JOHN F. KENNEDY SPACE CENTER

TR-1091

ACCEPTANCE CHECKOUT EQUIPMENT FOR SPACECRAFT

By Walter E. Parsons
Systems Engineering Division

January 26, 1971

National Aeronautics and Space Administration
John F. Kennedy Space Center
Kennedy Space Center, Florida 32899

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
TR-1091		

4. Title and Subtitle	5. Report Date
Acceptance Checkout Equipment for Spacecraft	January 26, 1971
	6. Performing Organization Code: DD-SED

7. Author(s)	8. Performing Organization Report No.
Walter E. Parsons	

9. Performing Organization Name and Address	10. Work Unit No.
Systems Engineering Division (DD-SED) John F. Kennedy Space Center Kennedy Space Center, Florida 32899	11. Contract or Grant No.
	13. Type of Report and Period Covered

12. Sponsoring Agency Name and Address	14. Sponsoring Agency Code
National Aeronautics and Space Administration John F. Kennedy Space Center Kennedy Space Center, Florida 32899	DD-SED

15. Supplementary Notes
Author is co-inventor of "Electronic Checkout Systems for Space Vehicles," patent number 3,535,683; and co-inventor of "Hardline Monitoring System," patent applied for.

16. Abstract

This paper summarizes the design requirements and development of the Acceptance Checkout Equipment for Spacecraft (ACE-S/C) for the United States Space Program. The concept of man in a system, the man-machine relationship, and the application of reliability predictive techniques are discussed. Man, the analyzer/decision-maker, is the monitor in a computer-controlled, electronic checkout system for spacecraft. Application of the techniques developed in the ACE-S/C subsystem to civilian earthbound systems can result in appreciable benefits to our society.

17. KeyWords	18. Distribution Statement
Space Vehicle Checkout Program, Man-Machine Systems, Real-Time Operation, Test Equipment, Reliability Engineering, Redundancy, Manned Spacecraft	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	29	

PREFACE

The concept of using man as a working component of a system was employed in the United States Space Program. This paper discusses the application of this concept in the development of one subsystem, the Acceptance Checkout Equipment for Spacecraft (ACE-S/C). This paper also describes the principles and applications of these principles with an emphasis on the reliability engineering practice that was used as a design tool.

The preparation of this paper has been substantially assisted by the contributions of Dr. John de S. Coutinho, Otto H. Fedor, Edgar A. Beard, and other associates. I am particularly indebted to Dr. Kurt Debus, Director, Kennedy Space Center, National Aeronautics and Space Administration, for his support and guidance.

January 26, 1971
Walter E. Parsons

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

INTRODUCTION

From the United States Space Program, a new concept of man as part of a system has evolved. Because of the schedule and operational constraints associated with the Mercury and Apollo Programs, the application of this concept has resulted not so much in the development of new equipment, as in new uses of available equipment. As additional projects develop, this concept could result in the development of new equipment which could find wide and significant applications beyond the scope of the Space Program.

Application of this concept in the development of one subsystem, the Acceptance Checkout Equipment for Spacecraft (ACE-S/C), will be discussed to illustrate the principles involved. Various applications of these principles have made a significant contribution to the success of the United States Space Program. Specifically, the application of this concept has permitted man to land successfully on the moon, knowing he had only 3 seconds of fuel in reserve.

A dramatic test of the usefulness of the concept was provided during the Apollo 13 manned mission. After the tragic failure of the Service Module on the approach to the moon, it was possible in a minimum of time, and in an optimum manner, to reprogram the flight and utilize the resources still available to achieve a successful emergency return to earth.

MAN IN SPACE

The United States Space Exploration Program was conceived as a comprehensive, long-term program, encompassing both automatic and manned systems. Each type of system has its inherent limitations; the intent is to employ that system which will best satisfy the requirements of a specific mission.

Because of the weight constraints associated with spacecraft, it is necessary to take full advantage of the capabilities of every component included in the flight vehicle. This principle also applies to man as a member of the flight crew, and to the cumulative capabilities of the crew; that is, man should be considered as an integral part of the system, and every effort must be made to take maximum advantage of the unique characteristics he adds to the system. It follows that a manned system will have capabilities not inherent in an automatic system.

The current concept of the role of man in a spacecraft is that of observer/analyzer decision-maker. Man should not be required to perform functions which can be accomplished more effectively by machines. Hence, the problem is to use these unique capabilities of man (observation and decision-making) to extend the capabilities of equipment. This has been the underlying concept which has been fostered throughout the Mercury and Apollo Programs (Figure 1).

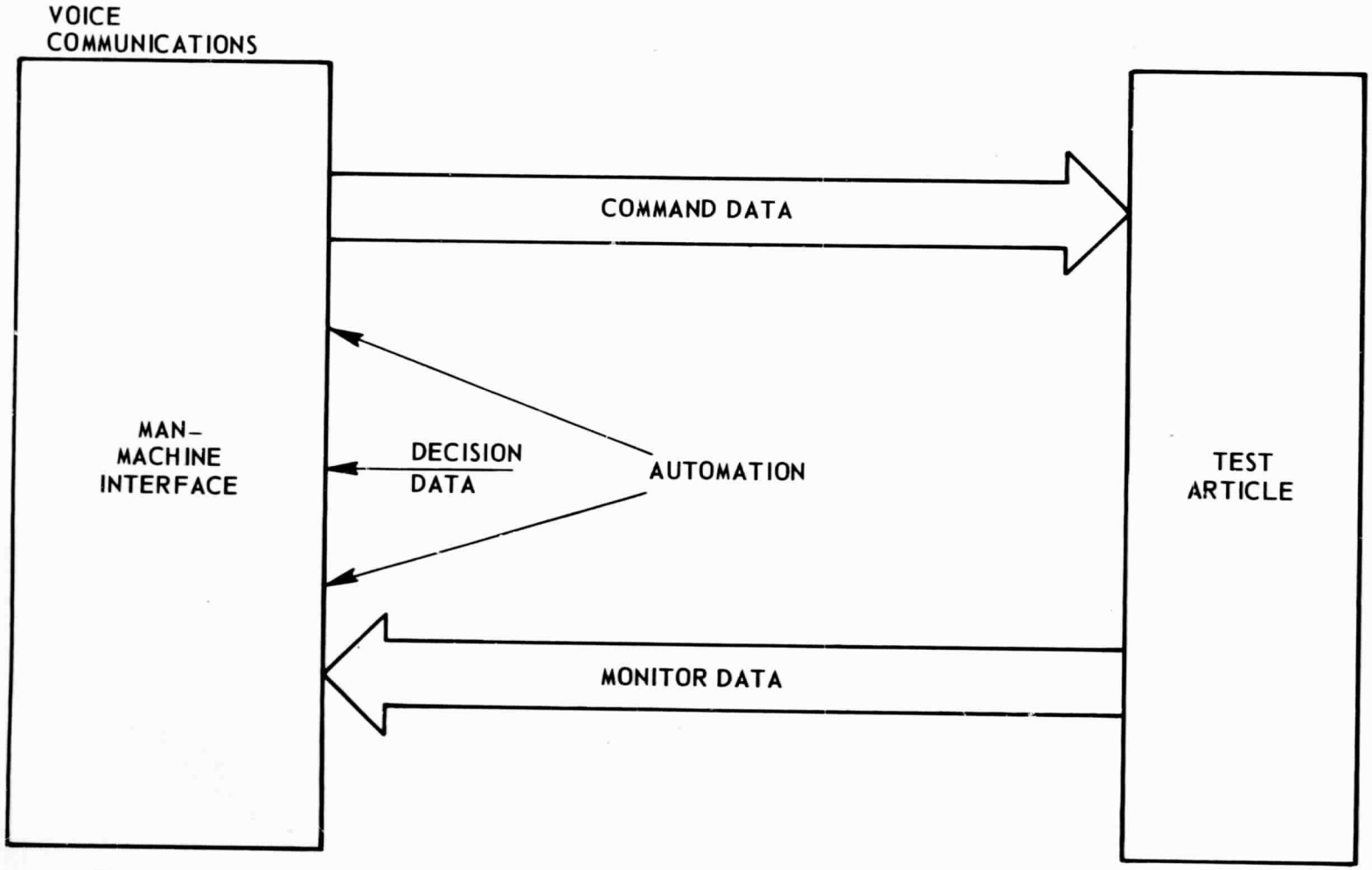

Figure 1. ACE-S/C Concept Block Diagram

SYSTEMS EQUIPMENT

A manned space system is considered to consist of three basic elements: hardware, software, and man.

For present purposes it is not necessary to define man or hardware. Software consists of written analyses and procedures which define the relationship between man and hardware within the system as required for mission accomplishment.

The integration of man into a space system presents a particular challenge. In contrast to hardware, man possesses dynamic characteristics; he learns with experience. As he learns, he becomes more effective, thus modifying the hardware and software design requirements. It has not been possible to model man's learning characteristics. The approach has been to build special-purpose simulators to integrate man, software, and hardware; and, within selected and limited scopes, to develop hardware and software requirements based on man's changing capabilities. The Apollo Program was based on the use of the most sophisticated simulators for crew and ground support personnel. However, because of practical deadlines, the approach could never be followed to its final conclusion. Those in the Space Program find themselves at the beginning of an exciting new development.

Hardware can be classified from various viewpoints. A common classification is the breakdown of hardware into flight and ground-based equipment. Flight hardware is basically different from ground-based equipment because of the prime emphasis on weight-effectiveness. Ground-based equipment includes all facilities and equipment necessary to support the launch, flight, and retrieval of spacecraft.

An important element of the hardware system is the instrumentation. The ACE-S/C is a subset of the instrumentation group and includes both flight and ground-based equipment (Figure 2). The mission of the ACE-S/C is to provide for the adequate checkout of manned spacecraft and experiments in the preparation area during prelaunch operations. The ACE-S/C subsystem provides assurance that the various onboard systems are in operating order, and, in case of failure, pertinent information is presented in a form to the human monitor so he can make decisions on the best use of available equipment.

MONITORING REQUIREMENTS

Some of the design requirements applicable to the ACE-S/C were established for the total instrumentation/monitoring package. To enable flight personnel to concentrate on their duties of observation and decision-making, detail monitoring is accomplished to the greatest possible extent by specialized ground-based personnel and instrumentation. The monitoring encompasses the following classes of information:

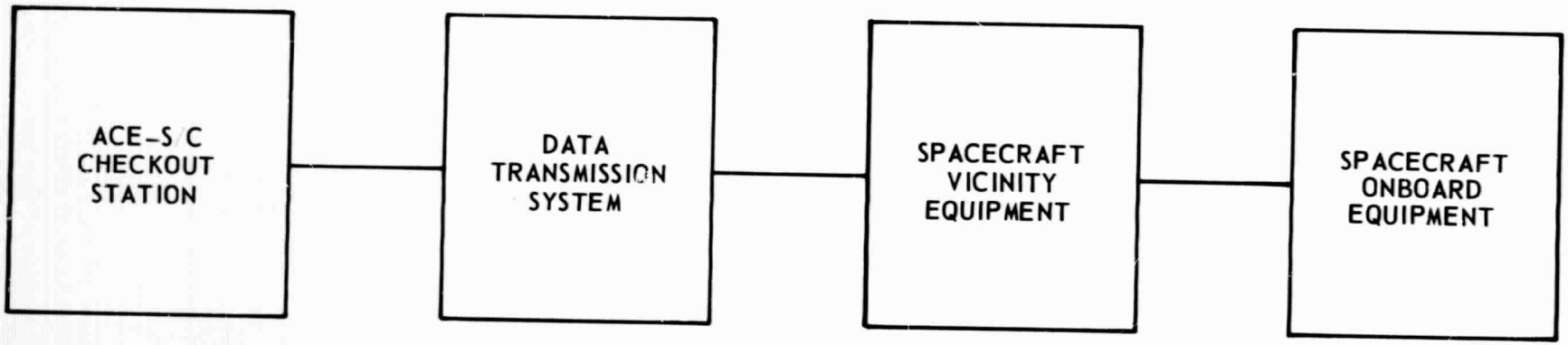

Figure 2. ACE-S/C Operational Block Diagram

1. Operational parameters.
2. Indicators of the integrity of flight and critical ground support subsystems.
3. Indicators of the integrity of the instrumentation.

The operational parameters include those values necessary to control the progress of flight operations, such as velocity and acceleration versus time, navigational information, fuel and oxygen management, etc. These parameters are of interest to both the flight crew and to ground advisory personnel, whose functions are to advise flight personnel on how to attain the best utilization of available equipment.

The indicators of the integrity of flight and critical ground support subsystems provide the basis for the assessment of the operational condition of onboard and ground-based equipment during ground and flight operations. Flight crews are interested in information for this class only as may be necessary as a basis for their decision-making. All details, however, are of interest to specialized ground-based monitors.

Ground personnel also are interested specifically in the integrity of the instrumentation to ensure that the operational information presented to flight personnel and ground advisors is correct.

The same concept of the human function developed for flight crews, namely that man is an observer and decision-maker, is also applied to the ground monitors. The ground monitor observes the real-time performance parameters of specific hardware elements and makes decisions which are communicated to the ground-based advisors. He performs no functions which can be performed by available machines. This approach has resulted in revolutionary new requirements for data processing and display. The application of these concepts has led to the development of the unique Unites States Space Control Room (Figure 3).

The complete ACE-S/C subsystem, including the control room (Figure 4) consists of a number of modules which provide for considerable operational flexibility in testing various systems at various subsystem levels. This flexibility is provided by a series of major control loops containing a number of smaller control loops, and these in turn contain a number of lesser control loops. Provisions are made for manned intervention so that selectable levels of automation can be attained. The standardization of data elements at the interfaces between modules has been a major design consideration. Since it must be possible to monitor the spacecraft while it is in flight, the subsystem design must be based on remote control and remote monitoring techniques.

The concept of man as a continuously operating decision-maker within a system established a new set of requirements for the timely presentation and format of analyzed data. In conventional flight test work, individual items of data such as readings of temperatures, accelerations, pressures, stresses, and deflections are telemetered and recorded. Rooms full of data are accumulated. The speed with which these data are analyzed depends on the facilities available for the analysis work; often the analyzed

Figure 3. United States Space Control Room

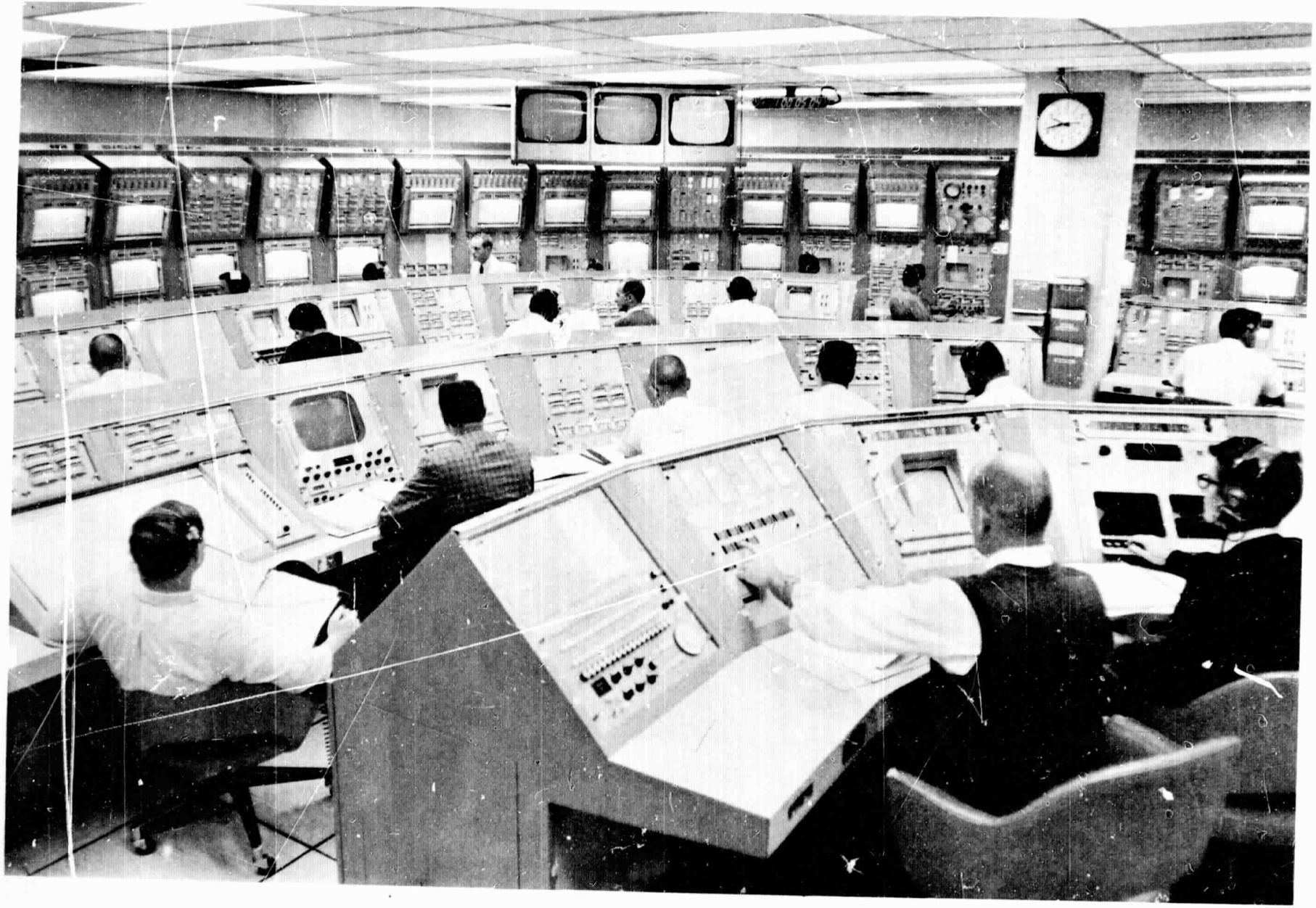

Figure 4. ACE-S/C Control Room

results are available only weeks or months after completion of the test. This procedure has been quite satisfactory for aircraft programs, during which the test vehicles approach critical flight conditions in gradual steps, and which may require 1,500 flight test hours to reach full development.

These conventional procedures first proved inadequate on the Mercury Program, where some 2 miles of taped data was being accumulated per launch. Subsequent analyses proved to be of little value; the need was to recognize conditions as they were occurring so that in case of irregularities they could be recognized and immediate action could be taken.

This need represented a new requirement for data to be analyzed immediately in real time upon acquisition, and to be displayed in proper context with previous measurements so that it would be meaningful to the human monitor. From the technical viewpoint, the overriding design requirement was for the reduction to a minimum of the processing time for data acquisition, integration with historical data, and the complete analysis and the display of all pertinent information, so that it appears as real time to the observing monitor.

The instrumentation system evolved into three basic functional groupings:

1. The Command or Uplink System.
2. The Monitoring or Downlink System.
3. The System Software (automation).

The requirement for the display of real-time information to test and operations personnel presented a new and revolutionary design challenge. The remainder of this paper will discuss the ACE-S/C; that is, the equipment dedicated to the monitoring of the integrity of flight hardware.

ACE-S/C

The primary function of the ACE-S/C subsystem is monitoring the integrity of spacecraft flight equipment; however, the effective performance of this function also requires the monitoring of the integrity of the associated instrumentation. The subsystem is compatible with all other elements of the total instrumentation syster .

A highly simplified diagram of the ACE-S/C subsystem is shown in Figure 5. The spacecraft is shown in the flight mode; it is therefore necessary for all data to be telemetered. All telemetry is based on digital technology; the same is true for all data transfer at subsystem interfaces. When the spacecraft is on the ground, data acquisition is accomplished by means of cables which are disconnected just prior to liftoff. Re-used cables provide a much more effective capability for fault isolation than can be provided by a telemetry link. This is of significance during the complete checkout which is performed just prior to launch to ensure that all systems are GO.

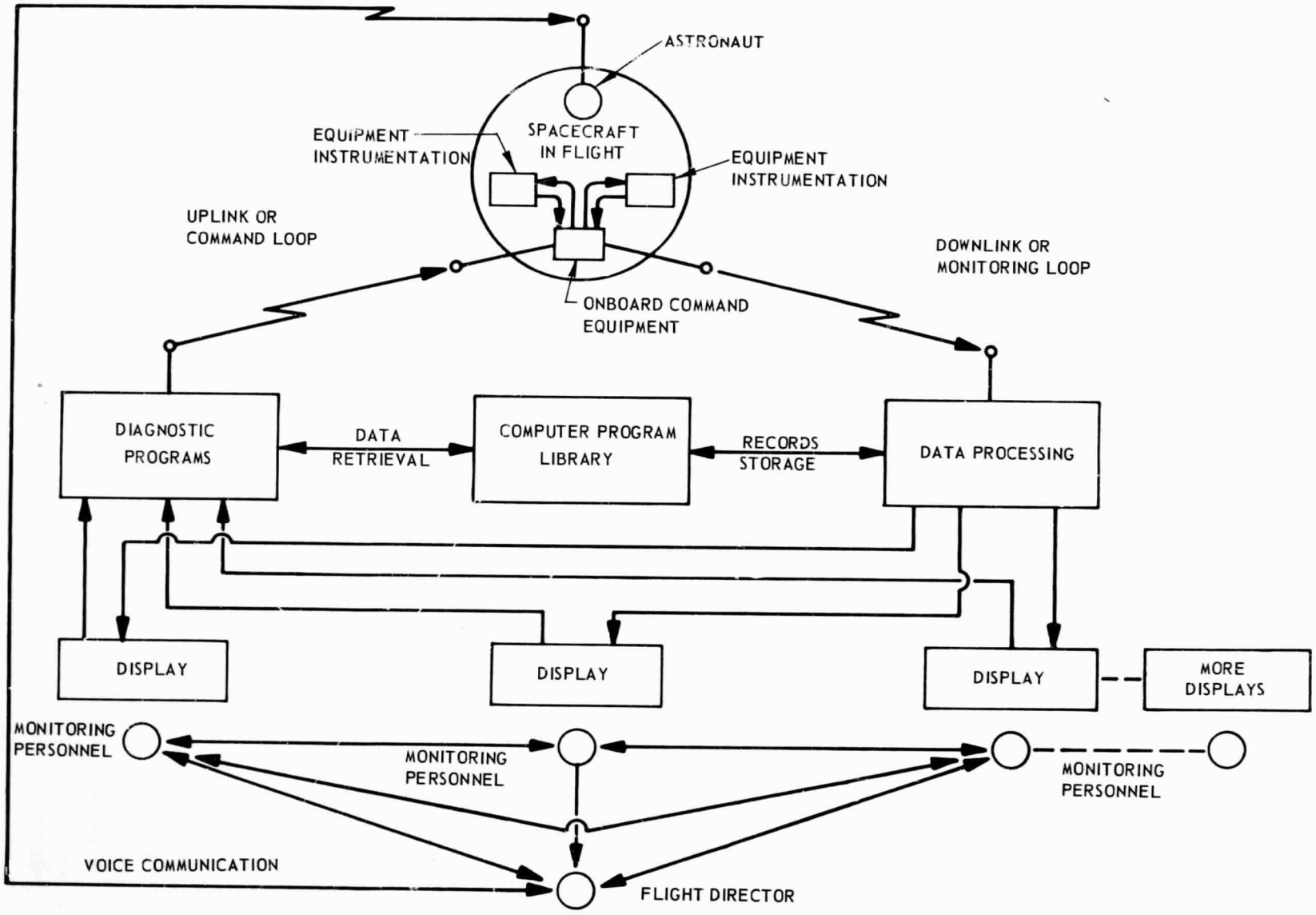

Figure 5. ACE-S/C Simplified Block Diagram

For simplicity, Figure 5 shows only two equipment/instrumentation packages in the spacecraft, and three display consoles. Actually, there are approximately 11 monitored systems in the flight vehicle, and 11 groups of display consoles.

All monitoring personnel are representatives of cognizant systems engineering groups and may initiate tests through the command link. Tests may also be preprogrammed for automatic execution, either periodically or continuously. However, the monitors are in control of all tests at all times, and may select various testing modes, such as: manual, manual/semi-automatic, or automatic with override. This flexible capability is essential under conditions which are constantly and progressively changing.

Commands for tests from all consoles are collected and presented at a central ground-based Diagnostic Program Center and relayed to the Onboard Command System in the spacecraft.

The Onboard Command System executes the commands received, including those for preprogrammed self-checks, and relays the self-test data back to the central, ground-based Data Processor. The response data and the routine operational and environmental data are also transmitted to the ground-based Data Processor by the monitoring link.

The data received by the Data Processor is reduced and collated with all previously acquired data which is stored in the Library (Central Data Bank). The status of all command and monitored data is recorded in the Library and kept available for real-time retrieval. The status of all critical or pertinent parameters is transmitted continuously in real time and in meaningful engineering units to the proper display units. Information is presented immediately in decisive form to test and operations personnel, enabling quick decisions in a highly significant and dynamic situation.

The displays are designed to present information in such a manner as to reduce the manipulative load on monitoring personnel as much as possible, to free them for their main decision-making functions, and to increase the confidence in the monitoring program. The real-time processing is provided to allow immediate detection of changes in active data channels, to provide data by exception, and to identify potentially significant trends. The same reasoning is used in providing for automatic self-checks, calibrations, validations, continuous limit checks, out-of-tolerance indications, and significant trends. Every effort is made to permit recognition of gradual degradation and the timely initiation of corrective actions to avoid catastrophic failures.

Monitoring personnel also have free access to the Library and may retrieve in real time any previous data stored there to support their trend analyses. Provisions are made for independent testing from separate locations, at the option of test personnel.

Monitoring personnel maintain close oral communications with one another and with the Flight Director, who in turn also maintains continuous communication with the

astronaut in the spacecraft. None of the monitoring functions interfere with normal astronaut activity during operational modes.

The implementation of these concepts requires the integration of spacecraft and monitoring equipment; that is, each piece of onboard operating equipment must be designed so that its critical parameters can be monitored by the ACE-S/C devices.

Subsystems and systems are analyzed during design to determine all potential failure points and possible failure modes (Reference 1). Provisions must be made for independent subsystem testing, integrated systems testing, and testing across systems interfaces. The parameters to be monitored will vary with the type and function of the equipment and the characteristics of the potential failure.

The prerecorded test programs are utilized to simulate critical functions and potential failures, and to exercise critical components. In the case of a system or subsystem failure, the test routines follow the plans developed in the fault-tree analysis (Reference 2), which as far as practicable isolates the failed device and pinpoints the failed components. In mechanizing the ACE-S/C design, prime consideration was given to the requirement for on-time launching, to be accomplished in full public view. The ACE-S/C development time was established by the spacecraft schedule, and therefore, emphasis was placed on adherence to rigid schedules and fundings. Commercial and other existing equipment was utilized whenever available, and the necessary reliability had to be achieved by the use of redundant techniques rather than by sophisticated design. Available commercial equipment was invariably designed for other applications and was usually not completely suitable to satisfy the requirements of the ACE-S/C subsystem. It was therefore not possible under these circumstances to achieve an optimum design.

The greatest difficulties were encountered in meeting the telemetry requirements, and particularly the stringent weight requirements applicable to onboard equipment. In the beginning of the program, power line transients in the public power supply caused voltage transients and wave form distortions; it became necessary to provide battery backup for the onboard equipment, and to power the ground system by use of diesel generators. The removal of the test cables from the spacecraft had to be accomplished without invalidating the onboard systems. The accuracy of the instrumentation also presented a problem. Available instrumentation is designed to measure operational parameters with an accuracy required for navigation and guidance. This accuracy is not always adequate for the measurements required for trend analysis and for monitoring the integrity of the instrumentation itself.

A large number of papers have been published describing the various subsystems and equipment comprising the ACE-S/C; it serves no purpose to repeat such details here. References 3 and 4 are representative of those publications.

RELIABILITY REQUIREMENTS

Compliance with the reliability requirements for the ACE-S/C constituted an overriding major design consideration. The requirements for the ACE-S/C subsystem were derived from those for the Apollo Program.

Since there was no precedent for the Apollo Program, there were also no accepted guidelines for establishing reliability requirements. Now that the initial flights of the Apollo Program have been successful, the associated requirements will provide a baseline for use on all future programs.

The final Apollo reliability requirements were based on the inputs of many studies. The development of a representative early input is described in Reference 5 as follows. In an effort to determine a morally acceptable level of risk to which a man may be subjected, a quantitative study was made of the probability of survival of U.S. Navy carrier-based pilots, both during peacetime and wartime flight operations. There appeared to be no significant difference between the peacetime and wartime results. At first, this result was surprising until it was realized that 85 to 95 percent of all wartime flight operations consist of the same training exercises as in peacetime, to keep pilots at top proficiency.

This study led to further statistical research involving the probabilities of survival at the Indianapolis Racetrack and the Mexico City Bullfighting Ring. These topics were selected because of the high risks associated with these activities as well as the cultural differences, and the different nature of the risks. The results were again surprising in that they indicated that the probability of survival at Indianapolis was about the same as at Mexico City. Both risks were an order of magnitude higher than those required of a naval carrier pilot.

Although the scope of this research was limited, it led to a number of tentative conclusions. At Indianapolis as well as at Mexico City, the risks are determined exclusively by the actions of the participants; the individual himself determines the magnitude of the risks in a series of successive trade-offs between risk and glory. The glory accruing to the naval carrier pilot is not as great as that accorded to the victor at Indianapolis or Mexico City; he cannot be subjected to the same level of risk.

For the Apollo Program, it was decided that the glory which would accrue to a volunteer astronaut as a result of a successful round trip to the moon would be much greater than any which he could win in earth-based events. Right or wrong, it was decided that manned spaceflight legitimately and morally may be associated with risks greater than those measured at Indianapolis and Mexico City. This type of thinking influenced the establishment of the original reliability requirements for the Apollo Program, which now provides the precedent for requirements for future systems.

The Apollo Program reliability requirements were apportioned to the various subsystems by means of accepted techniques such as those described in Reference 2. These

techniques are based on the use of the product rule. The following three quantitative requirements were apportioned to the ACE-S/C subsystem:

Hardware Reliability: $R_h = 0.9995$

Operational Reliability: $R_o = 0.99995$

Crew Safety: $R_s = 0.999995$

These numbers are applicable to the originally proposed 72-hour mission. The term "Hardware Reliability" refers to the capability of the subsystem hardware, operating under the specified design conditions. "Operational Reliability" refers to the probability of mission success of the man-machine assembly and considers the use of degraded operating modes. "Crew Safety" takes into consideration the redundancies provided by emergency standby subsystems which provide the astronauts with means for escape in case of mission abort.

In conjunction with quantitative requirements, it is necesary to establish demonstration test policies. These numbers are so large that the use of conventional demonstration techniques is not feasible. In this situation, it was decided to speak of design "goals" rather than "requirements," and to establish modified demonstration procedures.

For all design decisions, it was required that attainment of the goals be demonstrated analytically, following standard procedures (Reference 2) based on published data and selected component and element test results. To standardize the computations, the goals for the 72-hour mission were expressed in the equivalent terms for a 1-hour mission and converted to Mean Time Between Failure (MTBF). Thus, the subsystem Hardware Reliability requirement:

$$R_h = 0.9995 \text{ (for a 1-hour mission)}$$

converts to a design goal of

$$MTBF_h = 2{,}000 \text{ hours}$$

This conversion permitted all calculations and test results to be expressed in conventional units.

A test plan was established to demonstrate, whenever feasible, the validity of the design assumptions and of analytical conclusions. Normally, such tests could not demonstrate attainment of reliability goals; however, they could and did demonstrate in certain instances that the goals had not been attained and that further design effort was indicated. In particular, this program included special-purpose tests as well as all development tests, system integration tests, and reliability monitoring of activation, prelaunch, and flight operations. In situations where such high reliability figures are involved, it is

essential to establish an evaluation system which will not neglect to make use of every bit of data which becomes available in all types of operations.

In addition to the quantitative requirements, it was necessary to establish a number of configuration requirements which affected reliability. All potential single point failures had to be identified and eliminated to the greatest extent possible. The established design policy specified that no single failure should produce a subsystem failure.

For each potential component or element failure, either catastrophic or degradation, the resulting degraded operating mode was identified and it was determined to what extent the degraded mode could still support the accomplishment of the mission.

Since weight and space requirements are not critical on ground-based equipment, heavy emphasis was placed on the selection of commercial or other equipment which had a prior history of successful operation.

In the discussion that follows, both the design and reliability problems that existed at the project initiation will be described, followed by an explanation of the approach that was taken to meet the assigned goals.

DESIGNING FOR OPERATIONAL RELIABILITY

The reliability implications of a complex high-performance, computer-controlled checkout system (which was to be the only link between the spacecraft and the test engineers for command and control, and for data collection, processing, and display) dictated a unique design approach that would yield a systems design with a reliability that would exceed the intrinsic reliability of the component parts. In addition to hardware reliability goals of 0.9995, the operational reliability requirement was 0.99995 for mission success, and 0.999995 for crew safety. The 0.9995 converts to an equivalent 1-hour MTBF of 2,000 hours for the entire system. A design utilizing six or more major subsystems in series established a design requirement for each subsystem to have a predicted equivalent 1-hour MTBF approaching 100,000 hours (approximately 12 years).

The design concept was to utilize commercially available equipment, and the operational concept required non-catastrophic failure modes and a design that would degrade in a controlled manner.

The state of the art of component reliability as it existed during the initial design phase is described here in order to facilitate understanding of the options that were available to the designer in achieving the required MTBF's for the ACE-S/C subsystem. At that time, an electronic system containing a few hundred discrete electronic parts with a MTBF of 2,000 hours was considered most satisfactory. Application of the same design techniques and the same discrete components would yield decreasing equipment reliability

with increasing equipment complexity (Figure 6 and Reference 6). To maintain MTBF constant with increasing equipment complexity required a reduction in component part failure rates. For example, to achieve the ACE-S/C 1-hour equivalent MTBF's of 100,000 hours (assuming a system complexity of 125,000 parts) would have required a component part failure rate equivalent to one failure in 100 billion part hours, a value considered to be unattainable within the schedule and resources available. The need for a better understanding of failure effects and the need for alternate design approaches were clearly indicated.

Electronic parts, in general, have a constant failure rate. Since the major concern was continuous uninterrupted operation of the Acceptance Checkout Equipment subsequent to the early failure or debugging period, the estimate of the probability or relative frequency of failure was best described by an exponential failure distribution $R(t) = e^{-\lambda t}$ rather than a gamma distribution. The inherent reliability R (t) or survival probability in a system is expressed in terms of its constant inherent failure rate (λ) and period of system operation (t) by the following equation:

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

The mathematical model expressing the relationship between parts and system reliabilities is simply the "product rule," expressed in the following equation:

$$R(t) = \prod_{i=1}^{n} R_i(t) = \prod_{i=1}^{n} e^{-\lambda_i t} = e^{-\lambda t} = e^{-t/\theta} \qquad (1)$$

where $R(t)$ = system reliability at time t

$R_i(t)$ = part i reliability at time t

$\lambda = \sum_{i=1}^{n} \lambda_i$ = system failure rate (since the exponents of an exponential product are additive)

λ_i = part i failure rate

n = number of parts

t = operating time

θ = mean life

The chief concern in the part selection program was to reduce, to an absolute minimum, the catastrophic part failure rates during period constant failure rate.

MTBF SYSTEM HOURS	n COMPLEXITY (NO. OF PARTS)	PER PART FAILURE RATE	ONE FAILURE IN n PART HOURS
2,000	500	.1%/1000 hours	1 million
2,000	5,000	.01%/1000 hours	10 million
2,000	50,000	.001%/1000 hours	100 billion
2,000	500,000	.0001%/1000 hours	1 billion
10 years (80,000 hours)	500,000	.0000024%/1000 hours	410 billion
35 hours	500,000	.0057%/1000 hours	17.5 million
Family Car 35 hours	2,000	1.5%/1000 hours	70,000

Figure 6 . Relative Reliability

In determining the ACE-S/C system configuration, consideration was also given to the following:

1. Utilization of existing equipment, and determination of the best configuration commensurate with the consequence of failure.

2. Improvement of existing equipment to minimize inherent failure rate.

3. Complete redesign of critical systems to meet the overall system reliability goal.

4. Utilization of selective redundancy with existing equipment.

5. A combination of these approaches.

At the time of preliminary design, a reliability predictive phase was initiated. The use of accepted formulas and physical parameters was based on a balance between the physical world with its demonstrated empirical features and the formulation of theoretical models which allowed the development of a first-order design. Subsequently, the design parameters were adjusted to adequately treat the problem of catastrophic failure in electronic parts. Also recognized was the fact that a part could fail to adjust to its circuit condition and environment; it could fail in random fashion long after compatibility had been established, or it could fail in fatigue through time and usage. All such failures entail irreversible processes which require part replacement to establish normal conditions, as contrasted with performance degradations which are often reversible in nature, allowing readjustment but not replacement. Therefore, when, through the reliability prediction technique, critical parts were identified as single failure points, and when the modeling exercise demonstrated a limitation of adjustment to either the part failure rate or design parameters, the only other avenue of system reliability improvement was to establish redundant functions.

Also recognized was the fact that latent defects, primary and/or complementary design errors, or irreversible failure modes (if present in both the primary path and the redundant path) would yield an equipment reliability performance significantly less than initially planned. In view of the above and of the limited time available for development, the technique of functional asymmetrical redundancy was employed in certain critical areas to ensure compatible paths of operation as shown in Figure 7 and Reference 3.

It is accepted practice that redundancy is not a substitute for good design. While it is true that the reliability of some critical components will almost always be too low for use in a simple (non-redundant) system, it is possible to develop a system configuration for high reliability by incorporating redundant components and/or redundant functions. The major task was to obtain an optimum trade-off between the reliability of the system operating modes and performance, weight, space, cost, availability, maintainability, and other critical constraints.

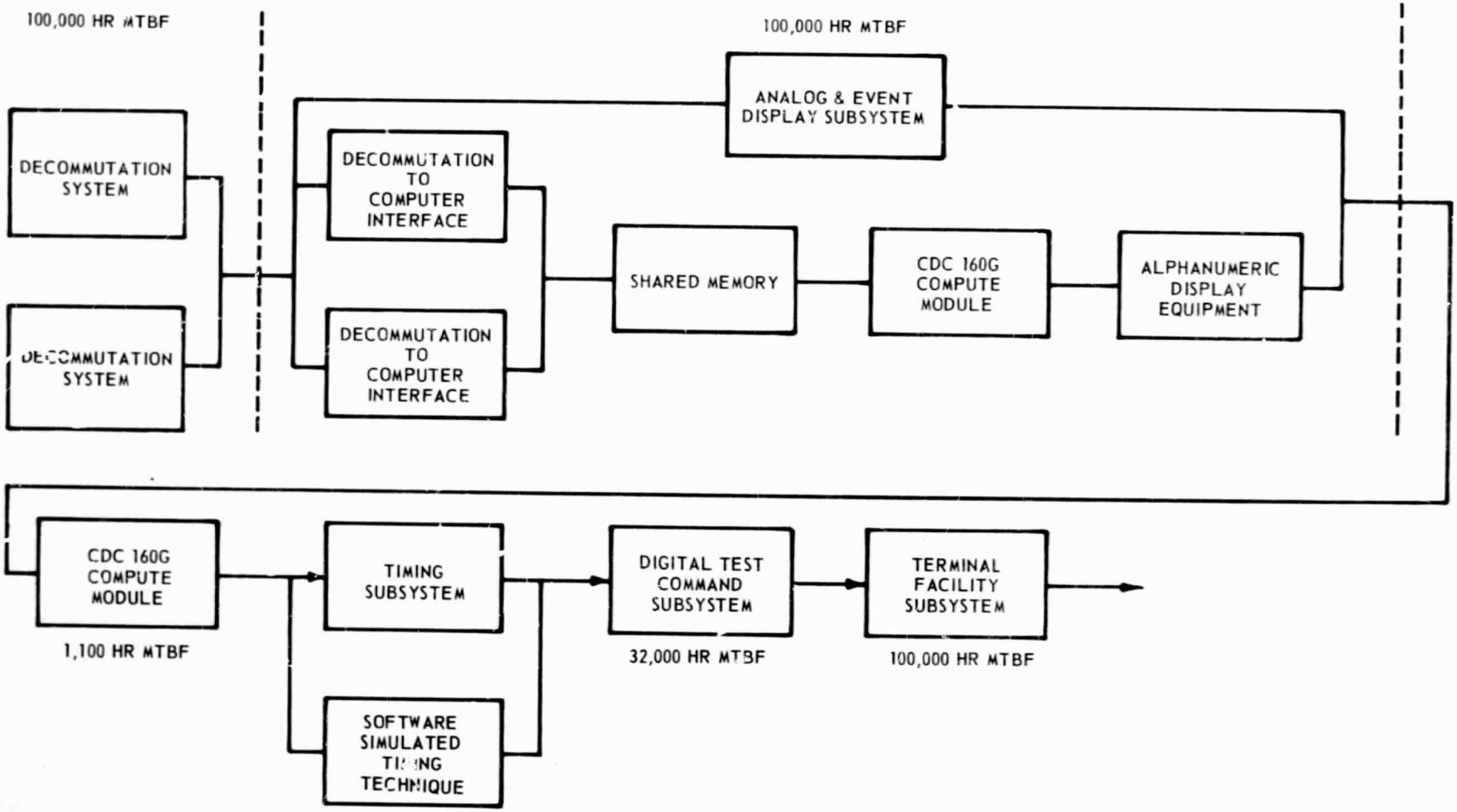

Figure 7. Checkout Station Redundancies

Early in the design phase, it was discovered that improperly applied redundancy not only added to system complexity and equipment costs but also substantially increased the probability of mission failure due to the increase in "passive single paths" (e.g. wiring, ducting, etc.). For redundancies to be meaningful, it must be possible to utilize them operationally within a very short time frame after the prime equipment is discovered to be inoperative (Figure 7).

It is significant that the first reliability analysis revealed that major subsystems, as initially configured (Figure 8), would have 1-hour equivalent MTBF's of less than 100 hours. This would result in a total system reliability of less than 25 hours, which was unacceptable since a 1-hour equivalent MTBF of 2,000 hours was required. The predictive technique employed the equation $R(t) = e^{-\lambda t}$ which yielded MTBF's that appeared too low and were further complicating the design process. Based on the experience of the design team, the value of equation (1) was multiplied by 4 for equipment currently in production and constructed of solid-state components. This value then became the basis for further design analysis.

After adjustment of the prediction process and optimization of the equipment design, the projected ground checkout station equipment 1-hour equivalent MTBF was approximately 1,000 hours. This was below the system requirement of 2,000 hours and did not include the data links and the spacecraft vicinity equipment. By use of a conservative design approach, independent subsystems, built-in self-check capability, and the requirement of two checkout stations operating in parallel, it was possible to predict operational continuity despite localized component or subsystem failure (Figure 8). The reliability analysis indicated that the prime data lines required a 20-percent backup capability to meet the reliability goals. This is based on the calculated reliability of one transmission line as analyzed against the need for all ten lines being operational at any given time. The system reliability design philosophy and procedure used to determine backup capability was the classical approach. Having established the reliability goals and failure rates for each functional part within the proposed configuration, a prediction model was developed to determine the necessary redundancy. A partial list of predicted values is presented in Figure 9 along with observed MTBF's.

While the overall system contains redundant functions as well as redundant stations, the prediction of the line reliability involved consideration of the availability allocation problem of ten lines being operational. The principal parts and failure rates were determined. A computation of the time required for the maintenance of each part was then made to determine the expected maintenance time for the prime data lines. Then, the probability of having ten good lines out of "n" total lines to obtain an overall reliability of 0.9995 (regardless of the order of failure occurrence for mutually exclusive events) was calculated by using the binomial distribution.

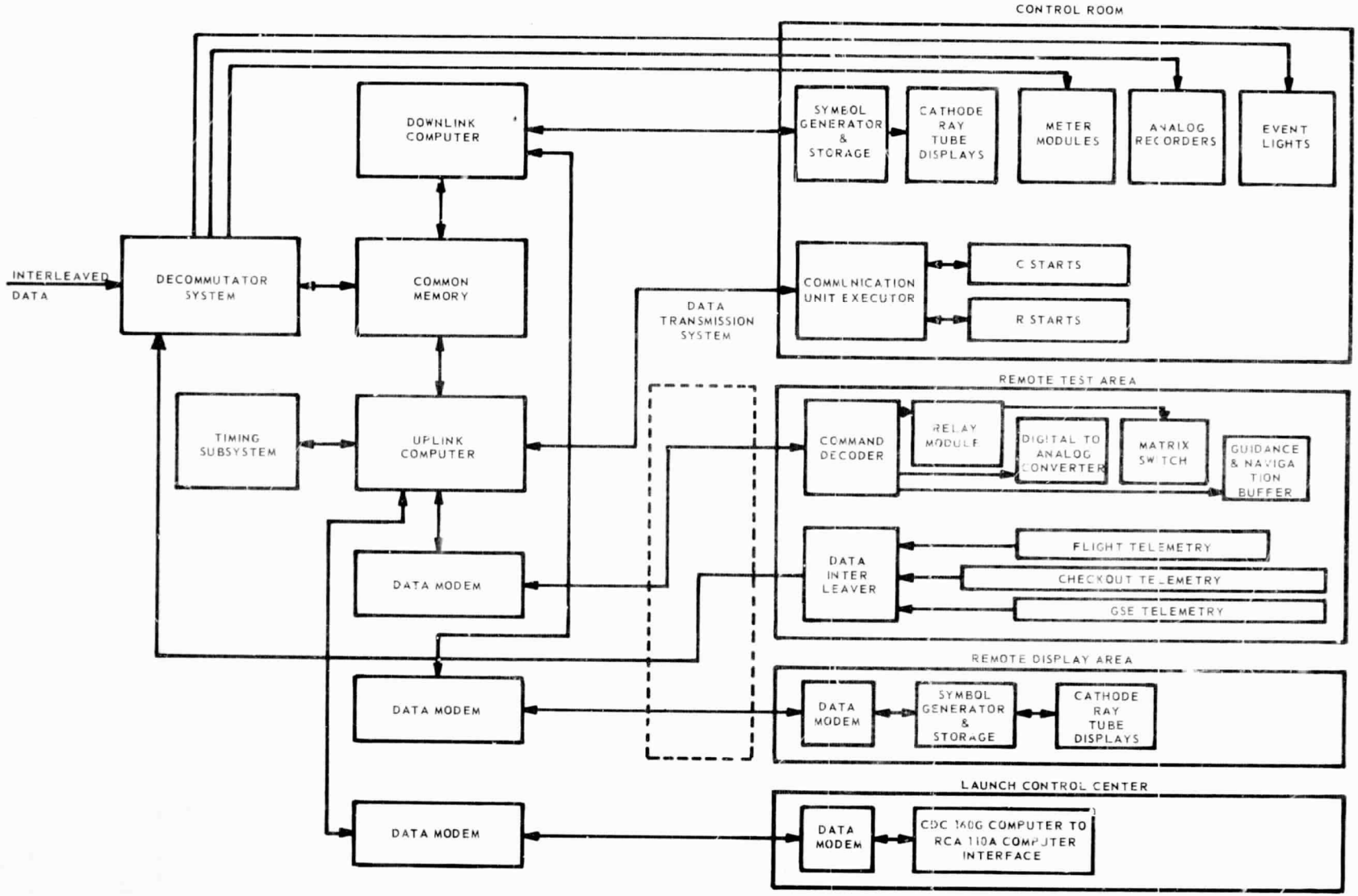

Figure 8. Initial Checkout Station Configuration

ACE-S/C Components	MTBF in Hours Measured Through 1969	Predicted MTBF in Hours in 1962
Decommutator	600	267
Data Display, Inc., Symbol Generator and Storage	1,008	1,112
Control Data Corp., 160G Computer	1,112	1,138
Magnetic Tape Transport	3,029	2,007
Memory Module	3,591	4,098
Digital Communications and Control Unit	3,900	6,000
Magnetic Tape Control	4,460	1,968
Computer Console	4,993	13,315
Digital Transmission and Verification Converter	5,700	9,430
Input/Output Module	7,230	4,566
Decommutator to Computer Interface	15,000	12,000
Analog Recorders	15,180	7,250
Communication Unit Executor	32,000	11,800
Computer Communication START	32,000	65,443
Relay Selection START	110,000	209,237
Power Supplies	220,000	55,000
Control Room Power Supplies	293,202	55,000
Event Module	370,721	170,000
Meter Module	9,000,000	5,000,000

Figure 9. Mean Time Between Failures for ACE-S/C Components

The equation for the binomial distribution is as follows:

$$f(x) = \binom{n}{x} p^x q^{(n-x)} = \frac{n!}{x!\,(n-x)!} p^x q^{(n-x)}$$

where: f (x) is the probability density distribution function

x = operational lines

n = total number of lines

p = probability of successful operation

q = probability of a failure that would degrade the system reliability

This means that ten lines and two spare lines are required to better the 0.9995 system reliability requirements. Further, the analysis revealed that the incorporation of selective component redundancy in the spacecraft peripheral equipment would be required to meet the reliability goals.

Once the configuration and optimum arrangement had been achieved and hardware became available, it was logical to concentrate upon maximum component reliability. A vigorous field evaluation with accurate and timely nonconformance reporting resulted in meaningful corrective action. Each failure was analyzed and tracked to determine component characteristics of sensitivity or insensitivity to the usage environments. When a group of parts exhibited an abnormal failure rate, they were removed. Then it was observed that by continuous failure screening the remaining population of component failures diminished in a linear fashion. Those wearout failures characterized by irreversible processes with only moderate periods of time were provided for by imposing low stresses and developing a parts replacement plan which removes these parts just short of the impending wearout phase. This allows the assumption that in the ACE-S/C, only a constant failure rate exists in the system.

CONCLUSION

The manned Apollo Program is based upon maximum use of man's unique capabilities such as observation, analysis, decision-making, and control, while simultaneously relieving him of any tasks which could be better accomplished by machine. The utilization of this concept resulted in flight and ground-based system efficiency and flexibility which could not have been attained otherwise, and which exceeded the capabilities that could be attained in a fully automatic system.

The applications of the principles involved have been illustrated in the discussion of the ACE-S/C subsystem. The operational capabilities of the ACE-S/C subsystem include the acquisition of data, its running collation with all pertinent stored historical information, mechanical analyses, and immediate display in a meaningful manner and in such rapid sequence to a specialized human monitor, that the illusion of real-time

operation is created. Monitors are representatives of systems engineering groups and maintain full control of all checkout operations at all times. The monitoring operation puts them in a position to advise the astronaut on how to utilize his flight equipment in the most efficient manner.

Reliability considerations were given high priorities throughout all phases of design and development of the ACE-S/C subsystems. The success of the hardware performance confirms the effectiveness of the reliability effort and establishes a baseline for future development programs.

The technical capabilities developed in the ACE-S/C subsystem have applications beyond the Space Program to many major problems facing our society. The transfer of technology from the Space Program by the application of these techniques to civilian earthbound systems can result in appreciable benefits.

REFERENCES

1. Parsons, W. E.; Johnson, Harold G.; and Woods, Gary J., "PACE: Preflight Acceptance Checkout Equipment." Astronautics and Aerospace Engineering, Easton, Pennsylvania: American Institute of Aeronautics and Astronautics, July, 1963, p. 51.

2. Myers, Richard H.; Wong, Kam L.; and Gordy, Harold M. Reliability Engineering for Electronic Systems. New York: John Wiley and Sons, Inc., 1964.

3. Zegan, Peter James, Optimizing the Utilization of Redundancy of the Apollo Acceptance Checkout Equipment, A Thesis presented to the University of Florida toward the Degree of Master of Science, Gainesville, Florida, 1970.

4. Goodman, David M., Automation in Electronic Test Equipment, Vol. VI: Article by William C. Bradford, NASA, Houston, "Acceptance Checkout Equipment for Spacecraft, ACE-S/C," p. 149; Article by Walter T. Murphy, NASA, Houston, "ACE-S/C Programming System," p. 173, New York: New York University Press, 1968.

5. Apollo Panel Pre-Flight Operations Division, Spacecraft Pre-Launch Automatic Checkout Equipment (SPACE), Cape Canaveral, Florida: Manned Spacecraft Center, National Aeronautics and Space Administration, 1962.

6. Ryerson, C. M. Lower Level Testing and Parts Screening, Culver City, California: Hughes Aircraft Company, 1969.