 production units. The two test specimens used in this part of the program will be subjected to higher levels of environmental intensity later, along with the test specimens mentioned in the next paragraph.

The test specimens selected for IC, II, and III of Table 3 will undergo the standard reliability search-for-critical-weakness (SFCW) test program. This will include combined environmental testing at design-level intensities and two levels beyond. The test units will be required to successfully complete design-level testing to satisfy production monitoring requirements. The two specimens mentioned in the previous paragraph will undergo the two higher levels of environmental testing. Procedures and test results will be approved jointly by the Reliability Organization and Quality Assurance. The sampling plan shown in Table 3 was established to permit the acceptance by production lots, the size of which increases as production advances.

Table 3. Sampling Plan for the Combined Reliability and Production (CRP) Test Program

I. First 10 Production Items:

a. First item--combined airborne environmental pre-production test.

b. Second item--Ground environmental pre-production test.

c. One item from remaining 8--Reliability SFCW test.

II. Next 45 Production Items:

One item from each group of 15--Reliability SFCW tests.

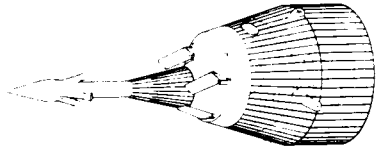
III. All Remaining Production Items:

One item from each group of 25--Reliability SFCW tests.

This program will be initiated when the first pre-production component has been completed and will continue through the first manned flight. This program will remain in effect until the last flight, on a reduced scale, to monitor new or changed components on each flight.

4.4 FLIGHT TEST. Reliability flight tests will be monitored by resident reliability engineers at static and flight test bases. These engineers will

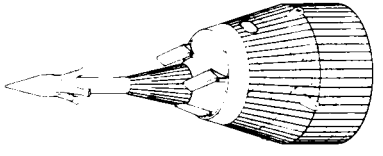
perform preliminary failure analyzes of failed hardware, collect reliability data, monitor Failure and Consumption Data cards and operational life data cards to furnish information to the reliability organization. They will also assist flight test engineers in systems analyses, where required or applicable. All Flight Readiness Firings (FRF) will also be monitored as above.



5 MATHEMATICAL MODELS

The methods of analysis described in paragraph 2.2 will be expanded as the Apollo vehicle progresses from design through tests. The time sequence and duration of operation of elements of the system that will be added to determine time-oriented reliability models are important. Variation of the environment throughout the mission development can be introduced in the same models. This allows reliability predictions and optimizations that include all the pertinent parameters affecting reliability.

The time-oriented reliability model method of analysis can be used at any phase of the program with varying degrees of sophistication, depending on the available details of the hardware. A model for the complete system will be delineated to the lowest replacable component.

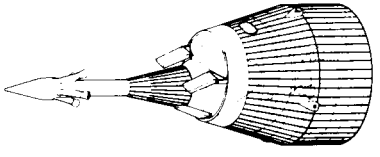


6 DATA SYSTEM

Reliability data for Apollo will necessarily include a wide range of data types for day-to-day analyses and comparative evaluations. Machine processing of data by specially developed, high-speed, digital computers will be used. Processing by a punch-card electronic accounting machine is too slow and the data storage too bulky and cumbersome to handle these tasks. Taped data or another form of memory storage to provide simple programing and rapid access will be utilized. Data processed into the system and stored will include quantitative design conditions and operating parameters, all engineering and reliability test results, and test conditions. Purchased parts and assemblies from vendor and subcontractor plants and all production details and experience obtained from detailed "clean-up sheet" type data through quality control detected discrepancies, including initial, in-process, and final acceptance testing, will be covered, along with transportation, handling, storage, field use, field failure, maintenance action, and field problem data. Data will be acquired on operating life, in terms of time or cycles, and service life, in terms of storage time, transport distances, handling operations, repair actions, maintenance actions, and types of dispositions ultimately established for obsolete, damaged-beyond-repair, and otherwise expended materials and equipments.

In implementing this system, data accuracy requires that each part at each level be clearly marked with its part number and serialized. Complete and accurate data recording and enforcement will be established as a specific management requirement. Wherever applicable, a specific inspection requirement against which inspection rejections must be written when data is incomplete or apparently inaccurate, will be used. Cross-check or audit data from other sources, from which determinations can be made as to the accuracy of the reliability data on a continuing basis, will be necessary.

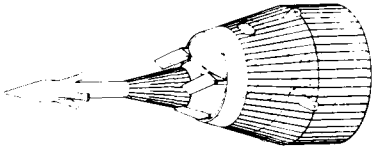
Needless to say, the data gathered for reliability assessments and indices will also be used to establish timely logistics requirements, provide the basis for cost analyses, and indicate procedures improvements, worker output and error indices, supervisory capability indices, maintenance effectiveness factors, program status, and progress summary information.



7 MAINTAINABILITY

Activities associated with design for maintainability for Apollo are of critical importance to product reliability during the end-use phase. Human reliability is also a vital consideration in maintenance actions; therefore, human-use factors must be an integral element of design for maintainability.

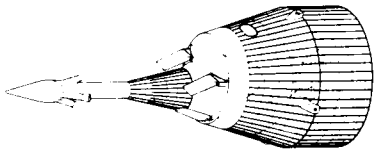
Effective design for maintainability, when applied to the degree needed for Apollo, will affect packaging to allow adjustment, calibration, or alignment with minimum difficulty.



8 PRODUCIBILITY

Producibility considerations involve not only the ability to produce a highly reliable product, but also the means by which it can be inspected and tested to measure and assure its quality and reliability. Thus, designing for optimum producibility must include a review of, and contributions to, the design for inspection and testing as well as for the existence of consistent, repeatable methods for fabrication and assembly. The basis for most such design decisions will therefore be a study of the elements of reliability data on various equipment and processes contained within the comprehensive reliability data system. This data must be provided to the designer at the system design (functional block diagram) level and producibility must be made an element of reliability design reviews. Subsequently, both quality control personnel and reliability engineers should perform producibility reviews of equipment operating procedures and material and manufacturing process specifications.

Recognizing that some producibility problems will pass undetected through the producibility screening actions, no matter how thoroughly they are accomplished, the reliability data system for the Apollo must be sensitive to and rapidly responsive to producibility problems that develop in production.



9 QUALITY CONTROL

An effective reliability program must have a comprehensive and effective contractor quality control effort. Present cooperative collaboration between reliability and quality control organizations will be continued on the Apollo program.

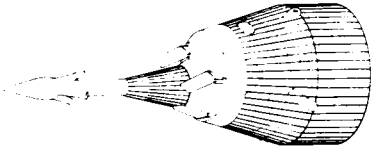
9.1 QUALITY CONTROL SUPPORT. In general, quality control areas of concern to an adequate reliability effort on this project are the introduction of controls for in-plant processes, surveillance of testing activities, control of hardware rejections, cooperative discrepancy-failure actions and specific support, both in-plant and at outside facilities, on vendor and subcontractor reliability and quality problems.

9.2 QUALITY CONTROL DATA. Quality control personnel will contribute to the reliability program by providing complete records on hardware rejections. These records with reliability data will provide trend indicators of reliability program effectiveness. Thus, both quality control and reliability engineers will follow rejections and initiate actions to avoid the use of marginal items. Follow-up of corrective actions will be a cooperative effort in-plant and at the test sites.

9.3 VENDOR AND ASSOCIATE CONTRACTOR SURVEILLANCE. Special emphasis will be given to procedures and techniques for coordinating with associate contractor reliability activities. Also, an appreciable effort will be made to promote and control selected subcontractor and vendor reliability activities. Of particular importance here is the accumulation and interchange of data, obtaining accurate operational time records on procured components and assemblies as they are received, and being alerted as quickly as possible to failure areas encountered in production and inspection processes within the contractor's plant and at vendor and subcontractor plants.

Since several important GSE and vehicleborne components in the program are likely to be designed, developed, and/or produced by major subcontractors, integrated subcontractor and vendor reliability control activities are considered essential elements of the overall Apollo reliability program. In this area, contractor's responsibilities for engineering coordination and control of major subcontractors will involve joint efforts of both contractor engineering project office personnel and reliability organization personnel.

Emphasis will be placed primarily upon data interchange regarding failures and discrepancies detected throughout the course of production in the associate contractor's facilities. Accurate logging and transmission to the contractor's reliability data center of operating times on the Apollo vehicle and GSE systems, equipments, and components, accumulated in the associate contractor's plants and test operations prior to delivery, is an important requirement.



10 RELIABILITY REQUIREMENTS DOCUMENTATION

The reliability requirements for documentation in a comprehensive product-reliability program would encompass two basic areas: 1) establishing reliability requirements in various, key, overall program documents, and 2) maintaining reliability requirements up to date. Enforcement of reliability requirements should be performed by a reliability control function which also compares reliability measurements with requirements on the basis of data provided by the reliability data system.

The initial task of the reliability documentation function should be the study and interpretation of requirements contained in contractual documents. If numerical goals and/or requirements are established, the significance of these goals or requirements must be developed in detail and the implications in different overall program areas specified. Reliability program requirements must be delineated and task areas defined with budgetary limitations, and program elements must be spelled out on a strict scheduling basis to be used for program planning. Finally, the implications of prime contractual reliability requirements must be established for subcontractors and vendor tasks, and tentative reliability cost estimates and schedules prepared to be used as bases for comparisons in evaluations of subcontractor reliability proposals or work statement items. In addition to interpreting contractual reliability requirements, a number of working program documents should have definitive reliability requirements sections. These are:

a. Process and materials specifications;

b. Design, structures, parts, materials, and drafting room manuals standards;

c. All test specifications and test plans;

d. Purchase orders;

e. Quality control procedures documents such as equipment operating procedures;

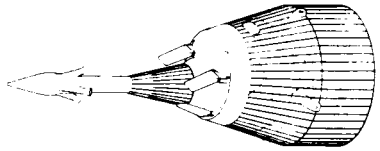
f. All inspection procedures;

g. All handling, packaging, storage, and transportation specifications and procedures; and

h. Design and procurement specifications.

Reliability requirements sections must be prepared and inserted into design and procurement specifications and subcontractor work statements. The requirements should include reliability goals to be attained and a number of required activities to be performed by vendors and subcontractors as integral parts of the overall reliability program. A significant part of these activities is the accumulation and supplying of appropriate reliability data for input into the prime contractor comprehensive reliability data system. Such data should include, but not be limited to: results of inprocess inspections and tests; results of final acceptance tests; proposed and affected design, material, and process specification changes; incoming or receiving-inspection test results or parts and materials used for the end products to be delivered by vendors; and changes in tooling and jigs and fixtures in use by vendors.

Once reliability requirements are established in the appropriate program documents, a continuing task would be the maintenance of these requirements. Program "soft spots" detected by the reliability data system will result in making requirements more stringent in areas with lagging improvement or overall poor performance. The introduction of design improvements or new production techniques must also be accommodated by changes in reliability requirements that fit the new conditions. Thus, the updating activity must be continued throughout the program.



11 RELIABILITY PROGRAM MANAGEMENT

Direction of the reliability program on the Apollo project should be accomplished at the highest management level through reliability policy committee which, in turn, directs the activities of a reliability organization. The reliability organization should be supported by all division departments in implementing the reliability program for Apollo. A reliability policy committee should direct the reliability effort, and should be an active, top-level management, formulating body.

All major areas where reliability problems can occur and where remedial actions must take place should be represented on this committee.

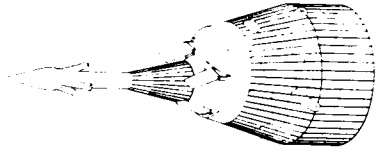
Regularly scheduled division reliability policy committee meetings should be held at least once each month. When required, special meetings should be held to consider and render decisions on urgent policy-level and technical reliability problems.

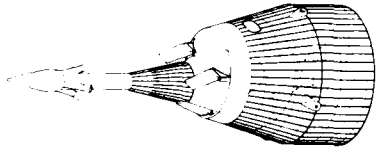
The committee should formulate reliability policy, implement broad technical reliability decisions, and act as the organization means for directing activities required on the reliability program. It should direct reliability corrective and remedial actions directly through one or more of its members. Follow-up responsibility should be assigned to the head of reliability, who is to act for the committee on a day-to-day basis. All important decisions on product reliability programs are to originate with top management and should carry the necessary authority to bring about prompt action.

Committee decisions should be primarily implemented through direct action within the committee, and should be set forth in the minutes of each meeting, and distributed to all members. As the need arises, special problems should be handled by appointing various managers (members of the committee) to a special problems subcommittee. This subcommittee should act promptly to expedite investigations and, upon completion, submit its findings to the main committee for decisive action.

The committee should monitor the Apollo reliability program through regular reports on Apollo reliability activities. Reliability problems requiring committee decisions should be given immediate attention and steps taken to ensure corrective action. The committee should also review trends on reliability progress.

The Apollo reliability program should be carried out under the direction of a qualified, experienced reliability project coordinator assigned specifically to the Apollo program. This reliability project coordinator will be responsible for the effective administration and technical direction of Apollo reliability activities.



REFERENCE

1. Hosford, John E., Measures of Dependability, Operations Research, Vol. 8, No. 1, pp 53-63, Jan. - Feb. 1960.