APPLICATION OF REDUNDANCY IN THE SATURN V GUIDANCE AND CONTROL SYSTEM

F. B. Moore and J. B. White
Guidance and Control Division, Astrionics Laboratory
NASA, George C. Marshall Space Flight Center
Huntsville, Alabama

Abstract

The Saturn launch vehicle's guidance and control system is so complex that the reliability of a simplex system is not adequate to fulfill mission requirements. Thus, to achieve the desired reliability, redundancy encompassing a wide range of types and levels was employed. At one extreme, the lowest level, basic components (resistors, capacitors, relays, etc.) are employed in series, parallel, or quadruplex arrangements to insure continued system operation in the presence of possible failure conditions. At the other extreme, the highest level, complete subsystem duplication is provided so that a backup subsystem can be employed in case the primary system malfunctions. In between these two extremes, many other redundancy schemes and techniques are employed at various levels. Basic redundancy concepts are covered to gain insight into the advantages obtained with various techniques. Points and methods of application of these techniques are included. The theoretical gain in reliability resulting from redundancy is assessed and compared to a simplex system. Problems and limitations encountered in the practical application of redundancy are discussed as well as techniques verifying proper operation of the redundant channels. As background for the redundancy application discussion, a basic description of the guidance and control system is included.

Nomenclature

A	ratio of failures detected by current sensing to all failures in a duplex memory
F	number of units that have failed in a simplex system after time t
k	environmental adjustment factor
m	total number of trials in simulated sampling
N	number of remaining good elements in a simplex system after time t
N_d	number of duplex memory pairs in series
N_i	number of components of type i
N_o	number of components or elements comprising a simplex system
n	number of modules in a simplex computer
$P, \overline{P}$	probability of success and failure, respectively, of a redundant arrangement or system
P_a	actual but unknown system reliability
P_e	estimated reliability obtained through sampling
P_g	reliability gained by considering failures in opposite directions cancelling in a TMR digital arrangement
P_h, $P_{h'}$	probability that the h and h' converter, respectively, in a duplex power supply is good
$\overline{P}_{h\ low}$, $\overline{P}_{h'\ low}$	probability that the h and h' converter, respectively, in a duplex power supply fails low
$p_1, p_2, \cdots p_n$	probability that the events, $\xi_1, \xi_2, \cdots \xi_n$, respectively, will occur
$R, \overline{R}$	probability of success (or reliability) and failure, respectively, of a simplex unit
R_1, R_2	reliability of memory modules 1 and 2, respectively, of a duplex pair
R_a, R_b, R_c, R_d	probability of success of a simplex unit denoted by the subscript
$\overline{R}_{a1}, \overline{R}_{b1}, \overline{R}_{c1}$	probability that the a, b, or c unit, respectively, fails to a logical "1"
R_{a0}, R_{b0}, R_{c0}	probability that the a, b, or c unit, respectively, fails to a logical "0"
R_e, R_f	reliability of a power supply (or excitation source) and a simplex feedback amplifier, respectively
R_h, R_k	reliability of a simplex converter and the accelerometer encoder and signal conditioning circuitry, respectively
R_i, R_j	reliability of the logic and an actuator-servoamplifier channel, respectively
R_m, R_o	multiplexer and oscillator reliability, respectively

R_q, R_s	reliability of the subtract and limit check circuitry and a switch, respectively
R_t	reliability of platform sliprings, gimbal angle resolver, and two crossover detectors
R_v, R_w	reliability of a decision element (or voter) and a hydraulic supply, respectively
$R_{\dot{\varphi}}$, R_{Ψ}	reliability of an attitude rate command channel and an attitude command channel, respectively
S	possible states of an element
T, t	total mission time and operating time, respectively
t_{ik}	time at which the k^{th} failure of i^{th} type component occurs
U	unreliability or probability of system failure, expressed in terms of failures per million
U_r	unreliability of a redundant arrangement, expressed in failures per million
U_{ra}	unreliability of the redundant platform system through the orbital injection phase, expressed in failures per million
U_{rb}	unreliability of the redundant platform system during earth orbit and lunar injection phase, expressed in failures per million
U_{rab}	unreliability of the redundant platform system during all flight phases, expressed in failures per million
U_{rp}	unreliability of the redundant portion of an arrangement containing both redundancy and simplex units, expressed in terms of failures per million
U_s	unreliability of a simplex subsystem or system, expressed in failures per million
U_{sp}	unreliability of the simplex portion of an arrangement containing both redundancy and simplex units, expressed in terms of failures per million
V_a, V_b, V_c	decision element state denoted by the subscript
Z_c	confidence limit expressed in terms of standard deviations
λ, λ_i	unit failure rate and failure rate of the i^{th} component, respectively
ξ_1, ξ_2, --- ξ_n	independent events with probabilities p_1, p_2, --- p_n, respectively

Introduction

The development of the Saturn V launch vehicle system may be traced through successive developments of the Saturn I and Saturn IB vehicles, which consist of two propelled stages and an Instrument Unit. The first stage (S-I) of Saturn I consisted of eight engines with a combined thrust of 6.7×10^6 N (1.5 million lb); the second stage (S-IV) has six LH_2/LOX engines with a total thrust of 0.4×10^6 N (90,000 lb). A boilerplate of the Apollo spacecraft was flown with Saturn I. The first stage (S-IB) of Saturn IB has the same basic eight engine configuration as the Saturn I, but the engines have been modified to increase performance to a total thrust of 7.1×10^6 N (1.6 million lb). The second stage (S-IVB) of Saturn IB has one large LH_2/LOX engine with a thrust of 0.9×10^6 N (200,000 lb). The Instrument Unit in both vehicles provides guidance and control, vehicle sequencing, telemetry, and other instrumentation.

The Saturn IB system, whose maiden flight occurred early in 1966, bridges the gap between the Saturn I and Saturn V vehicles. This system consists of concepts and hardware developed for the Saturn I program and incorporates new ideas, techniques, and hardware required in the Saturn V system. It has the capability of orbiting the Apollo spacecraft.

In the Saturn V system, which is being developed to place a man on the moon, the second stage (S-IVB) of the Saturn IB vehicle moves up to become the third stage. Likewise, the Instrument Unit and the payload remain basically intact and make up the forward portion of the vehicle. The first stage (S-IC) consists of five newly developed engines; each has a thrust approximately equivalent to that of the total Saturn I first stage, and the total thrust is 33.5×10^6 N (7.5 million lb). The second stage (S-II) is being developed with five LH_2/LOX engines, each with a thrust equivalent to that used on the S-IVB stage; the total thrust is 4.5×10^6 N (1.0 million lb). The Instrument Unit of the Saturn V vehicle is basically equivalent to that of Saturn I and IB with slight modifications or equipment rearrangement to accommodate and facilitate the Apollo mission. The Saturn V guidance and control system discussed applies generally to the Saturn IB system as well.

The primary mission of the Apollo project is to place three astronauts in a lunar orbit, to land two of the astronauts on the moon's surface, and to safely return the crew to the earth's surface. The Saturn V launch vehicle is instrumental in the first phase of this operation for it is the vehicle system that will inject the spacecraft and its crew into the lunar trajectory. Since

so much is at stake in this project, both in terms of the lives of entire crews as well as the tremendous expense of such an undertaking, it is imperative that each mission be successfully completed. Considerable effort has been expended from the outset of the conceptual design phase to insure that the Saturn V launch vehicle is as reliable as today's technology permits. In many cases, the technology has been extended considerably to meet the stringent reliability requirements for these complex missions. In addition to the Apollo mission, it is expected that the Saturn V vehicle system will be required for other critical earth orbit and possibly interplanetary missions.

Major emphasis has been placed on attaining the highest reasonable reliability in the development of the flight-critical guidance and control system of the Saturn V launch vehicle. The emphasis on reliability has overshadowed other design considerations such as minimized weight, power consumption, and, to some extent, cost.

Historically, reliability improvement has been attacked through simplicity in concept, conservative design, high reliability component parts, and extensive testing programs and techniques. These basic principles have been extensively employed in the guidance and control system design. The number and type of functional units required to fulfill the prescribed mission have been kept to the absolute minimum. The hardware in the Saturn system is conservatively designed with flight-proven components and techniques being employed to the maximum extent. In spite of the conservatism and emphasis on simplicity employed in the basic system layout and detailed hardware design, the implemented system is still extremely complex, consisting of millions of component parts which must operate over extended periods of time. Therefore, redundancy is required to achieve the desired reliability.

Basic Redundancy Concepts

Within the past two decades, tremendous strides have been made in improving component part reliability. The transistor demonstrated a marked reliability improvement in comparison to the electronic tube; and, in more recent years, microminiaturization and integrated circuits have contributed significantly to electronic circuit reliability improvement. However, even with this advancement in basic technology, overall system reliability has not improved sufficiently to meet today's demand for the following reasons. First, the number of component parts in today's systems has increased significantly compared to those of a few years ago. Second, reliability requirements have increased considerably because of man-rated systems and the necessity of extended periods of operation. For these reasons, new techniques utilizing redundancy concepts have been developed. The concepts themselves are not new and were investigated by J. von Neumann and others; however, only recently have they been employed on such a large scale. The Saturn V guidance and control system represents the largest scale application of redundancy that exists in any present flight system.

The types of redundancy employed fall into the following categories: duplex, triple modular redundant (TMR), prime-reference-standby (PRS), quadruplex, and multiple parallel elements (MPE). Each approach is discussed to point out the reliability improvement obtained.

Three axioms of probability theory useful in the following derivations of reliability are as follows.

1. If p denotes the probability that an event will occur, then 1-p denotes the probability that the event will not occur.

2. If the events ξ_1, ξ_2, --- ξ_n are independent events with probabilities p_1, p_2, --- p_n, respectively, then the probability that all of the events should happen simultaneously when all are in question is the product of the probabilities

$$p = \prod_{i=1}^{n} p_i . \qquad (1)$$

3. If the probabilities of mutually exclusive events ξ_1, ξ_2, --- ξ_n are p_1, p_2, --- p_n, respectively, then the probability that any one of these events should happen when all are in question is the sum of the probabilities

$$p = \sum_{i=1}^{n} p_i . \qquad (2)$$

The reliability or probability of success of a single unit, whether a single component or a system, will be represented by R, and the reliability of the redundant arrangement by P. It is assumed that the equipment under discussion has been operated through a burn-in phase and does not have or has not reached the wearout phase. The reliability can therefore be conveniently expressed as a time dependent function. The expression relating reliability to time may be simply derived as follows.

Consider that N_o integral units, either single components or subsystems, comprise a system. Assume that each unit is functioning independently of the others and that the number of units which have failed at time t is F. Then, the number of good units (N) remaining after time (t) is

$$N = N_o - F . \qquad (3)$$

Assuming that the failure rate of the units is directly proportional to the number of good units results in

$$\frac{dF}{dt} = \lambda N \qquad (4)$$

where λ is the constant of proportionality and is commonly referred to as unit failure rate.

Substituting equation 3 into equation 4 results in

$$\frac{dF}{dt} = \lambda (N_o - F) . \qquad (5)$$

Solving this differential equation for F and evaluating the solution at t = 0 and F = 0 for the constant of integration yields

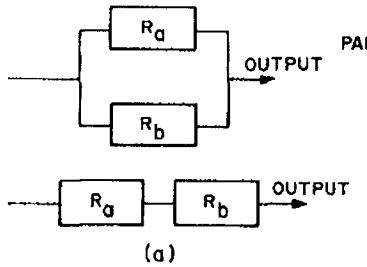
$$F = N_o (1 - e^{-\lambda t}) . \qquad (6)$$

If a unit is selected from the set, the probability that it has failed is, by definition, F/N_o; from axiom 1 the probability that it is good is $1 - F/N_o$ or from equation 4 is given by

$$R = e^{-\lambda t} \qquad (7)$$

The simplest and lowest level of redundancy utilized is that which duplicates a component part to prevent a system failure in the presence of a short or open of the component. With a component that tends to fail in the shorted mode, an additional component would be added in series; likewise, for a predominant open failure mode, a parallel component would be added. These arrangements are shown symbolically in Figure 1; the truth table represents the possible states of the units. The total number of combinations of states is derived from S^n, where S is the number of possible states and n is the number of units. In this arrangement, there are two states since each unit can either be good or bad, and the number of units is two, giving four possible combinations. If in the truth table a "0" is interpreted as a failure in the predominant mode and a "1" represents an operative unit, the same table applies to both the series and parallel combinations.

Truth tables, which are of primary importance in the design of logical systems, are useful in enumerating the possible combinations or states of a system and selecting the combinations which result in a system failure as well as indicating the assumptions and failure modes in each case. With a truth table and axioms 1, 2, and 3, the Boolean expression for system reliability can be readily derived. This technique will be used throughout to derive the reliability expressions.



TRUTH TABLE FOR SERIES OR PARALLEL COMPONENTS

R_a	R_b	SYSTEM STATUS
0	0	FAILED
0	1	OPERATIVE
1	0	OPERATIVE
1	1	OPERATIVE

(b)

Figure 1. Series and Parallel Configuration with Truth Table

The probability that the system is operative is given by

$$P = \bar{R}_a R_b + R_a \bar{R}_b + R_a R_b . \qquad (8)$$

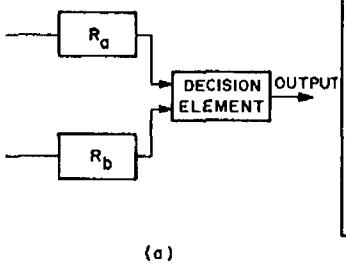
Assuming $R = R_a = R_b$, we obtain

$$P = (1-R)\ R + R\ (1-R) + R^2 = 2R - R^2 . \qquad (9)$$

The reliability of the system as a function of time and unit failure rate is obtained by substituting equation 7 into equation 9 which results in

$$P = e^{-\lambda t} (2 - e^{-\lambda t}) . \qquad (10)$$

The duplex arrangement can also be employed at the module and subsystem level, where a single predominant failure mode cannot be assumed to exist. In this arrangement a decision element to determine which channel is operating correctly must be added. Consider a duplex arrangement, composed of identical units, and a decision element with the ability to determine which of the two units is good in case of a unit failure. This is shown symbolically in Figure 2; the truth table represents the possible states of the unit.



TRUTH TABLE FOR DUPLEX UNITS

R_a	R_b	DECISION ELEMENT STATE	SYSTEM STATUS
0	0	B	FAILED
0	0	A	FAILED
0	1	B	OPERATIVE
0	1	A	FAILED
1	0	B	FAILED
1	0	A	OPERATIVE
1	1	B	OPERATIVE
1	1	A	OPERATIVE

(b)

Figure 2. Duplex Configuration with Truth Table

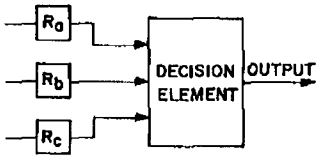
In the truth table, a "0" is interpreted as a failed unit and a "1" represents an operative unit. The A or B in the decision element state column indicates which element has been selected. It has been assumed that the decision element must select one element, but that both cannot be selected simultaneously. The logical conditions necessary for the system to be operative are $\bar{R}_a \cdot R_b \cdot V_b + R_a \cdot \bar{R}_b \cdot V_a + R_a \cdot R_b \cdot V_b + R_a \cdot R_b \cdot V_a$ where V_b and V_a indicate which unit has been selected. The reliability of the duplex system, when the reliability of the decision element is considered, is given by

$$P = R^2 + 2\ (R - R^2)\ R_v \qquad (11)$$

where R_v is the decision element reliability. This equation reduces to that for the series or parallel cases (equation 10) if the reliability of the decision element is ignored; i.e., it has a reliability of one.

The duplex technique is one of the most desirable forms of redundancy, both in terms of simplicity and reliability improvement. However, the major disadvantage which limits its application considerably is the problem of determining the functional unit when a failure has occurred. The techniques used in the Saturn system to overcome this shortcoming are discussed later.

A triplex, or triple modular redundant (TMR), arrangement is shown in Figure 3. In this system the decision element, sometimes called voter, reacts to the majority inputs; consequently, only one failure can be tolerated.



(a)

TRUTH TABLE FOR TMR UNITS

R_a	R_b	R_c	SYSTEM STATUS
0	0	0	FAILED
0	0	1	FAILED
0	1	0	FAILED
0	1	1	OPERATIVE
1	0	0	FAILED
1	0	1	OPERATIVE
1	1	0	OPERATIVE
1	1	1	OPERATIVE

(b)

Figure 3. TMR Configuration with Truth Table

Four of the combinations result in system failure while the other four yield proper operation. The Boolean expression for proper operation is

$$P = \bar{R}_a R_b R_c + R_a \bar{R}_b R_c + R_a R_b \bar{R}_c + R_a R_b R_c \quad (12)$$

indicating that only one failure can be tolerated. Therefore, assuming identical units, the reliability of the system is given by

$$P = 3\,(1-R)\,R^2 + R^3 = 3R^2 - 2R^3. \quad (13)$$

The reliability of the decision element in a TMR arrangement may be considered in one of two ways. If three decision elements are used per trio, i.e., one for each element, the reliability of the voter may be lumped with that of the unit. The reliability of the unit then is decreased accordingly. If a single decision element is used for a trio, the result is a trio in series with a single element resulting in a reliability given by

$$P = (3R^2 - 2R^3)\,R_v \quad (14)$$

where R_v is the voter reliability. In either case, when the voter is assumed to be perfect, $R_v = 1$, the reliability of the system is given by equation 13.

Where TMR techniques are utilized in digital applications, advantage can be taken of the possibility of failures in opposite directions cancelling. For example, the second combination in the truth table (Fig. 3) would not have resulted in a system failure if R_a had failed to a logical "0" and R_b to a logical "1," or if R_a had failed to a logical "1" and R_b to a logical "0." This may be expressed in the form

$$\bar{R}_{a0} \cdot \bar{R}_{b1} \cdot R_c + \bar{R}_{a1} \cdot \bar{R}_{b0} \cdot R_c$$

where the second subscript indicates failure mode. Since this can occur in three such combinations, the Boolean expression for the reliability gained by opposite failures cancelling is

$$P_g = \bar{R}_{a0} \cdot \bar{R}_{b1} \cdot R_c + \bar{R}_{a1} \cdot \bar{R}_{b0} \cdot R_c + \bar{R}_{a0} \cdot R_b \cdot \bar{R}_{c1} +$$

$$\bar{R}_{a1} \cdot R_b \cdot \bar{R}_{c0} + R_a \cdot \bar{R}_{b0} \cdot \bar{R}_{c1} + R_a \cdot \bar{R}_{b1} \cdot \bar{R}_{c0}. \quad (15)$$

The probability of unit failure is the sum of the probabilities of component failures to a "0" state and to a "1" state; thus $\bar{R} = \bar{R}_0 + \bar{R}_1$. Without investigating the details of a specific application there is no reason to suspect a failure to any particular state to be more prevalent than to the other state; consequently, $\bar{R}_0 = 1/2\,\bar{R}$ and $\bar{R}_1 = 1/2\,\bar{R}$. This leads to the conclusion that $\bar{R}_0 = 1/2\,(1-R)$ and $\bar{R}_1 = 1/2\,(1-R)$. Substituting these values into equation 15 yields the reliability gained from consideration of failures in opposite directions and is given by

$$P_g = 6\,[(R)\ 1/2\,(1-R)\ 1/2\,(1-R)]$$

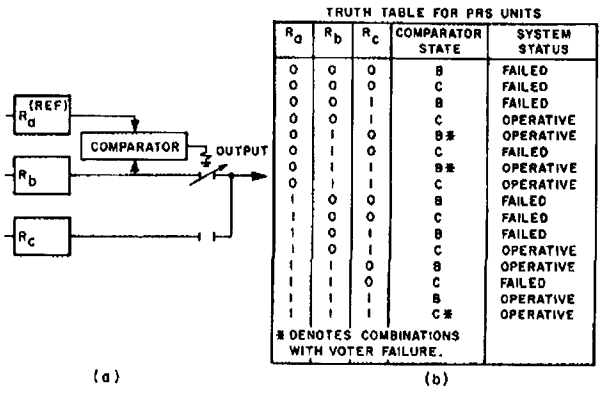
$$= \frac{3R}{2}\,[(1-2R+R^2)]. \quad (16)$$

The reliability of a TMR system when failures in opposite directions are considered is given by the sum of equations 13 and 16 yielding

$$P = (3R^2 - 2R^3) + \left(\frac{3R}{2} - 3R + 3/2\,R^3\right)$$

$$= 1/2\,(3R - R^3). \quad (17)$$

Another redundancy scheme is the primary-reference-standby (PRS) technique employing three channels that serve, as the name implies, three separate functions. In the normal unfailed condition, the primary channel B is functional in the system. Its output is compared to the reference A; and, in case of disagreement beyond an established level, the standby channel C is substituted for B. This scheme along with its truth table is shown in Figure 4.



TRUTH TABLE FOR PRS UNITS

R_a	R_b	R_c	COMPARATOR STATE	SYSTEM STATUS
0	0	0	B	FAILED
0	0	0	C	FAILED
0	0	1	B	FAILED
0	0	1	C	OPERATIVE
0	1	0	B*	OPERATIVE
0	1	0	C	FAILED
0	1	1	B*	OPERATIVE
0	1	1	C	OPERATIVE
1	0	0	B	FAILED
1	0	0	C	FAILED
1	0	1	B	FAILED
1	0	1	C	OPERATIVE
1	1	0	B	OPERATIVE
1	1	0	C	FAILED
1	1	1	B	OPERATIVE
1	1	1	C*	OPERATIVE

* DENOTES COMBINATIONS WITH VOTER FAILURE.

Figure 4. PRS Configuration with Truth Table

Again it has been assumed that the comparator has selected either B or C, but that it cannot select both simultaneously. The necessary logical conditions for this system to be operative are

$$\bar{R}_a \cdot \bar{R}_b \cdot R_c \cdot V_c + \bar{R}_a \cdot R_b \cdot \bar{R}_c \cdot V_b + \bar{R}_a \cdot R_b \cdot R_c \cdot V_b$$

$$+\bar{R}_a \cdot R_b \cdot R_c \cdot V_c + R_a \cdot \bar{R}_b \cdot R_c \cdot V_c + R_a \cdot R_b \cdot \bar{R}_c \cdot V_b$$

$$+R_a \cdot R_b \cdot R_c \cdot V_b + R_a \cdot R_b \cdot R_c \cdot V_c$$

where V_b and V_c indicate which element has been selected. When the units are assumed to be identical, the reliability of the system is given by

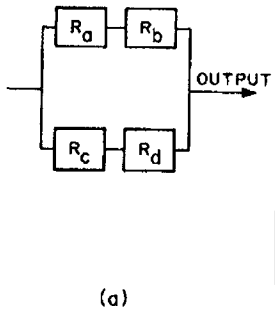
$$P = (R^3 - R^2)\ (1 - 2R_v) + R \qquad (18)$$

where R_v is the comparator reliability. If the comparator is assumed to have a reliability of one, equation 18 reduces to

$$P = R\,(1 + R - R^2)\,. \qquad (19)$$

The PRS technique has a major disadvantage in that is is more susceptible to transients or intermittents than the other schemes. Consequently, if a transient causes the comparator to switch to the standby unit, means should be available to switch back to the original unit with its reference; otherwise all the advantages of the redundant system have been lost from that point on. As discussed later, the switchback technique is employed in some PRS portions of the Saturn system but not in others.

The next technique to be considered is the quadruplex arrangement shown with its truth table in Figure 5. Since the arrangement has four units, 2^4 combinations are possible. In Figure 5, assume that only one failure in each or in both branches can be tolerated, and two failures in any one branch will result in a system malfunction.



TRUTH TABLE FOR QUADRUPLEX UNITS

R_a	R_b	R_c	R_d	SYSTEM STATUS
0	0	0	0	FAILED
0	0	0	1	FAILED
0	0	1	0	FAILED
0	0	1	1	FAILED
0	1	0	0	FAILED
0	1	0	1	OPERATIVE
0	1	1	0	OPERATIVE
0	1	1	1	OPERATIVE
1	0	0	0	FAILED
1	0	0	1	OPERATIVE
1	0	1	0	OPERATIVE
1	0	1	1	OPERATIVE
1	1	0	0	FAILED
1	1	0	1	OPERATIVE
1	1	1	0	OPERATIVE
1	1	1	1	OPERATIVE

Figure 5. Quadruplex Configuration with Truth Table

Inspection of the truth table for the quadruplex arrangement reveals that the system reliability may be obtained by

$$P = 1 - (1-R)^4 - 4(1-R)^3 R - 2(1-R)^2 R^2$$

$$= R^2\,(4 - 4R + R^2). \qquad (20)$$

The quadruplex arrangement is most useful when applied at the component level, i.e., to resistors, capacitors, diodes, valves, relays, etc., where the component does not have a single predominant failure mode. In applications where a single failure mode exists, two components in series or parallel would be employed in preference to the quadruplex arrangement.

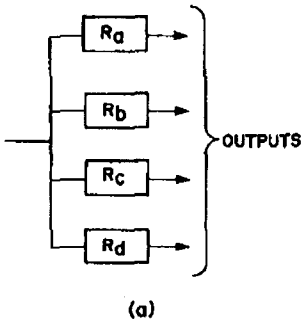
An inherent redundancy exists in some subsystems because of certain features of the overall system configuration dictated by other subsystems. In such cases the subsystem may continue to operate either with no degradation or with an acceptable degradation of performance in the presence of one or more failed elements. An example of such a situation exists in the Saturn guidance and control system because of the required clustering of engines to provide the necessary vehicle thrust. Since four engines are gimbaled to maintain vehicle control, the failure of one of the four control channels in each plane does not cause a system failure. The subsystem can be treated as one having four parallel elements, with the failure of any one element being permissible. This arrangement is referred to as multiple parallel elements (MPE). The applicable schematic and truth table are shown in Figure 6. Five combinations in Figure 6 result in continued successful operations. The resulting expression for proper operation is

$$P = \bar{R}_a\, R_b\, R_c\, R_d + R_a\, \bar{R}_b\, R_c\, R_d + R_a\, R_b\, \bar{R}_c\, R_d$$

$$+ R_a\, R_b\, R_c\, \bar{R}_d + R_a\, R_b\, R_c\, R_d\,.$$

Again, assuming identical units results in

$$P = 4(1-R)\, R^3 + R^4 = 4R^3 - 3R^4. \qquad (21)$$



(a)

TRUTH TABLE FOR MPE UNITS

R_a	R_b	R_c	R_d	SYSTEM STATUS
0	0	0	0	FAILED
0	0	0	1	FAILED
0	0	1	0	FAILED
0	0	1	1	FAILED
0	1	0	0	FAILED
0	1	0	1	FAILED
0	1	1	0	FAILED
0	1	1	1	OPERATIVE
1	0	0	0	FAILED
1	0	0	1	FAILED
1	0	1	0	FAILED
1	0	1	1	OPERATIVE
1	1	0	0	FAILED
1	1	0	1	OPERATIVE
1	1	1	0	OPERATIVE
1	1	1	1	OPERATIVE

(b)

Figure 6. MPE Configuration with Truth Table

Any of the redundant arrangements may be cascaded and the total system reliability may be found from axiom 2. For example, a system composed of two duplex subsystems similar to those in Figure 2 would have a reliability given by

$$P = (2R-R^2)^2. \tag{22}$$

Similarly, a system composed of a duplex subsystem and a TMR subsystem would have a reliability given by

$$P = (2R-R^2)\ (3R^2-2R^3). \tag{23}$$

To summarize, Table 1 shows the reliability expression for each scheme discussed in order of reliability preference. However, practical limitations usually determine the choice of schemes.

Table 1. Redundancy Schemes

Scheme	Reliability Expression	Assumptions
Duplex	$2R-R^2$	Proper decision element can be determined.
TMR	$1/2\,(3R-R^3)$	Failures in opposite directions can cancel.
PRS	$R\,(1+R-R^2)$	Reference and normally used unit do not fail to the same state simultaneously.
Quadruplex	$R^2\,(4-4R+R^2)$	Limited generally to component part application.
MPE	$4R^3-3R^4$	4 elements
Simplex	R	

In applying the theory to the assessment of the reliability of a complex system, it is sometimes more convenient to express reliability equations in terms of unreliability which can be derived from unit failure rates. The unreliability of each component, subsystem, or system is then expressed as a number of failures per unit of time, permitting easier separation or combination of the associated numbers without resorting to the manipulation of numbers involving a series of "nines."

Since R in the reliability expressions may be replaced by $1-\bar{R}$ where $\bar{R}$ is the probability of subsystem failure, the reliability of a redundant unit may be expressed in terms of the probability of failure of the single nonredundant unit. The result for each type of redundancy is as follows.

$$\begin{aligned}
&\text{Duplex} && P = 1-\bar{R}^2 \\
&\text{TMR} && P = 1/2\,[2-3\bar{R}^2+\bar{R}^3] \\
&\text{PRS} && P = 1-2\bar{R}^2+\bar{R}^3 \\
&\text{Quadruplex} && P = 1-2\bar{R}^2+\bar{R}^4 \\
&\text{MPE} && P = 1-6\bar{R}^2+8\bar{R}^3-3\bar{R}^4
\end{aligned} \tag{24}$$

Further, $R = e^{-\lambda t}$ and $\bar{R} = 1-e^{-\lambda t} \approx 1-(1-\lambda t+\cdots) \approx \lambda t$, for very small λt. Since in equations 24, $\bar{R}$ is also very small, terms higher than the second order may be ignored. If the higher order terms are ignored, the approximations for redundant system unreliability expressed in terms of component failure rates and operating time are

$$\begin{aligned}
&\text{Duplex} && \bar{P} \approx (\lambda t)^2 \\
&\text{TMR} && \bar{P} \approx 3/2\,(\lambda t)^2 \\
&\text{PRS} && \bar{P} \approx 2\,(\lambda t)^2 \\
&\text{Quadruplex} && \bar{P} \approx 2\,(\lambda t)^2 \\
&\text{MPE} && \bar{P} \approx 6\,(\lambda t)^2
\end{aligned} \tag{25}$$

From equations 25, the ordering of the system in rank of reliability becomes obvious.

Figure 7 is a graphical comparison of the reliability of the simplex, duplex, TMR, PRS, MPE, and quadruplex schemes as a function of unit failure rate and time, where $R = e^{-\lambda t}$ has been substituted into the equations previously derived. In the case of the TMR arrangement, failures in opposite directions cancelling were assumed; for the PRS arrangement, it was assumed that the reference unit and the unit to which it is normally compared do not fail simultaneously to a state which cannot be detected by the comparator. The figure further substantiates the relative desirability of each scheme. The fact that a portion of the reliability curve of the quadruplex and MPE scheme falls below that of a simplex system is not significant because this occurs at a reliability far below that which would be permissible in a practical application. It is interesting to note that in the region above 0.9, the reliability of the quadruplex and PRS schemes is practically identical (equations 24 and 25).

Figure 8 further demonstrates the merits of redundant systems compared to a simplex system and indicates quantitatively what can be gained through the

various techniques. For convenience, unreliability in terms of failures per million is shown for both the simplex and redundant systems. In the reliability assessment and comparisons appearing in the following sections, the quantities are expressed in these terms.

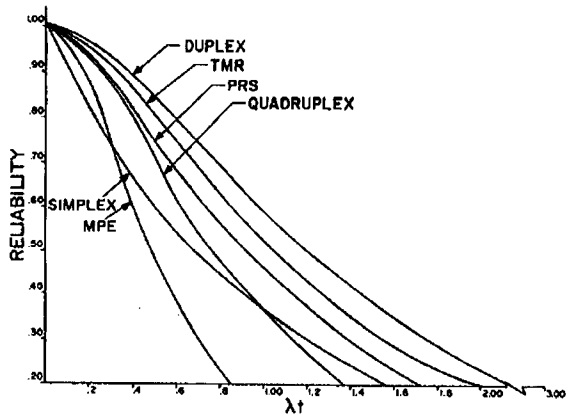


Figure 7. Reliability Versus λt for Various Redundancy Schemes

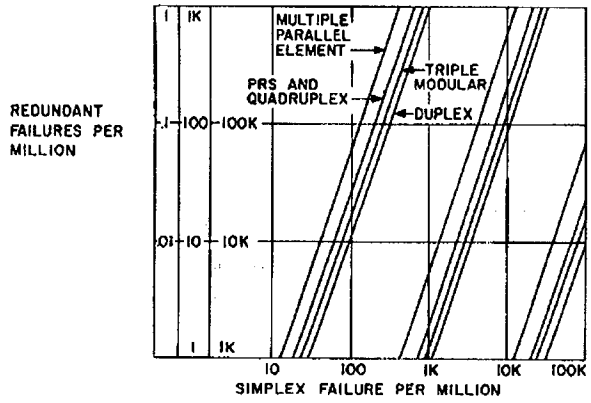


Figure 8. Redundant Failure per Million Versus Simplex Failures per Million for Various Redundancy Schemes

Guidance and Control System Description

The Saturn navigation, guidance, and control system is completely self-contained within the vehicle and utilizes onboard inertial sensors, computation, and control to direct the vehicle according to the desired path and end conditions. A digital command system is available as a part of the onboard astrionics system, but is not planned for use in the primary mode.

The navigation function is accomplished through the use of acceleration measurements provided by accelerometers mounted on the space-direction-fixed stable element of the stabilized platform. The resulting information is processed within the onboard digital computation system. The acceleration information is integrated to obtain vehicle velocity and position information. The current measured position information is used to continuously calculate and combine the gravitational effects with the measured data to obtain space-fixed vehicle velocity and position.

The guidance function, which is the computation of the necessary maneuvers to satisfactorily reach the specified end conditions, is accomplished within the onboard digital computer system. To give the desired result, the implemented guidance equations must take into account various mission and vehicle constraints, one of the most significant of which is that of propellant consumption optimization. The equations programed into the onboard digital computer system represent a path adaptive guidance scheme, termed the iterative guidance mode (IGM), which fulfills the optimization requirements and the guidance requirements for insertion both into earth orbit and injection into the lunar trajectory. The specific results of the guidance computation are as follows.

1. Instantaneous required thrust direction expressed as three Euler angles.

2. Required time of engine cutoff to achieve the specified orbital conditions.

3. Required time of engine ignition to leave earth orbit.

4. Required time of second cutoff to satisfy the lunar trajectory end conditions.

The required angular directions resulting from the guidance calculations are applied to the vehicle through the control system. In addition to responding to the commands of the guidance system, the control system must maintain stabilization of the vehicle attitude in the presence of various vehicle propellant sloshing, structural bending, and load constraints. The elements of the control system required to accomplish this task can be divided into three specific functional areas: sensing of vehicle state information, computation, and vehicle torquing. In the Saturn V system, the vehicle state information required is that of attitude and rate. (On the Saturn I and IB vehicles, additional information obtained through vehicle-fixed lateral accelerometers was required to obtain structural load relief.) The attitude information is obtained from resolvers mounted on the stabilized platform gimbals. The information on actual vehicle orientation from the resolvers is compared in the onboard digital computer system with the desired orientation determined from the guidance calculations, resulting in the desired attitude control commands. The three-axis attitude rate information required to accomplish vehicle stabilization is obtained from vehicle-fixed rate gyros.

The control "computation" consists of the gain modification, filtering, mixing input attitude and rate information, and shaping of this information to provide vehicle stabilization in the presence of structural bending, propellant sloshing, and other dynamic

characteristics. Routing of the control signals to the proper end element to develop the desired vehicle controlling torques is also part of this function.

Two methods are used to develop the control torques in the Saturn V vehicle. Positioning of the primary propulsion engines by hydraulic actuators is used to control pitch and yaw on each of the three stages. In addition, control about the roll axis is obtained on the first two multiengine stages by the proper differential positioning of the gimbaled engines. Roll control on the single-engine third stage, and control of this stage about all three axes during coasting phases, is accomplished by an array of fixed direction thrusters. Pulses of thrust from these low thrust devices are commanded by the control electronics to provide corrective control torques about the appropriate vehicle axes.

The basic elements of the navigation, guidance, and control system are shown in block diagram form in Figure 9, which indicates the primary form of redundancy employed in each element. For a more detailed description, the system is broken down into the digital computer subsystem, the stabilized platform subsystem, and the control subsystem. Each of these subsystems encompasses a number of hardware elements, with many performing a variety of functions in the overall system.

The major systems are broken down in some instances to the "black box" level and in others to a specific functional level, depending on which breakdown is more convenient and appropriate to illustrate the application of redundancy. Although no attempt is made to describe in detail the total application of redundancy, examples of the different types are cited and described in each subsystem. Where available, reliability numbers are shown for the various modules in the sub-

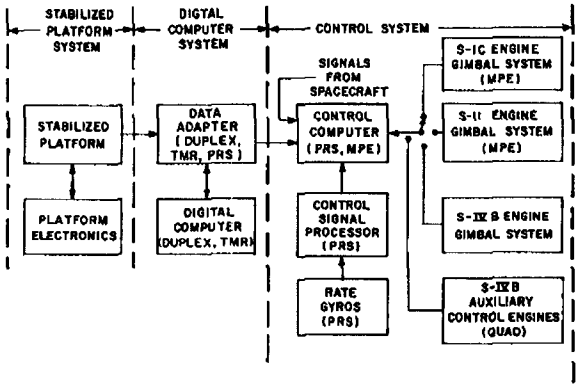


Figure 9. Saturn V Guidance and Control System

systems as well as for the total subsystems. The theoretical gain in reliability through redundancy is also shown in each case. Since the reliability assessments of various elements were conducted by different groups, the numbers may not be universally compatible. However, some adjustment of the failure rates has been effected where obvious discrepancies existed between the numbers set forth in the various references. In spite of these adjustments, caution should be exercised in using the reliability numbers presented, even though the numbers do indicate in gross terms the relative reliability of the various elements and subsystems. The prime intent is not to provide an accurate and intensive reliability analysis, but rather to illustrate the benefits of the various redundancy techniques employed.

The simplified equations previously developed are used where possible. In many instances, the simplifying assumptions made in the development of those equations do not apply; therefore, specific equations that apply to the particular situation must be developed.

For convenience, the module, subsystem, and system assessments are expressed in terms of unreliability. Through this approach, the relative contributions of the various elements can be more easily portrayed. Additionally, with the simplifying assumptions made, the unreliability numbers of the various subelements can be added directly to obtain the total unreliability.

As previously shown for highly reliable systems,

$$R \approx \lambda t.$$

This approximation can be made with an error less than $(\lambda t)^2/2$.

In component or system operation in a particular application, a degradation factor to account for the effect of the particular environment must be considered. This is generally called the environmental adjustment factor, designated by k. Therefore $\bar{R} \approx k\lambda t$. The unreliability numbers are expressed as $U = k\lambda t \times 10^6$ indicating the number of failures per million flights. Note that the term "failures" as expressed here is intended to designate component or system malfunctions or out-of-tolerance operation in a million flights; it does not indicate the number of vehicle or mission losses in a million flights. To obtain the latter, which is not covered in this analysis, the failure modes of the various elements and the effects of those failures on the vehicle behavior would have to be additionally considered. Table II shows the k-factors for the various stages and the phase times used in deriving the unreliability numbers.

Table II. Phase Times and k-Factor for Various Stages

Flight Phase	k-factor				Phase time (hrs)
	Location of Component				
	S-IC Stage	S-II Stage	S-IVB	IU	
S-IC Burn	1500	900	700	115	0.041
S-II Burn	-	900	700	45	0.106
First S-IVB Burn	-	-	700	45	0.046
Orbital Coast	-	-	10	1	4.5
Second S-IVB Burn	-	-	700	45	0.087
Translunar Coast	-	-	10	1	2.0

Digital Computer System

The digital computer system developed for the Saturn V vehicle consists of two basic units, a launch vehicle digital computer (LVDC) and a launch vehicle data adapter (LVDA). The LVDC is the basic computing element in the vehicle with the capability of performing arithmetic operations such as add, subtract, multiply, and divide; it provides the intelligence for making logical choices. The LVDA is essentially the LVDC input/output unit and all signals to and from the LVDC are processed in this unit. In addition, it performs certain simple computational and logical operations on data. The computer system is instrumental in all three phases of operation for the Saturn V vehicle; i.e., it plays a major role in the automatic checkout of the vehicle before launch, solves the guidance equations, provides attitude correction signals and vehicle sequences during the boost phase, and assists in vehicle checkout during the orbital coast phase.

The LVDC is a serial, fixed-point, stored program, general purpose machine with a basic clock of 2.048 MHz. Four clocks comprise a bit time and 14 bits a phase time. The machine is organized to operate around three phases or cycles. For example, data may be read from memory during one phase or cycle and operated upon during the next two cycles. Data words 28 bits in length (25 magnitude bits, 1 sign, and 2 parity bits) are used in computation. The memory, which contains from one to eight random-access magnetic core modules each consisting of 4096 data words, is arranged in such a manner that one data word or two instructions (each instruction contains a parity bit) may occupy one 28-bit memory word. Special algorithms have been developed and implemented for multiplication and division; multiplication is done four bits at a time and division is done two bits at a time. The system utilizes microminiature circuitry where power and accuracy requirements permit. Where microminiaturization cannot be employed, conventional discrete components are used.

During flight, the digital computer system inputs are (1) platform accelerometer outputs, (2) platform gimbal angles representing vehicle attitude, (3) discrete inputs indicating vehicle functions such as liftoff, first stage cutoff, separation, second stage ignition, second stage cutoff, and engine out, and (4) command receiver signals allowing memory alteration and ground control.

During flight, the digital computer system outputs are (1) steering or attitude correction commands, (2) discrete outputs commanding vehicle sequencing such as cutoff and separation, and (3) telemetry data words, 40 bits each, at a maximum rate of 240 per second for monitoring trajectory parameters and computer system operation.

Because of the critical functions performed by this system, every effort has been made to make it as reliable as possible. Many forms of redundancy have been incorporated into the system, which utilizes quadruplex components and circuits, and duplex, TMR, and PRS techniques as well as overall system backups. The system represents one of the largest scale applications of redundancy employed to date. The LVDC and LVDA form a complex system containing more than 95,000 equivalent electronic components. Of this number, less than one half of one percent are employed in such a manner that a single component failure would result in a system failure.

Figure 10 shows a simplified block diagram of the LVDC and indicates the redundancy techniques employed in that unit, with the corresponding unreliability indicated in each block. The fact that the TMR timing and logic depicted in Figure 10 is very much simplified is borne out when the TMR organization of the LVDC is considered in any detail. For example, since the TMR logic of the machine is considered to consist of seven functional modules, in the idealized case, it would be expected that 21 voters would be employed in the machine. However, because of the various feedback paths and the fact that each module has several output signals feeding various other modules, the idealized model cannot be employed accurately. For example, instead of 21 voters being employed in the LVDC timing and logic, approximately 155 signals are voted on, giving a total of 395 voters. The LVDA employs 237 voters in its TMR logic.

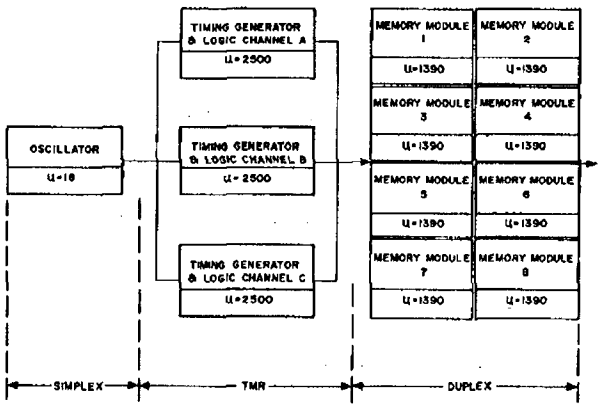


Figure 10. Block Diagram of the Launch Vehicle Digital Computer

67-553

Because of the relative simplicity of the basic 2.048 MHz oscillator (it contains only five electronic components) and the technical problems inherent in synchronizing multioscillators, a simplex oscillator system is employed in the LVDC. The output of the basic oscillator is used to form the necessary phasing and clock signals in the timing generator. Each channel of the TMR logic contains its own timing generator; consequently, a failure of the timing generator results in a failure of that channel. The memory system, expandable in modules of 4096 words, 28 bits in length, up to eight memory modules, is employed either in a duplex or simplex manner depending upon the criticality of the program being run. For instance, prelaunch programs are simplexed while flight routines are duplexed. From Figure 10, it is evident that the reliability of the LVDC may be approximated by

$$P = (R_o)\ (R_i)\ (R_m) \tag{26}$$

where R_o is the reliability of the simplex oscillator, R_i is the reliability of the combined TMR timing generator and logic, and R_m is the reliability of the duplex memories. The methods determining the reliability for each of these will now be considered.

The number of component parts in the system and their failure rate, the Saturn V mission time, and environmental conditions determine the unreliability of the oscillator which is $U_s = 16$.

The reliability for the timing generator and logic cannot be determined so simply for reasons indicated previously. Any attempt to accurately compute analytically the reliability of the timing generator and the complex logic it feeds, without making a great number of simplifying assumptions, would lead to a mathematical expression containing literally thousands of terms. Therefore, a method employing the Monte Carlo technique, which is basically a technique of simulated sampling, has been devised so that the reliability may be approximated.

Although the Monte Carlo technique is general and has been applied in many other fields, it represents a rather unique application in this particular field. Thus, a brief description of the basic procedures using this technique is in order; the evaluation procedures consist basically of three phases:

1. With simulation techniques, generate a set of failed components

2. Locate the computer subsystems containing the failed components

3. Trace the simulated failures through the logic to determine their consequence.

The first step consists of generating, by a random process, a set of failed components. If an exponential distribution of time to failure is assumed for a component, the probability of failure for that component is

$$\bar{R} = 1 - \epsilon^{-\lambda t} \tag{27}$$

where t is time and λ is the failure rate of the component. When the design contains N components of type i, the probability of failure becomes

$$\bar{R} = 1 - \epsilon^{-N_i \lambda_i t} \tag{28}$$

Solving equation 28 for t yields

$$t_{ik} = - \frac{\ln\ (1-\bar{R})}{N_i \lambda_i} \tag{29}$$

where t_{ik} is the time at which the k^{th} failure of component type i occurs. In each trial a random number between "0" and "1" is chosen and substituted for $\bar{R}$, and equation 29 is evaluated. The result is the time, t_{ik}, at which the first failure of component type i occurs. Then t_{ik} is compared to mission time T; if $t_{ik} < T$, a failure is recorded, N_i is reduced by one, and the process is repeated. As each t_{ik} is calculated, it is added to the sum of the previous t_{ik}'s and the new total is compared to mission time. The process is completed when the summation of the failure times exceeds the mission time, i.e., $\Sigma t_{ik} > T$.

Each of the i^{th} components in the system is assigned a number. The system's functional component that failed at time t_{ik} is determined by multiplying the random number generated by the total number of i components in the group; i.e., the random number chosen gives both time of failure and component that failed. This process is repeated for each component type in the system.

The second step consists of locating, within the logic framework of the machine, the component parts that failed. The third and final step consists of tracing the effects of the failed components, in the sequence in which they occur, upon the TMR logic. If in time T, the total combination of failures did not result in a system failure, a successful trial resulted. After many trials, the reliability of the system is then determined from

$$P = \frac{\text{number of successful trials}}{\text{total number of trials}}$$

The unreliability of the LVDC timing generator and logic using simulated sampling is $U_r = 10$. Approximately 20,000 "games" were played to determine this value. The confidence interval, which can be associated with this estimate as a function of the number of trials, is determined by

$$P_a = P_e \pm Z_c \sqrt{\frac{P_e\ (1 - P_e)}{m}} \tag{30}$$

where P_a is the actual but unknown reliability, P_e is the estimated reliability obtained from simulated sampling, Z_c is the confidence limit expressed in terms of standard deviations, and m is the total number of trials. From this, there is 90 percent confidence that $0 < U_r < 50$.

It is of interest to apply the simplified analytical technique derived earlier and to compare these results with those obtained from the Monte Carlo method. From the number of component parts in a simplex system and their failure rates and a Saturn V mission, the unreliability of a simplex computer timing and logic has been determined by Monte Carlo to be $U_s = 2500$.

A voter for a logic module adds approximately 25 percent to the number of component parts of that module; therefore, a simplex machine with enough component parts necessary for voters for one channel would have 25 percent more component parts than a simplex machine and would have a reliability given by

$$R = e^{-1.25n\lambda t}$$

where $n\lambda t = \ln (1-2500 \times 10^{-6})$. The unreliability of a simplex channel with voters then is $U_s = 3120$. If a simplex machine is divided into n modules, each of which has a reliability of $R^{1/n}$, and triplicated, the reliability of one trio as given by equation 17 is

$$P = 1/2 \left[3R^{1/n} - R^{3/n}\right]. \qquad (31)$$

Now, the reliability of a TMR machine consisting of n sets of triplicated modules is given by

$$P = 1/2\left[\left(3R^{1/n} - R^{3/n}\right)\right]^n. \qquad (32)$$

For the LVDC, since a simplex machine may be considered to have been divided in seven equivalent parts, n = 7, and R for each of the elements is 0.996880 as previously derived, the unreliability for the entire TMR logic is

$$U_r = 2.$$

Since in the ideal case it was assumed that the seven logic modules have equal reliabilities and that the logic was organized in such a manner to utilize 21 voters (neither of which is true in practice), it is expected that the ideal case would result in higher reliability than that obtained through simulated sampling. The more accurate result derived by Monte Carlo techniques for the LVDC is U = 10, which is used in the subsequent assessment.

The reliability of the LVDC toroidal core memory system may be found directly from component part count and failure rates using analytical means. Since a major problem in duplex systems often is failure detection mechanisms, it is of interest to note the type of failure detection employed in the LVDC memory system. The memory has two types of failure detection circuitry: odd parity checking and half select current monitoring. It is felt that parity checking will detect major failures in the sense amplifiers, cores, inhibit drivers, memory buffer registers, and variable strobe gate; while half select current monitoring will indicate major failures in the voltage and current drivers, decoupling circuitry, memory timing, and connection circuitry. Errors not determined by current checking, however, may be detected by parity checking.

The reliability of the memory system may be found directly from the relationship

$$P = \{R_1 + R_2 (1-R_1) [A + (1-A) (0.5)]\}^{N_d} \qquad (33)$$

where R_1 is the reliability of memory module 1 of a duplex pair, R_2 is the reliability of memory module 2 of the pair, A is ratio of failures detected by current sensing to all failures, (1-A) is ratio of failures not detected by current sensing to all failures, and N_d is the number of duplex pairs operating in series. Equation 33 infers that memory 1 is good or that memory 1 fails but 2 is good and that the failure is detected by the current sensing circuits or, if it is not detected, there is a 50/50 chance that it will be picked up with parity checking.

The reliability of a single memory module found from part count, generic failure rates, and Saturn V mission operating conditions is R = 0.998610; and from engineering design analysis the chances of a nondetectable failure (1-A) is 0.073. From equation 33, the unreliability of an eight memory module configuration with a storage capacity of 16,000 duplexed words is $U_r = 226$.

In summary, the unreliability of the LVDC for the Saturn V mission is the sum of the unreliabilities of the simplex oscillator, the TMR timing and logic, and the four duplexed memory modules, i.e., $U_r = 16 + 10 + 226 = 252$.

The reliability of the LVDA is not as straightforward as the LVDC because many varied functions entangled with the other systems, primarily the LVDC and platform, are performed in the LVDA. For example, the LVDA power supplies are required for operating the LVDC, processing vehicle attitude and velocity information, and issuing attitude correction commands. Parts of the LVDA TMR logic are time shared and are required with various critical vehicle functions. The LVDA utilizes various types of redundancy techniques: duplex, TMR, PRS, as well as system backup. However, only isolated types such as the LVDA power supplies and the digital-to-analog converter subsystem are discussed. All of these functions are flight critical. The reliability of the logic portion of the LVDA is found similarly to that for the LVDC. The TMR logic of the LVDA has an accessed unreliability of $U_r = 10$ for the Saturn V mission.

Six power supplies in the LVDA, which supply dc power to the LVDC as well as the LVDA, are all duplexed. Figure 11 shows a typical power supply. The dc to dc power converters are tied together through isolation diodes. Should a converter fail low, the other converter

picks up the load. It is imperative that a converter not fail high because the diodes isolation between the two units would be worthless. The feedback amplifiers used with each converter are duplexed to minimize the probability of this happening. One duplex system is functional provided the following condition is fulfilled.

$$P = \overline{P}_{h(low)} \cdot P_{h'} + P_h \cdot \overline{P}_{h'(low)} + P_h \cdot P_{h'} , \quad (34)$$

i.e., the output of converter h can be low and h' can be correct, or the output of converter h' can be low and h can be correct, or both outputs can be correct. Under the assumption that the chances of a feedback amplifier failing low are equal to those of it failing high (this is a valid and accurate assumption in this case), the expression for a simplex power supply (one converter and two feedback amplifiers) failing low is

$$\overline{P}_{h(low)} = \overline{P}_{h'(low)} = 1 - R_h R_f^2 - 2 R_h R_f (1-R_f) - R_h (1-R_f)^2 \quad (35)$$

where

$R_h R_f^2$ - probability that the converter and both amplifiers are good. (The output of the converter is correct.)

$2R_h R_f (1-R_f)$ - probability that the converter is good, one amplifier is good, and one has failed low. (The output of the converter is correct.)

$R_h (1-R_f)^2$ - probability that the converter is good and that both amplifiers have failed low. (The output of the converter is therefore high.)

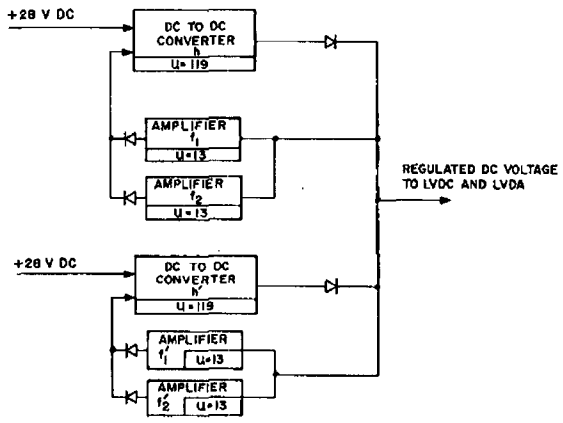


Figure 11. Typical LVDA Duplex Power Supply

Now, the probability that the output of a simplex power supply is correct is given by the first two terms and is

$$P_h = P_{h'} = R_h R_f^2 + 2R_h R_f (1-R_f) . \quad (36)$$

Substituting equations 35 and 36 into equation 34 and simplying yields

$$P = [R_h R_f (2-R_f)] [2(1-R_h) + R_h R_f (2-R_f)] . \quad (37)$$

From generic failure rates, it has been determined that $R_f = 0.999987$ and $R_h = 0.999881$ yielding $U_r \approx 0$ for a duplex supply. In comparison, the reliability of a completely simplex supply, i.e., one converter and one feedback amplifier, is $R = R_h R_f$ which has an unreliability of $U_s = 132$.

Six supplies are used in the LVDA system; four have an unreliability of $U_r \approx 0$, and two which do not have isolation diodes because of high current requirements have an unreliability of $U_r = 5$. The unreliability of the complete LVDA duplexed power supply system is $U_r \approx 4(0) + 2(5) \approx 10$.

A block diagram of the LVDA digital-to-analog attitude correction conversion system is shown in Figure 12. The system accepts the attitude correction commands from the LVDC and converts them to an analog form which is compatible with the control computer. It therefore plays a vital and critical function in the guidance and control of the vehicle. The reliability scheme employed is basically a PRS system with a reference channel being compared with that which is normally active. Two comparators are used in the system; one is an accurate fine comparator while the other is a coarse comparator and compares the outputs from the sample and hold devices and the output amplifiers. The block diagram of Figure 12 can be further simplified to the PRS redundancy system shown in Figure 13. If this is done, the prime, the reference, and the standby units consist essentially of the nine-bit register, the ladder network, sample and hold circuits, and two amplifiers. The voter then consists of the fine and coarse comparator. A single failure in the channel select switch results in a loss of redundancy. (Although in many cases, multiple failures can be tolerated, particularly in the various subsystems within the vehicle, the basic ground rule used for subsystem design was toleration of one failure.) The reliability of the system (for all three axes) may be approximated by the expression derived earlier for this type of redundancy (equation 18) but must be modified to take into account the single failure mode of the switch. The approximate reliability is given

$$P = [(R^3 - R^2)(1 - 2R_v) + R] R_s \quad (38)$$

where R is the reliability of a channel, R_v is the reliability of the voter or comparator, and R_s is the reliability of the switch. It has been estimated that for a Saturn V mission, $R = 0.999648$, $R_v = 0.999956$, and

$R_s = 0.999912$ resulting in an overall digital-to-analog converter unreliability of $U_r = 89$. In comparison, the unreliability of a simplex system is $U_s = 352$. The redundancy has consequently resulted in a decrease in unreliability by a factor of 3.94.

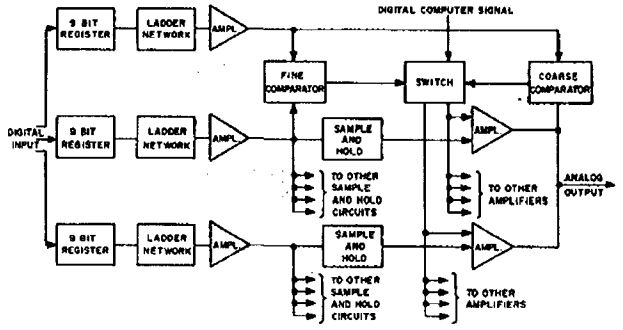


Figure 12. LVDA Digital-To-Analog Attitude Correction Conversion

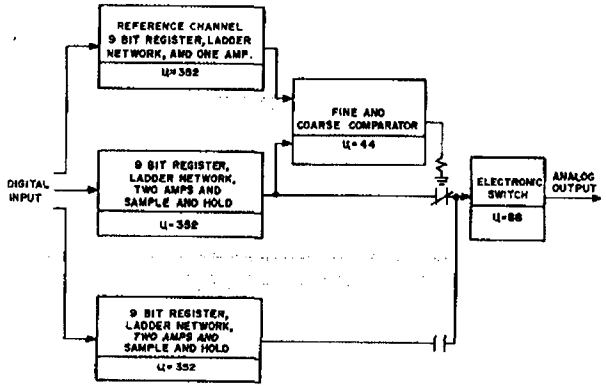


Figure 13. LVDA Digital-to-Analog Attitude Correction Conversion

Because of the nature of digital systems, intermittent failures are much more predominant than hard or solid failures. Therefore, the ability to switch from the standby unit back to the prime-reference system has been incorporated in the converter and the LVDC system. Since types of failures were not considered in the analysis, the reliability estimate is pessimistic from this standpoint.

In the LVDA, the reliability accessment has dealt with isolated examples, mainly the power supply and the digital-to-analog converter. Two other examples, that of processing attitude and acceleration inputs, are covered later. Table III summarizes the reliability of each major subsystem of the two units, both for the simplex and redundant case. Also shown is the ratio of the probability of failure of a simplex unit to that of a redundant unit. This factor indicates to some degree what has been gained through redundancy.

Table III. Summary of Unreliability of Simplex and Redundant LVDC and LVDA

Element	Simplex Unreliability U_s	Redundant Unreliability U_r	$\frac{U_s}{U_r}$
LVDC			
Logic	2,500	10	250
Memory (8mm duplex)	5,960	226	26.4
Oscillator	16		
Total LVDC	8,476	252	33.6
LVDA			
Power Supply	792	10	79.2
Input/Output	800	10	80.0
Logic	2,430	10	243
Total LVDA	4,022	30	134
Total Computer System	12,498	282	44.3

Stabilized Platform System

The stabilized platform is the basic reference for the Saturn navigation, guidance, and control systems. The system provides a space-direction-fixed coordinate reference frame which serves as a reference for the vehicle's attitude. The stabilized element serves as a base for three mutually-orthogonal accelerometers which provide the information from which translational velocity and position of the vehicle are derived. The stabilized platform system consists of an inertial platform, the associated electronics for internal stabilization and processing of output information, an electrical power supply, and a nitrogen gas supply.

The ST124-M platform used in the Saturn V system is a three-gimbal device which allows unlimited rotation of the vehicle about the pitch and roll axes. Rotation about the vehicle yaw axis (referenced to launch position) is limited to ±60 degrees, which is adequate to accomplish the Apollo mission. To accommodate missions requiring unlimited gimbal freedom about all three axes, the capability of incorporating a fourth gimbal has been designed into the system. On the three-gimbal platform, the order of the gimbals from the stabilized table outward is pitch, yaw, and roll, referenced to the vehicle position at liftoff. Dual-speed resolvers used as angular encoders on the gimbal pivots provide information from which the vehicle attitude is derived. Three single-degree-of-freedom gyroscopes provide the reference for the stable table on which the three pendulous integrating gyro accelerometers are mounted. Signal generators on the output axes of the reference gyroscopes derive electrical signals proportional to disturbance torques about the mutually perpendicular axes. These signals are amplified and shaped in the associated electronics and used to drive servotorque motors which maintain the inertial gimbal space-direction-fixed.

The inertial element of the reference gyroscope is a synchonous hysteresis gyro wheel having an angular momentum of 2.6×10^6 g cm^2/s. The wheel is driven at

24,000 rpm from a 400 Hz excitation source. The gyro wheel is mounted inside a cylinder which serves as the journal of a gas bearing. The cylinder is suspended on the side and ends by a film of gaseous nitrogen emanating from a series of holes in the supporting sleeve. The signal generator, which senses the angular displacement of the output axis, and a torque generator used in initial erection are coupled to the cylinder.

Each pendulous integrating gyro accelerometer (three of which are mounted on the stable table) contains a single-degree-of-freedom gyro. The gyro motor and flywheel are shifted along the spin reference axis to provide the desired pendulosity about the output axis. The gyro is a synchronous hysteresis type similar in construction to the reference gyro but smaller in size. It has an angular momentum of 94,000 g cm^2/s at a wheel speed of 12,000 rpm and is driven by the same 400 Hz source that drives the reference gyros. The accelerometer gyro is also mounted in a gas floated cylinder. The pendulous cylinder is free to rotate about the gyro input axis along which the acceleration is to be measured. The pendulosity causes a torque and therefore a precession proportional to acceleration along the input axis. The speed at which the gyro cylinder rotates is therefore proportional to acceleration and the position is proportional to velocity. An optical incremental encoder on the input axis is used to measure the velocity information.

A significant portion of the platform supporting electronics is required to close the platform gimbal servoloops and the accelerometer servoloops. The servoloops use a 4.8 kHz suppressed carrier modulation system with the signal generator outputs being amplified and demodulated on the gimbals of the platform. The resulting dc signal from the platform is routed to a separate electronics box where it is shaped by a lead-lag stabilization network, remodulated, amplified, and demodulated to drive a dc power bridge which supplies current to the appropriate torquer. Another major function of the supporting electronics is shaping the accelerometer optical encoder outputs. The encoder sine and cosine waves are amplified and converted to square waves for processing in the digital computer system. This system as well as the gimbal readout system, both of which interface very tightly with the digital computer system, is discussed in more detail later.

The supporting subsystems include separate power supplies which derive, from the vehicle 28 V dc buss, all ac and dc voltages necessary to operate the platform system. A three-phase 400 Hz sine wave and three single-phase square wave reference signals at 4.8 kHz, 1.92 kHz, 1.6 kHz, and 56 V dc are provided. Another supporting subsystem is the gaseous nitrogen supply utilized to float the gyro cylinders. Nitrogen is supplied from a 0.056 m^3 (2 ft^3) storage reservoir pressurized to 20.7×10^6 N/m^2 (3000 psi). The gas is regulated to 10.3×10^4 N/m^2 d (15 psid) for use in the platform.

Because of the problems involved in providing redundant stabilizing gyros and other platform elements, the platform does not utilize the extensive redundancy found in some of the other guidance and control subsystems. Instead of providing redundancy at the component or module level, it is more expedient in this case to provide a total system backup. The spacecraft is used to back up the Saturn launch vehicle guidance system during the orbital and translunar injection phases. It will also provide a backup for the Saturn platform as well as the guidance computations performed in the digital computer system. The backup is limited to the later phases since it is not feasible to implement the guidance equations used to inject the vehicle into earth orbit because of limitations of the spacecraft computer memory capacity. Some consideration is being given to a secondary simplified reference system within the launch vehicle (e.g., a strapped-down system) to provide a backup to the platform during all flight phases. Another approach being considered is the provision for manual booster control in the event of a platform system failure. In any case, the launch vehicle digital system must continue to function in all phases regardless of the guidance system backup employed since sequencing, telemetry calibration, and other functions are still performed by the launch vehicle digital computer.

In addition to the total system backup, redundancy is incorporated in certain critical portions of the platform where it can be readily applied. Primary examples of this are as follows:

1. The multispeed analog resolvers on the gimbal pivots, which are used to measure the vehicle angular orientation with respect to the platform.

2. Two channels of information are provided from each optical incremental encoder on the accelerometer. Both the optisyns and signal conditioning circuitry are duplexed. The two channels have equal resolution and provide a redundant channel of information into the data adapter.

3. Duplex redundancy is applied in portions of the circuitry of the power supply package used for excitation of the stabilizing and accelerometer gyros.

Since items 1 and 2 involve very close interfaces with the digital computer system, a detailed functional description of this portion of the guidance and control system, which includes some platform and some digital system elements, is covered here. The accompanying demonstration of reliability improvement through the use of redundancy is also covered on a functional basis rather than as individual elements in separate subsystems. In the overall subsystem reliability assessments, however, the reliability of the individual elements are included in their respective subsystems.

A block diagram of the multispeed resolver channels, including those portions of the digital computer system data adapter used to process the information and provide vehicle attitude correction commands, is shown in Figure 14.

The three resolvers, one for each coordinate axis, have both a 32:1 and a 1:1 winding on the same magnetic structure. For the 32:1 winding, 32 electrical degrees correspond to one mechanical degree. The outputs of the

resolvers are fed through successive platform gimbals by means of sliprings. The resolver excitation frequency (1016 Hz) is derived from the digital computer clock and fed to the platform. Two power supplies are used, and the system is organized such that no 32:1 and 1:1 system in the same channel receives power from the same supply. Therefore, the system is arranged such that a failure in one resolver system or power supply is backed up by the other system.

The outputs of the resolvers are fed to RC phase shift networks in the data adapter and then to crossover detectors (COD) which detect when each signal crosses zero going positive. This signal is then gated to an 11-bit counter in the data adapter. Crossover of one of the sinusoidal signals is used as a start pulse and gates the 2.048 MHz computer clock to the counter. The other sinusoidal crossover is used to stop or turn off the 2.048 MHz counter. Therefore, the value obtained by the counter is directly proportional to the phase shift between the two signals and is representative of resolver shaft position and vehicle attitude. Either a single or a double RC network is employed on the single speed resolver. The 32:1 system employs a double RC network resulting in an equivalent resolution of 64:1. The selection of a single or double RC network for the single speed system is under program control. The single network provides a whole value; however, in case of failure of the 32:1 system, the resolution of the 1:1 system may be doubled (2:1) by employing the additional RC network. (For the 2:1 system to back up the 64:1 system, a decrease in resolution by a factor of 32 must be tolerated.)

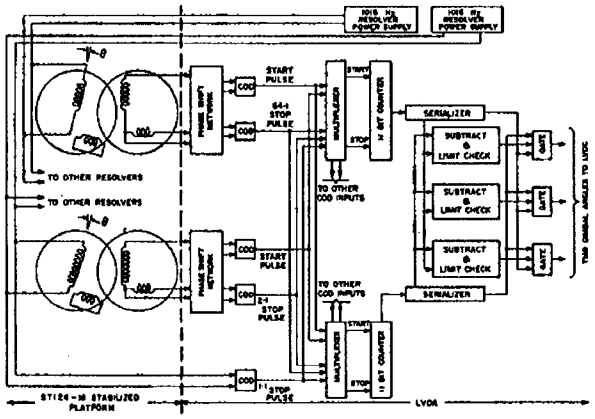


Figure 14. LVDA Gimbal Angle Processing System

The multiplexers in the data adapter are duplexed and all resolver inputs are gated through each multiplexer. The resolver to be read into the duplexed counters is selected by computer program. The output of each counter is routed to three (TMR) subtract and limit check circuits, which compare the counter readings within a predetermined range. The computer is alerted if the subtract and limit test has failed. A counter disagreement indicates either a power supply, COD, resolver, or counter failure. A power supply failure results in multiresolver error readings which may be logically assessed by the computer program. When the subtract and limit test fails to determine if the failure is due to a counter, a pseudo-resolver signal, which is dependent on the computer program, is used to turn on the start and stop signal thereby setting a predetermined value in the counter. If a failure does not occur in this test, it may be assumed that the counters are good and that either a code or resolver error caused the disagreement between the two values. If the error is not corrected within a prescribed period of time or within a given number of iterations, the backup system is employed. If a failure occurs in the counter test, the proper counter and serializer channel may be selected for further use.

For a reliability analysis, this system may be further simplified as shown in Figure 15. Indicated in each block are the functions or hardware grouped together for this analysis. The reliability analysis of the system may be considered in three parts (Fig. 15). The first part uses nonconventional duplexing and consists of the resolver excitation sources, resolvers, platform sliprings, and COD's. The second portion is made up of conventionaly duplexed input multiplexers, counters, and serializers. The third part is the TMR subtract and limit check circuits. The reliability of each part may be considered independently of the others, and the reliability of the system is the product of the reliability of each part.

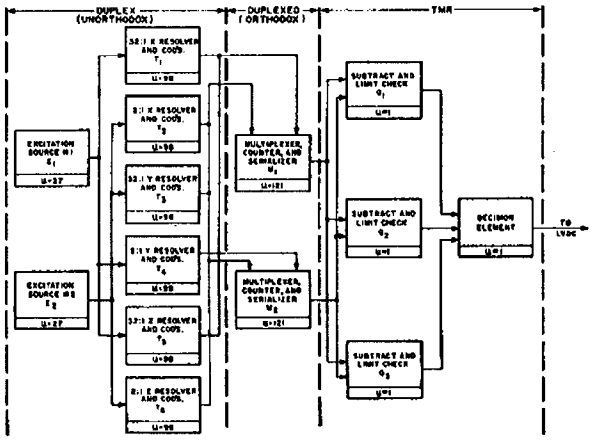


Figure 15. Block Diagram of Gimbal Angle Processing System

For the unorthodox duplex portion to function properly, the following conditions must be met:

$E_1 \cdot \overline{E}_2 \, (T_1 \cdot T_4 \cdot T_5)$ - one excitation source and three resolvers must be good, or

$\overline{E}_1 \cdot E_2 \, (T_2 \cdot T_3 \cdot T_6)$ - same as above except the other set of components are considered, or

$E_1 \cdot E_2 \left[(T_1 + T_2) \, (T_3 + T_4) \, (T_5 + T_6)\right]$ - both frequency sources and at least one resolver in each axis must be functional.

67-553

When these conditions are treated in detail, the reliability of the unorthodox duplex part is

$$P = R_e^2 \left[-R_t^6 + 6R_t^5 - 12R_t^4 + 6R_t^3\right] + 2R_e R_t^3 \quad (39)$$

where R_e is the reliability of one excitation source, and R_t is the reliability of platform sliprings, the gimbal angle resolver, and the two COD's required for each resolver output.

The reliability of the second and third parts, found by applying equations 10 and 17, is

$$P = 2R_m - R_m^2 \quad (40)$$

$$P = 3/2\,R_q - R_q^3/2 \quad (41)$$

where R_m is the combined reliability of one multiplexer, counter, and serializer and R_q is the reliability of the subtract and limit check circuitry. Combining these expressions yields the attitude input system reliability given by

$$P = \left[R_e^2 \left(-R_t^6 + 6R_t^5 - 12R_t^4 + 6R_t^3\right) + 2R_c - R_t^3\right]$$

$$\left[2R_m - R_m^2\right]\left[\frac{3}{2}R_q - \frac{R_q^3}{2}\right] \quad (42)$$

Generic failure rates for the various components have led to the following subsystem reliabilities for one flight.

$$R_e = 0.999973$$

$$R_t = (R_{resolver})\,(R_{COD})^2 = (0.999914)\,(0.999994)^2$$

$$= (0.999902)$$

$$R_m = 0.999879$$

$$R_q \approx 1.$$

The unreliability of the system can then be calculated to be $U_r = 1$. In comparison, the reliability of a simplex system is given by

$$P = (R_e)\,(R_t)^3\,(R_m)$$

and is found to yield an unreliability of $U_s = 442$. Utilizing redundancy in the system has therefore decreased the unreliability of the system by $U_s/U_r = 442/1 = 442$.

Note that in the system just described an additional decision technique has been used, i.e., the computer logical capability. Previous discussion has been confined to hardware redundancy; however, with this scheme, the computer program and logical capabilities ascertain the system or redundant path to be used for further operation. This type of decision element provides the greatest capability and flexibility; however, complicated programs become even more complex and the normal computational processes are interrupted while this task is performed.

The second portion of the platform employing redundancy, the accelerometer readout channels, also interfaces very closely with the digital subsystem. As was the case with the gimbal resolver channel, these elements are also functionally described and the benefits of redundancy are demonstrated as a single system. A block diagram of the system used in measuring and processing the acceleration information is shown in Figure 16. The figure shows a single measuring channel. Three identical channels are employed to measure the vehicle acceleration along three mutually perpendicular axes.

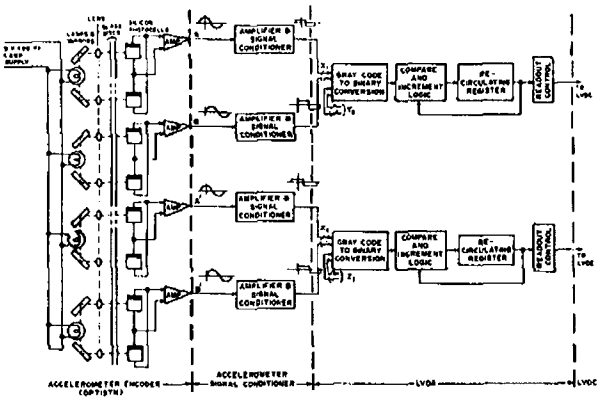


Figure 16. Accelerometer Processing System

The acceleration sensing device is a single-degree-of-freedom gyro unbalanced about its output axis. A torque is produced by the unbalance or pendulosity which is proportional to the acceleration to which the pendulous mass is subjected. The precession angle of the gyro is proportional to the integral of the acceleration. An optical incremental encoder provides a measure of inertial velocity with a resolution of 0.05 m/s^2.

The encoder, which is mounted directly to the gyro head on the platform, contains lamps, mirrors, lens, photocells, and amplifiers. The lamps are excited by a 5 V Hz supply from the platform system. Light from the lamps, which are equally spaced around the periphery of the encoder, is reflected from the mirrors through lenses and passes through two glass discs. Each disc has deposited on it equally spaced opaque lines. Mirrors are used to reduce the number of light bulbs required. One disc is fixed while the others rotate. The light input to each pair of photocells or the input signal to the amplifiers approximates sinusoidal functions as one of the discs rotates relative to the other. The photocells are connected such that maximum signal pickup occurs on one photocell while the other photocell pickup is minimum and vice versa. Effectively, one pair of the photocells

generates the positive portion of the sine wave while the other pair produces the negative portion of the wave. From the amplifier in the encoder on the stable element, the signal is fed through the three platform gimbals by means of sliprings to the accelerometer signal conditioner unit where the signal is further amplified and clipped to obtain square waves.

Two signals (one sine and one cosine) for each channel are fed to the data adapter. These signals represent, in gray code, incremental velocity inputs. One sine wave and one cosine wave are processed in the data adapter logic to give four velocity increments, each increment representing a change in velocity of 0.05 m/s. Before this is used by the computer system, it is converted to a binary number. After the gray code to binary conversion, the 0.05 m/s incremental inputs are summed in a recirculating register in the data adapter. The register is 12 bits plus sign; therefore, a velocity of 204.8 m/s can be accumulated before it overflows. This value is read into the computer approximately once per second, and the entire value velocity of 26 bits stored in computer memory is updated.

Figure 17 indicates the accelerometer readout system organization from a reliability standpoint. The +20 V dc and 5 V 400 Hz power required in the encoder amplifiers and for light bulb excitation is simplex. The voltages to the accelerometer encoders and signals from the platform to the LVDA are fed through platform sliprings. Each block to the immediate right of the power supply consists of the accelerometer encoder (made up of lamps, photocells, an amplifier, and platform sliprings), amplifiers, and signal conditioners located in the platform electronics. The output of each block consists of two signals, a sine and cosine wave, which are necessary to obtain the velocity increments in one axis. (Although magnitude can obviously be obtained from one signal, two signals are necessary to determine direction.) Each part of the gray code to binary conversion is unique to each of these signals and will be lumped with the block on its left for reliability analysis. After conversion to gray code, two accelerations in a different axis are stored together in a register in a glass delay line as indicated in the figure. One of three delay lines can fail without resulting in a system failure; however, other combinations of accelerometer or signal condition failures can result in a system failure. The system is rather complicated to analyze; however, the following general conditions apply:

1. With a failure in either the compare and increment logic, and/or one delay line, one of the other accelerometer signals not associated with the failed logic or delay line can be lost without a system failure; i.e., if in Figure 17 the top channel delay line is lost, X_1 and Y_2 are lost. A failure in either of the Z accelerometer inputs can be tolerated, but a failure in either X_2 or Y_1 results in a system failure. Similar reasoning is appropriate for each of the other channels.

2. With all increment logic and the three delay lines functional, only one accelerometer signal in each of the three axis is required.

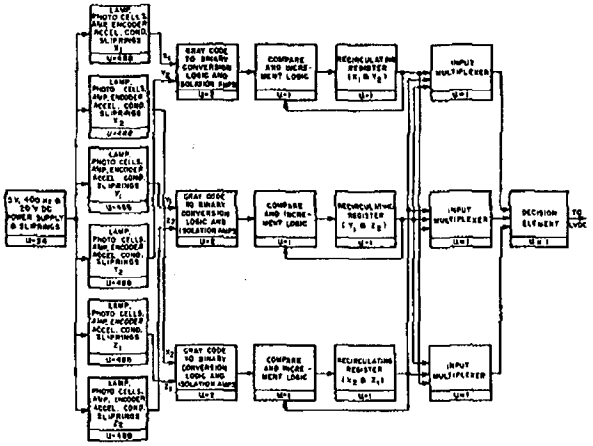


Figure 17. Accelerometer Processing System

The reliability of that part of the system between the power supplies and the input multiplexer is given by

$$P = 3R_i^2 (1-R_i) R_k^2 (2R_k - R_k^2) + R_i^3 (-R_k^6 + 6R_k^5 - 12R_k^4 + 8R_k^3) \quad (43)$$

where R_i is the reliability of one channel of logic including increment logic and the delay line, and R_k is the reliability primarily of the accelerometer encoder and signal conditioning circuitry although it also includes platform sliprings, isolation amplifiers, and gray code to binary conversion logic.

The input multiplexers are conventional TMR and from equation 17 have a reliability given by

$$P = \frac{3R_m}{2} - \frac{R_m^3}{2} \quad (44)$$

where advantage has been taken of failures in opposite directions. R_m is the reliability of a simplex multiplexer.

The reliability of the complete redundant system then is given by

$$P = [R_e] [3R_i^2 (1-R_i) R_k^2 (2R_k - R_k^2) + R_i^3 (-R_k^6 + 6R_k^5 - 12R_k^4 + 8R_k^3)] \left[\frac{3R_m}{2} - \frac{R_m^3}{2}\right] \quad (45)$$

where R_e is the reliability of the 20 V and 5 V excitation sources and includes those sliprings necessary to get power to the encoders, and all other quantities are as previously defined. Generic failure rates and subsystem analysis yield the following reliabilities for those terms in equation 45.

$R_e = 0.999966$, $R_l = 0.999998$, $R_k = 0.999510$, and $R_m = 0.999999$. Evaluation of equation 45 using these values yields a total system unreliability of $U_r = 35$.

A simplex system would have a reliability given by

$$P = (R_e) R_k^3 R_l^3 R_m. \quad (46)$$

Using these subsystem reliabilities results in a simplex unreliability of $U_s = 1511$.

Comparing the unreliabilities of the redundant and simplex systems indicates a gain factor of 43.2 over the simplex system.

Note that the reliability of the stable elements and the accelerometers was not included in this analysis. Only that part of the system used in processing accelerometer information was included. Since the accelerometers are simplex, an accelerometer failure could result in a system failure.

The value of the computer in recognizing failures is further illustrated in this system. The computer system reads both the prime acceleration and its backup, i.e., X_1 and X_2, etc., and performs a reasonableness test before either is used in the solution of the guidance equation. The computer subtracts the two values stored in the delay lines to determine if the values are consistent or in agreement. If they compare within reasonable limits, either value may be used. If a difference exists, the computer then compares each value with previous values to determine which delta value is more reasonable. The velocity profile of the vehicle can be approximated with a fair degree of accuracy through simulations before flight, and maximum delta velocities expected between successive readings can be determined within reasonable limits.

The third example of redundancy within the platform system is the ac power supply. Although a portion of the circuitry is simplex, duplex redundancy is employed in the oscillator and frequency divider circuitry.

From the primary 28 V dc vehicle power source, the power supply derives the ac power to drive the gyro wheels and provides the excitation voltage for the gimbal synchros and resolvers. A simplified block diagram of the power supply is shown in Figure 18.

The power supply uses a quartz crystal oscillator as a reference. By frequency division, temperature-stable square waves of 19.2 kHz, 4.8 kHz, 1.92 kHz, and 1.6 kHz are derived. The buffered 1.6 kHz and 1.92 kHz square waves are used as reference signals for the platform resolvers. The 4.8 kHz output is routed to the platform electronics assembly where it is utilized in the platform and accelerometer stabilizing circuits. The 4.8 kHz square wave is also used as the reference for a cyclic register, which produces six push-pull 400-Hz square wave outputs in 30-degree increments. The output of this circuitry is transformed and filtered to provide the 3-phase 400 Hz sine wave power which drives the platform gyros.

As indicated in Figure 18, the oscillator, frequency divider, and cyclic register circuits are duplicated. The signal from each channel is fed to the failure detection and switchover circuitry. Both of the duplicated channels are energized, with only one actively controlling the power supply. Any failure in the active oscillator circuitry causing a detectable loss of output voltage will result in an automatic switchover to the standby section.

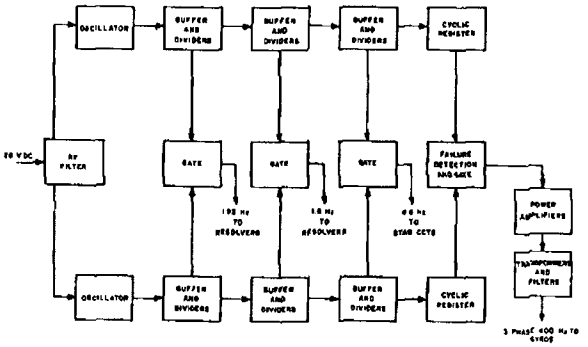


Figure 18. Platform AC Power Supply

To portray the benefits of the redundant circuitry on the overall power supply reliability, a simplified reliability model is shown in Figure 19. The reliability of a single channel of the redundant portion of the system is $R = 0.999845$. Applying equation 9 to the duplex redundant oscillator section yields $P \geq 0.999999$ and $U_{rp} \leq 1$. The equivalent unreliability of the various segments of the power supply is indicated in Figure 19. Considering the duplex oscillator and adding the unreliability of the simplex elements results in $U_r = U_{sp} + U_{rp} = 2 + 356 + 11 + 1 = 370$.

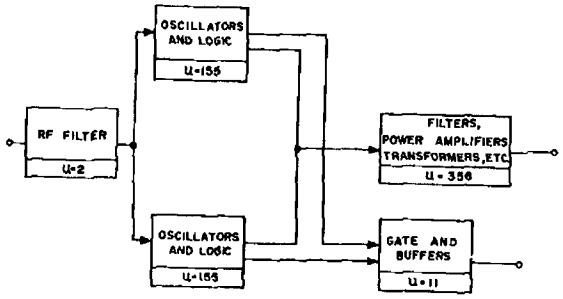


Figure 19. Platform AC Supply (Simplified Model)

If the total power supply including the oscillator was simplex, the unreliability would be

$$U_s = 2 + 155 + 356 + 11 = 524.$$

The overall benefit of redundancy in this case is the reduction of the unreliability by the following ratio:

$$\frac{U_s}{U_r} = \frac{524}{370} = 1.42.$$

The relative improvement is considerably below that obtained in some of the other subsystems because a significant portion of the power supply circuitry could not readily be made redundant.

To demonstrate the overall platform system reliability, the system is assessed by individual elements. The total system consists of six major elements: an inertial platform, a platform electronics assembly, an accclerometer signal conditioner, an ac power supply, a 56 V dc power supply, and a nitrogen gas supply. A block diagram indicating the interconnection of these various elements is shown in Figure 20; the unreliability of these elements for the 6.8 hour mission is indicated. The numbers shown include the reliability improvements in those various elements where redundancy is applied. As shown, the total unreliability of the system including the redundant elements is $U_r = 13,531$. If the system was totally simplex, the following increase in unreliability in the three segments previously discussed would result.

Resolver channels:	$U_s = (3 \times 86) = 258$
Accelerometer readout channels:	$U_s \quad (3 \times 488) = 1464$
Ac power supply:	$U_s = 155$
	Total increase = 1877

Therefore, the unreliability of a totally simplex platform system would be $U_s = 13,531 + 1877 = 15,408$. The overall system improvement ratio resulting from redundancy is therefore

$$\frac{U_s}{U_r} = \frac{15,408}{13,531} = 1.14.$$

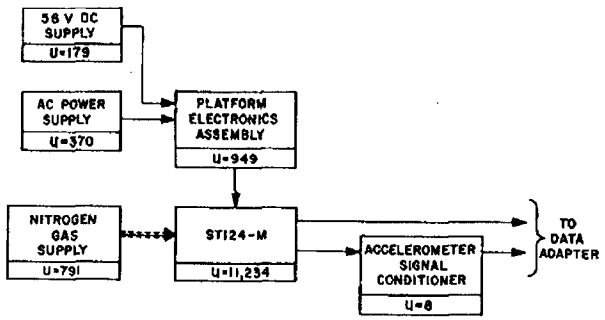


Figure 20. ST124-M Platform System

Figure 21 is a schematic of the guidance system indicating that the launch vehicle platform system is backed up by the spacecraft system. A failure of the Saturn launch vehicle platform is sensed by the digital system by comparing the measured gimbal angle rates with nominally expected values. When an unreasonable signal is read, the digital system operates a light on the astronaut's control panel. In addition, the astronaut has displayed information derived from various spacecraft sensors, as well as communications with ground, from which indication of the system performance can be derived. If a failure or degraded performance of the launch vehicle system is indicated, the astronaut can switch the spacecraft guidance signals directly into the launch vehicle control computer. This implementation does not provide a total backup for the digital system as well as the platform; the digital system must continue to perform many other vehicle functions.

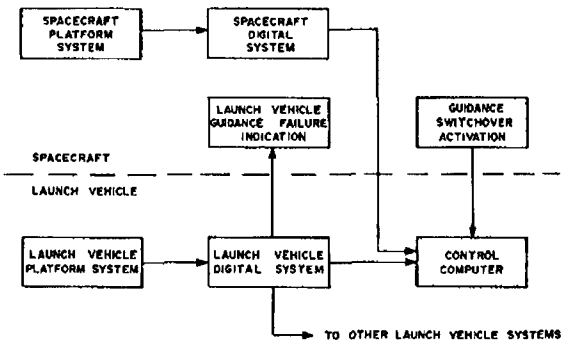


Figure 21. Platform Backup System

To obtain an approximation of the benefit derived from this backup arrangement, it is assumed that the two guidance systems are equally reliable and that the sensing and switching mechanisms are simple and reliable as compared to the overall systems. The unreliability of the launch vehicle platform system can be broken down as (1) through earth orbit injection, $U_{ra} = 8645$, and (2) balance of launch vehicle mission, $U_{rb} = 4886$.

Applying equation 9 to U_{rb} yields

$$(U_{rb})^2 = (4886 \times 10^{-6})^2 \times 10^6 = 24$$

where $(U_{rb})^2$ is the unreliability of the platform systems during the period when the launch vehicle platform is backed up by the spacecraft platform, i.e., from orbital injection to completion of the mission. With guidance backup applied only during the orbital and lunar injection phases, the platform system unreliability consequently is

$$U_r = U_{ra} + (U_{rb})^2 = 8645 + 24 = 8669$$

where U_{ra} is the unreliability of the launch vehicle platform through orbital injection.

Other backup approaches that would further reduce the unreliability have also been mentioned previously. The possibility exists that platform system backup could be provided throughout the launch vehicle flight by a

simplified strapped-down guidance system, or by relying on the astronaut to manually control the system in the event of failure. In the latter case, the astronaut would monitor vehicle angular and translational indications provided in the spacecraft to steer the vehicle into orbit with a degraded accuracy as compared to the primary guidance.

If the same simplifying assumptions as with the spacecraft guidance backup system are made (i.e., $\bar{P}$(backup) = $\bar{P}$(primary), and $\bar{P}$(sensing and switching) = 0), the following unreliability results from equation 9.

$$U_r = (U_{rab})^2 = (13,531 \times 10^{-6})^2 \times 10^6 = 183$$

where $(U_{rab})^2$ is the unreliability of the system when the launch vehicle platform is totally backed by another system during all phases of launch vehicle operation.

A resume of the platform system unreliability and the benefits of the backup schemes are shown in Table IV,

Table IV. Platform System

	U_r	U_s	U_s/U_r
Launch vehicle system	13,531	15,408	1.14
With backup out of orbit	8,669	15,408	1.77
With proposed total flight backup	183	15,408	84.30

which indicates that a very significant reduction in unreliability in the platform system can be obtained only by providing a backup throughout the total flight. Therefore, several total backup approaches are being pursued.

Control System

For a logical functional description and practical redundancy application, the control system is broken down as attitude rate sensing, multiengine (S-IC and S-II) stage propelled phase control, single-engine (S-IVB) propelled phase control, and S-IVB coast phase control.

The rate sensing system is composed of two boxes containing the rate sensors (the rate gyro package) and the associated electronics (the control signal processor package). The rate gyro package contains nine rate gyros so arranged that angular rate about each of the vehicle axes (pitch, yaw, and roll) is sensed by three separate instruments; thus three separate signals, independently derived, are available for each axis. The individual rate gyros are single-degree-of-freedom instruments containing a spin motor which operates at a synchronous speed of 24,000 rpm and has an angular momentum of 30,000 g cm^2/s. Angular rates about the input axis, which is aligned with the vehicle pitch, yaw, or roll axis depending on the case mounting direction, are sensed by a 400 Hz microsyn pickoff that is electromagnetically coupled to the gyro gimbal. The output of the microsyn is proportional to the vehicle angular rate about the input axis. The microsyn outputs, one from each of the three instruments in each axis, are fed in parallel into the control signal processor. Nine demodulator modules, three for each axis, receive the rate gyro error signals. Each demodulator module amplifies the input signal and provides a plus or minus dc voltage proportional to the ac input amplitude.

The power for the rate sensing system is obtained from three separate 28 V battery supplies over three busses. Three static inverters in the control signal processor supply the 26 Vrms 400 Hz power to the rate gyros and demodulators; likewise, three dc power circuits supply the necessary 60 volts to the demodulators. Each primary power buss with its associated inverter and dc power circuit supplies three gyros and associated electronics; one in each of the pitch, yaw, and roll groups.

The rate sensing utilizes the PRS form of redundancy. A simplified diagram of one channel neglecting power supplies is shown in Figure 22. The rate signal outputs from the primary command demodulator and the reference demodulator are sent to a comparator, which consists of two differential amplifiers, an amplitude sensor, and a relay driver. If the difference between the primary and reference channels exceeds a preset level, the comparator circuit operates relays which switch the primary channel out of operation and substitute the standby channel into the primary command position. Thus, if a malfunction occurs in either the primary or reference channels, the standby channel will be substituted. If a malfunction occurs in the standby channel with the other channels performing properly, no switching occurs. The difference level, at which the circuit switches (1.65 deg/s), is determined from compromise considerations of hardware tolerance characteristics and expected vehicle motions. The reference channel serves solely as a reference and is never used to provide the rate command to the remainder of the system. The PRS redundancy as implemented in this subsystem does not provide the capability of switching back during flight to the primary channel after the standby channel has been substituted. Such an arrangement causes the subsystem to revert to an equivalent simplex system after a single discrepancy, even if it is transient in nature. A multiple switching capability such as that utilized in the digital system would be more reliable, but would also be more difficult to implement in an analog system.

The reliability assessment of the individual blocks shown in Figure 22 is

$$R = (R_{demod})\ (R_{rate\ gyro}) = (0.999919)\ (0.998453)$$

$$= 0.998372$$

$$R_v = 0.999931.$$

These numbers are applicable to the total flight time, since the rate system must function throughout flight. Applying these numbers in equation 18 for the PRS system yields P = 0.999994; or, expressed in terms of malfunctions per million flights, U_r = 6. The numbers shown in

Figure 22 express the unreliability of the individual channels of the PRS system. For the equivalent simplex system, $U_s = 1628$.

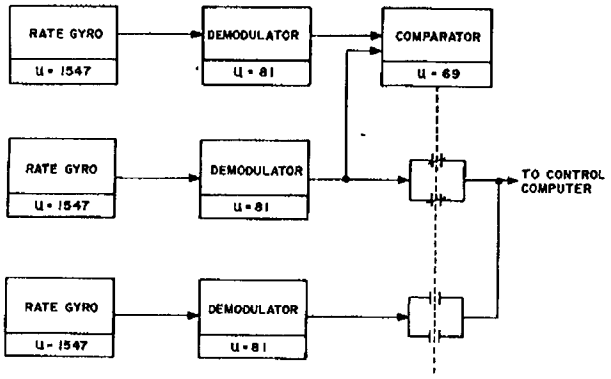


Figure 22. Attitude Rate System (Single Channel)

If the rate control system was composed of three uncoupled control axes, the unreliability of the total system could obviously be obtained by multiplying the above redundant unreliability (U_{PRS}) by three. The three axes are independent except for the internal power supplies. If the internal power supplies are considered, however, the treatment is not quite so straightforward since each of the three power supplies drives one channel in each of the pitch, yaw, and roll axes. A simplified block diagram of the complete three-axis system with the power supply interconnection arrangement is shown in Figure 23. The expression applicable to the total three-axis system shown is

$$R = R_e^3 [(R^3 - R^2)(1 - 2R_v) + R] + 3(1-R_e) R_e^2 R R_v [(1-R_v) - R(1-2R_v)] \quad (47)$$

where R_e = reliability of one of the three power supplies (inverter and 60 V dc supply, combined) and the other terms are as previously defined. The first term in the expression represents the probability of all outputs being good when all three power supplies are assumed to be good. The second term represents the combination of properly functioning situations which result when the power supplies are assumed to fail singly. When two or more power supplies are lost simultaneously, a failure results in either pitch, yaw, or roll. In equation 47,

$$R_e = (R_{\text{inverter}})(R_{\text{dc supply}}) = (0.999897)(0.999915)$$

$$= 0.999812$$

and R and R_v are as previously indicated.

For the total subsystem, P = 0.999980 and $U_r = 20$. If the system was simplex, $U_s = 4972$ would apply. Therefore, the improvement through redundancy is $U_s/U_r = 248$.

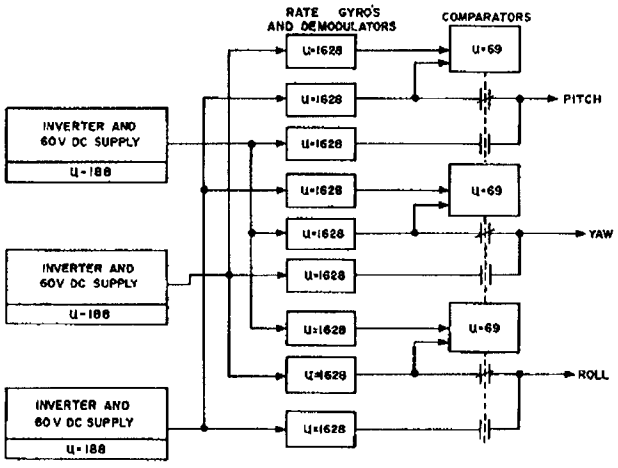


Figure 23. Attitude Rate System (All Channels)

The vehicle attitude rate signals derived in the subsystem, as well as the desired vehicle attitude derived from the stabilized platform and digital computer, are utilized to direct and stabilize the vehicle. The flight control computer processes these input signals and derives in an analog manner the appropriate command signals for the gimbaled engine actuators and auxiliary thruster valves to torque the vehicle as required. Control torques on the first two stages (S-IC and S-II) are derived by positioning the four gimbaled engines on each stage. The control torques for the upper stage (S-IVB) are obtained by gimbaling the single main engine and activating the six fixed-direction auxiliary engines. The two techniques are different in basic layout and are discussed separately.

A layout of the control system of the multiengine stages is shown in Figure 24. There are six inputs to the control computer, an attitude and attitude rate for each of the three axes. These signals are individually scaled, filtered, and then routed to the appropriate servoamplifiers which drive the engine actuators. The elements of particular interest in this chain are the filters, or shaping networks, the servoamplifiers, and the servoactuators. The characteristics of each shaping network are those required to satisfactorily provide the required stability margins, taking into account the vehicle structural bending, propellant sloshing, and transfer functions of the remainder of the guidance and control system. In this module, compensation is made for variation between individual vehicles and individual missions. Extensive analysis is required to derive the shaping networks for each particular mission. This particular module, along with its associated isolation amplifiers, is simplex in each of the two multiengine stages. The simplex approach was chosen in this case for two reasons. First, since the mission time of each

multiengine stage is relatively short in duration and the shaping networks are composed of only a few components, the predicted reliability is high even for the simplex version. The second reason is one of engineering compromise to conserve weight and space. Although simple in configuration, the networks are bulky compared to other modules of the control electronics because of the large size of some of the electronic components (capacitors and inductors) required to accomplish the necessary shaping at the low control bending mode frequencies in the range of 0.5 to 5 Hz.

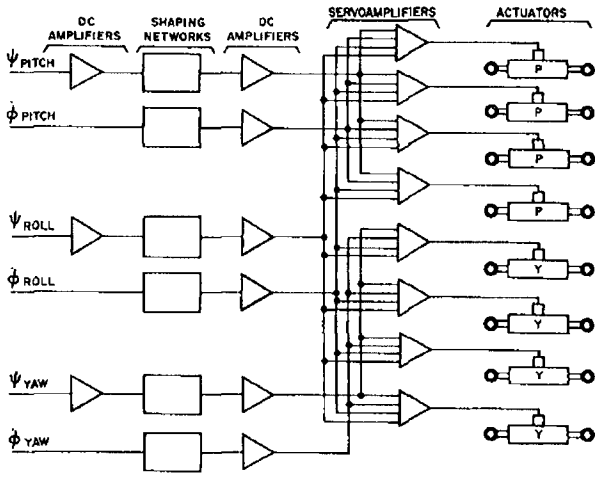


Figure 24. S-IC or S-II Stage Control System

Each servoamplifier is composed of a magnetic mixing amplifier, followed by transistor stages which provide the necessary power gain. A number of inputs are in each magnetic amplifier which is the point in the system where the attitude and rate signals from the appropriate axes are combined. The various input signals into the magnetic amplifier are galvanically isolated from each other since each is applied to a separate winding. The excitation signal for the magnetic amplifier is derived from a chopper-stabilized inverter which converts the dc source to a one kHz signal. The outputs of the eight servoamplifiers drive eight corresponding servoactuators which position the four gimbaled engines as required. These hydraulic servoactuators and the associated fluid supplies make up the other major elements in the multiengine control system. The hydraulic systems of the S-IC and S-II are designed differently to satisfy the individual stage requirements.

A simplified schematic of the S-IC hydraulic servoactuator is shown in Figure 25. The servoactuator receives from the servoamplifier an electrical signal which represents the desired engine position. The electrical signal is applied to the servovalve torque motor, causing a pressure differential to exist between two orifices. This pressure differential positions a spool which in turn regulates the flow in a manner to control the position of a second spool. The flow regulated by this second spool determines the actuator piston location and, therefore, the gimbal angle of the attached engine. The entire system is essentially a three-stage hydraulic power amplifier. In addition to providing the necessary power amplifications and conversion, the servoactuator must also meet certain dynamic response, load damping, and stiffness requirements. These features are provided by hydraulic pressure feedback and shaping within the actuator. The servoactuator also employs the principle of mechanical feedback, which improves reliability by eliminating the need for actuator position information to be electrically sensed and fed to the control computer over long lines through multiple interfaces. The feedback mechanism converts the rectilinear motion of the actuator to a force which counteracts the electromotive force of the input signal on the first stage of the servovalve.

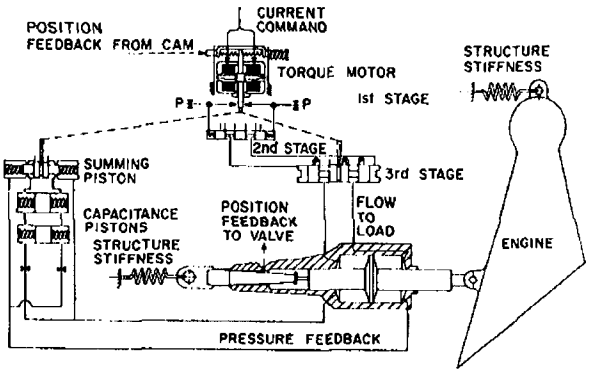


Figure 25. Schematic of S-IC Servoactuator

The actuator has a stall load of 507,000 N (114,000 lb) which is equivalent to a torque of 810,000 Nm (600,000 ft lb) as applied to the gimbaled engine. The expected operating torque range is 540,000 Nm and below; the major torques to be overcome are contributed by propellant duct loads and a thrust vector which does not pass through the center of the engine gimbal bearing. In the presence of these and other loads, the actuator can position the engine through an angle of ±5.2 degrees at a rate of 5 deg/s.

The fluid supply for the S-IC servoactuator is RP-1 fuel taken directly from the turbopump which also supplies the main engine. This makes an extremely simple and reliable onboard hydraulic supply since only filters and interconnecting ducting must be added to the propulsion distribution system. The individual gimbal systems are independent because the turbopump on each engine furnishes the supply for the actuators on that engine.

The S-II servoactuator is functionally similar to the S-IC servoactuator although physically much smaller. The hydraulic flow rates required to position the engine are much lower, so only two stages of hydraulic amplification are required. Mechanical feedback, pressure feedback, and hydraulic shaping are also employed in this actuator. The S-II actuator has a stall load of 202,000 N (45,500 lb). The maximum load expected

to occur during flight is 133,000 N (30,000 lb). The S-II (J-2) engine is gimbaled through an angle of ±7.3 degrees at a rate of 10 deg/s.

The S-II fluid supply is different from the S-IC in that a closed high-pressure system is utilized. The hydraulic power source is a pump driven by the turbopump shaft on each gimbaled engine. The other major components in the fluid supply are an accumulator, which supplies flow to supplement the main pump during periods of peak demands, and a low flow auxiliary pump.

To illustrate the reliability improvement afforded by the multielement control on the first two stages, a block diagram of one-axis control neglecting the hydraulic supply is shown in Figure 26. The case illustrated is S-IC or S-II pitch control; the shaping networks and associated amplifiers are simplex. The servoamplifiers and actuators are representative of the inherent MPE redundancy.

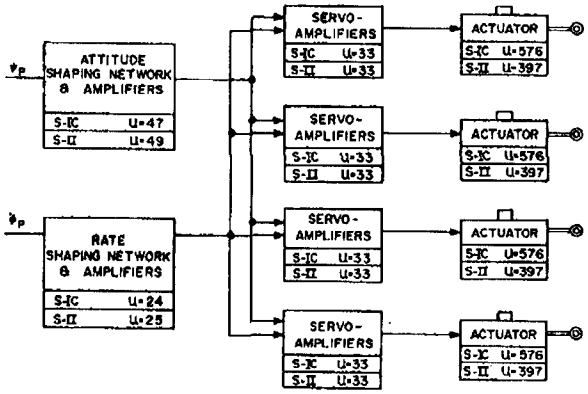


Figure 26. S-IC or S-II Stage Pitch Control System

If one element of the MPE configuration can fail without a loss of the mission, the unreliability is dramatically reduced compared to a system requiring all elements to function. This capability can be designed into a system by a certain overdesign as compared to a nominal failure-free situation. For instance in the gimbal system under discussion, an additional gimbal angle and gimbal rate capability must be provided. Structural and aerodynamic aspects must also be considered. During certain times of flight and under certain combinations of adverse conditions, the S-IC and S-II stages cannot be controlled with a failure in one element of the MPE configuration. In a precise analysis, the probability of loss of mission in the event of a failed channel during the various flight phases would have to be considered. The capability of maintaining control when a channel is lost exists during an appreciable portion of the flight; however, the simplifying assumption is made here that MPE redundancy exists throughout. With this assumption, the reliability of the MPE portion of the subsystem for the S-IC stage can be found from equation 21, where

$$R = (R_{electronics})\,(R_{actuator}) = (0.999967)\,(0.999424)$$

$$= 0.999391$$

resulting in $P = 0.999997$ and $U_{rp} = 3$. For the simplex portion of the electronics,

$$R = (R_{\Psi})\,(R_{\dot{\varphi}}) = (0.999953)\,(0.999976)$$

$$= 0.999929$$

and $U_{sp} = 71$. Adding the simplex and redundant portions yields $U_r = U_{sp} + U_{rp} = 71 + 3 = 74$.

The probability of failure for the simplex elements and individual parallel elements is shown in Figure 26. If all elements must function properly (i.e., if no inherent redundancy exists), the unreliability is found by adding the unreliability of all elements; thus $U_s = 47 + 24 + 4(33 + 576) = 2507$.

The layout for the yaw channel control is similar to that for pitch. Except for a slight difference in the shaping networks, the circuits for the two channels are identical. As shown in Figure 27, the roll signal is mixed with the pitch and yaw signals in all eight channels. The applicable unreliability numbers are also shown. In addition to the numbers developed, Table V shows the unreliability of the complete S-IC pitch, yaw, and roll control system (electronics plus actuators) for the implemented redundant system as well as a corresponding simplex system.

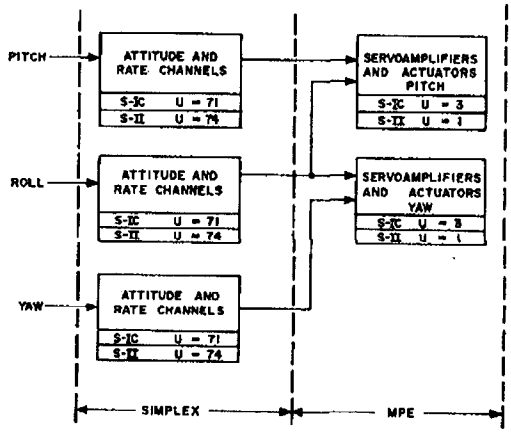


Figure 27. S-IC or S-II Stage Control System (Simplified Model)

The hydraulic fluid supply systems have not been included in this assessment. The layout of the S-IC and S-II hydraulic systems is such that the fluid supply attached to each engine drives the pitch and yaw actuator of that engine. A block diagram of the overall stage gimbal system and the unreliability of the individual blocks is shown in Figure 28. If a loss of one MPE

channel in both pitch and yaw can occur simultaneously without loss of control, which is consistent with the assumptions previously made, the capability of loss of one fluid supply out of the four also exists. Since the general equations cannot be applied directly to a multi-element system having this interconnection arrangement, a specific equation has been derived for this multi-element layout. With the assumptions stated, the following expression results:

$$P = R_j^8 R_w^4 + 8R_j^7 (1-R_j) R_w^4 + 4R_w^3 (1-R_w) R_j^8 + 16(1-R_j)^2 R_j^6 R_w^4 + 8(1-R_j) R_j^7 (1-R_w) R_w^3 \quad (48)$$

where R_j = individual actuator-servoamplifier reliability as previously indicated and R_w = individual hydraulic supply reliability = 0.998581 for the S-IC stage. Inserting the reliability numbers into equation 48 and reconverting results in the total subsystem assessment shown in Table V. The overall improvement ratio resulting from redundancy is $U_s/U_r = 43.1$.

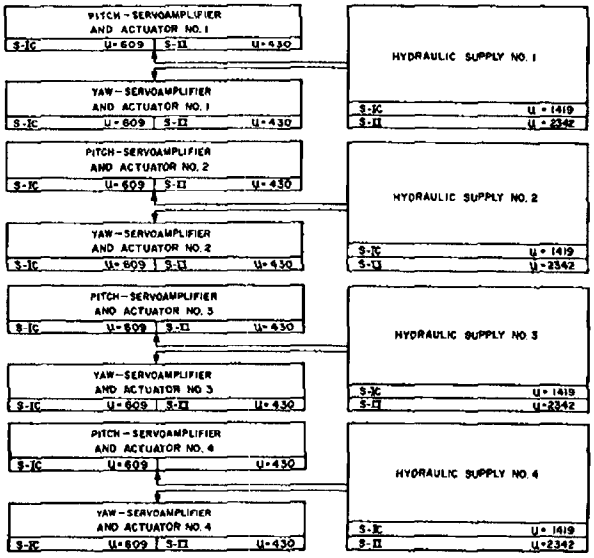


Figure 28. Multiengine Stage Gimbal System

Table V. S-IC Control

	U_{rp}	U_{sp}	$U_r + U_n$	U_s	U_s/U_r
Pitch, neglecting fluid supply	3	71	74	2507	33.9
Pitch, yaw, and roll, neglecting fluid supply	6	213	219	5085	23.2
Pitch, yaw, and roll, including fluid supply	37	213	250	10,760	43.1

Note that this analysis does not specifically consider the effect of "engine-out," i.e., the loss of propulsion of one of the four control engines. Even though the direct effect on the control system which would be the loss of control torques derived from one actuator in each axis is considered, other interactions are not treated in this simplified analysis.

As previously mentioned, the basic layout of the S-II control system is similar to that of the S-IC. Except for shaping networks, the electronics for the S-IC and S-II are identical, with the outputs of the servoamplifiers being switched at staging. Figures 26, 27, and 28 apply also to the S-II stage and show the corresponding unreliability numbers for the individual major elements for both stages. Similarly, equations 21 and 48 are used in the reliability assessment. The numbers used in the S-II stage assessment are $R_j = 0.999570$ and $R_w = 0.997658$. The results are shown in Table VI. The overall improvement ratio in the S-II stage through redundancy is $U_s/U_r = 46.8$.

Table VI. S-II Control

	U_{rp}	U_{sp}	U_r	U_s	U_s/U_r
Pitch, neglecting fluid supply	≤1	74	75	1794	23.9
Pitch, yaw, and roll, neglecting fluid supply	≤2	222	224	3662	16.3
Pitch, yaw, and roll, including fluid supply	61	222	283	13,254	46.8

The layout of the propelled phase pitch and yaw control of the S-IVB is basically different from that of the multiengine stages. Since only one main propulsion engine is employed, the control torques are derived by positioning a single actuator in each axis. A layout of the pitch and yaw control system is shown in Figure 29; the layout of the pitch and yaw channels is similar. Control about the roll axis is maintained by auxiliary engines and is discussed later. The electronic modules in the pitch and yaw channels are similar to those previously discussed, with the identical modules employed in the first two stages being used where possible. The shaping networks are different since they must have the particular characteristics required to stabilize the S-IVB stage. The S-IVB servoactuator is very similar in design to that previously described for the S-II stage, although a few features differ to adapt to the particular stage requirements. The S-IVB hydraulic fluid supply is also similar in layout to that of the S-II, but the individual components are of a different design. The major components of the inflight fluid supply system are the engine pump, a motor-driven auxiliary pump, an

integrated accumulator reservoir module, and associated interconnecting tubing.

Because the S-IVB pitch and yaw control torques are derived from a single engine, redundancy is employed to the maximum extent feasible. As shown in Figure 30, PRS redundancy is employed to derive the control signals to the servoactuators.

The reliability numbers applicable to a single PRS channel and the comparator electronics are $R = 0.999657$ and $R_v = 0.999932$. The corresponding

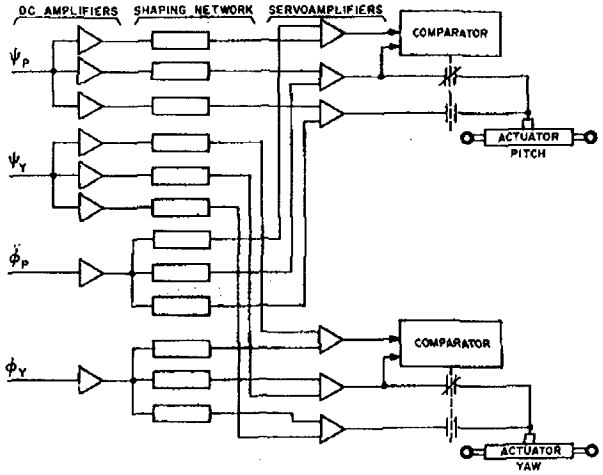


Figure 29. S-IVB Propelled Phase Pitch-Yaw System

unreliability numbers are shown in Figure 30. From equation 18, $P \geq 0.999999$ and $U_r \leq 1$. The reliability numbers for the simplex portions of the system are $R_{actuator} = 0.998437$ and $R_{supply} = 0.993563$. The equivalent unreliability numbers for these elements of the system are also shown in Figure 30. A single hydraulic fluid supply drives both the pitch and yaw actuators. Figure 31, a simplified block diagram of the total system, shows the unreliability associated with the various portions of the system, including the PRS redundant electronics. The resulting composite numbers are shown in Table VII.

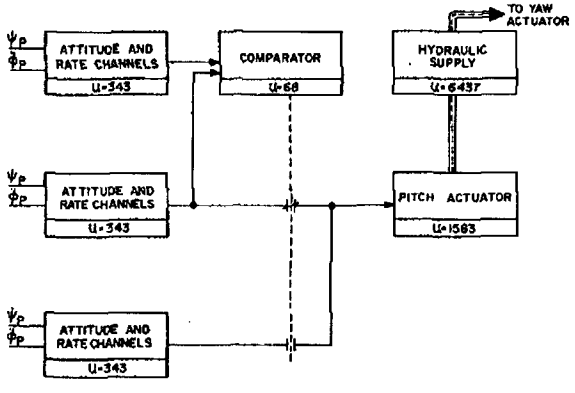


Figure 30. S-IVB Propelled Phase Pitch System (Simplified Model)

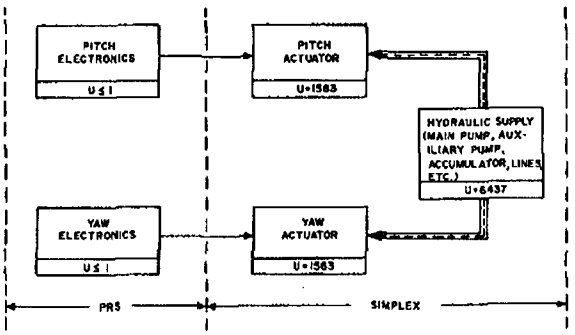


Figure 31. S-IVB Propelled Phase Pitch and Yaw Gimbal System Layout

Table VII. S-IVB Propelled Phase

	U_{rp}	U_{sp}	U_r	U_s	U_s/U_r
Pitch, neglecting fluid supply	≤1	1563	1564	1906	1.22
Yaw, neglecting fluid supply	≤1	1563	1564	1906	1.22
Hydraulic supply	0	6437	-	6437	-
Total system	≤2	9563	9565	10,249	1.07

Thus, for the total system, the unreliability has been decreased by the following factor through redundancy:

$$U_s/U_r = \frac{10,249}{9,565} = 1.07.$$

The numbers reveal a relatively small gain obtained by the redundancy applied in this subsystem; however, redundancy was applied only to the electronics, which is already the most reliable portion of the subsystem. This design is the result of engineering compromise. PRS redundancy was easily applied in the electronics; significant portions already existed in the control computer because of the multiengine stage requirements. On the other hand, the servoactuator and the hydraulic supply were not made redundant because of complexity of implementation and the resulting weight penalty.

This subsystem has a high unreliability because of the major simplex items and the possibility of introducing more redundancy is being pursued. A certain redundancy not considered in this analysis exists in the fluid supply because the system has two pumps. Although the auxiliary pump has a much lower flow than the main pump, it might sustain the system under certain main pump failure conditions. The addition of a second higher flow pump is being considered.

Also being considered is the use of a modified actuator design, which incorporates a "majority-voting" servovalve and essentially consists of a triplication of the valve and mechanical feedback mechanism in the servoactuator. In case of a malfunction in one channel, the two correctly operating channels overpower the third and the system continues to function properly. A considerable improvement could be expected in the valve

and feedback portions of the actuator; both contribute significantly to the actuator unreliability.

As previously mentioned, control about the S-IVB roll axis during propelled flight and about all axes during the coast phase is maintained by torques derived from the on-off operation of six auxiliary thrusters. A layout of the auxiliary control system is shown in Figure 32.

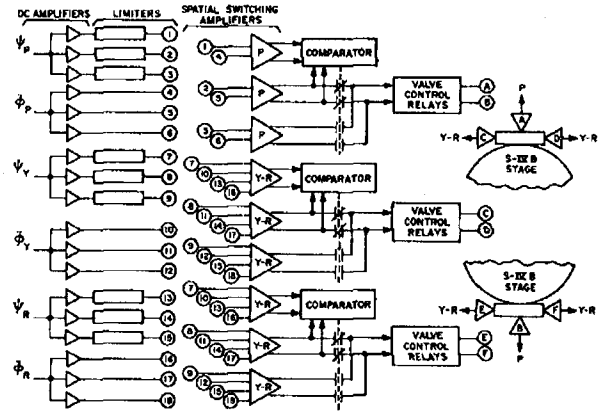


Figure 32. S-IVB Auxiliary Control System

The six inputs to the system (attitude and attitude rates) are derived in the same manner as during propelled phase control. The outputs of the electronic system actuate relays which operate the valves of the six auxiliary thrusters. As indicated, pitch is controlled by engines A and B; yaw and roll signals are intermixed and determine the operation of engines C, D, E, and F to maintain control about these two axes. In addition to scaling amplifiers similar to those employed in other flight phases to establish the correct relative gains in the system, the electronics also include attitude signal limiters, spatial switching amplifiers which operate the propellant valve relays, and spatial comparators. The attitude and attitude rate signals are summed in a magnetic amplifier stage similar to that employed in the propelled phases. The switching function is accomplished in a Schmitt trigger circuit which furnishes the input to the relay drivers. The relay drivers operate double-pole double-throw relays which switch power to the coils of the fuel and oxidizer valves of the thrusters. Pseudo-rate modulation circuitry, which provides a refinement of the simple on-off spatial attitude control techniques, is also included in the spatial amplifier module. The pseudo-rate circuitry provides a modulated band in which the duration and frequency of thruster pulses are varied depending on the input signals. When the input signal exceeds a certain level, the thrusters are commanded to the on position continuously; below a certain level, the thrusters are turned off and the vehicle attitude coasts within the prescribed deadband. The pseudo-rate modulated band provides a more rapid damping-out of disturbances and hence a more efficient utilization of thruster propellants. The electronics also contain a circuit which insures that when a thruster is activated it stays on for a certain minimum time. This characteristic is necessary to maintain the thruster specific impulse at the desired level.

The auxiliary control system employs two types of redundancy: (1) PRS redundancy similar to that previously described is employed in the electronics portion of the system, and (2) the propellant valves of the thrusters are connected in a quadruplex arrangement and are activated by parallel relays.

A simplified diagram of one axis of the auxiliary control system is shown in Figure 33. The pitch axis coast control represents the simplest layout. Roll and yaw coast control are similar to pitch with the exception that they are coupled and require four thrusters. The propelled phase roll control layout is similar to that of Figure 33 except that four thrusters are involved, with two being simultaneously activated for each roll correction.

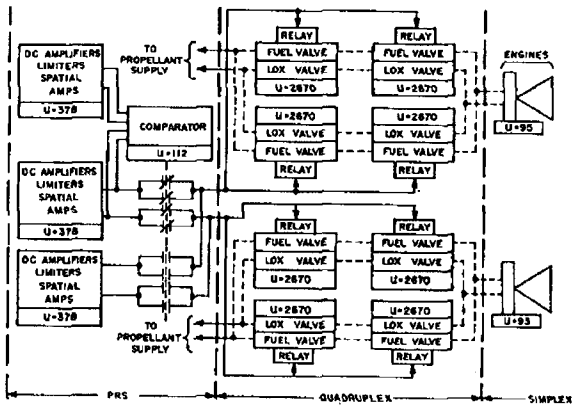


Figure 33. S-IVB Pitch Coast Control System

The reliability numbers applicable to the PRS electronics modules are R = 0.999622 and R_v = 0.999888. From equation 18, P ≥ 0.999999 and $U_{r(elect)} \leq 1$.

The numbers used for a single module of the quadruplex valving arrangement are $R = (R_{relay})\ (R_{valves}) =$ (0.999990) (0.997330) = 0.997340. Since the relay reliability is very high compared to the valves, the simplifying assumption is made that the relay can be included with the valves in this analysis. Using the numbers in equation 20 for a quadruplex arrangement yields R = 0.999986, $U_{r(valves)} = 14$. The total unreliability of the redundant portion is $U_{rp} = U_{r(elect)} + 2\,U_{r(valves)} = 1 + 2(14) = 29$. The term $2\,U_{r(valves)}$ arises from the two sets of quadruplex valves. Except for the valves, the APS engine is simplex. The applicable reliability number is R = 0.999905. Since two simplex engines are employed, the unreliability of this portion is $U_{sp} = 2(95) = 190$. The corresponding unreliability numbers for the individual electronic modules, valves, and engines are indicated in Figure 33. The unreliability of the pitch system as indicated is $U_r = U_{rp} + U_{sp} =$ 29 + 190 = 219.

The corresponding numbers for the yaw and roll channels can be similarly derived. These results along with those for the total system, an equivalent simplex system, and the improvement ratio are shown in Table VIII. The total system improvement ratio is $U_s/U_r = 27$.

Table VIII. S-IVB Auxiliary Attitude Control

	U_{rp}	U_{sp}	U_r	U_s	U_s/U_r
Pitch	29	190	219	5908	27.0
Yaw and roll	58	380	438	11,816	27.0
Total system	87	570	657	17,724	27.0

Note that the preceding assessment does not include the simplex APS propellant supply modules, which also supply the propellant for the S-IVB ullage engines.

The unreliability assessment for the various subsystems and the total control system is summarized in Table IX. As previously indicated, the improvement ratio is very large in the case of the rate system which is totally redundant; however, it is not very significant in the S-IVB propelled phase gimbal system because of the simplex hydraulic system. Primarily because of the relatively high unreliability of the latter, the improvement ratio of the total control system through redundancy is only a modest 5.3.

Table IX. Control System

	U_{rp}	U_{sp}	U_r	U_s	U_s/U_r
Pitch, yaw, and roll attitude rate sensing subsystem	20	0	20	4972	248
S-IC pitch, yaw, and roll subsystem	37	213	250	10,760	43.1
S-II pitch, yaw, and roll subsystem	61	222	283	13,254	46.8
S-IVB pitch and yaw propelled phase subsystem	≤2	9563	9565	10,249	1.07
S-IVB auxiliary attitude control subsystem	87	570	657	17,724	27
Total control system	207	10,568	10,775	56,959	5.3

Problems Associated With Redundant Applications

The benefits to be derived from redundancy have been demonstrated, and it has been shown that the unreliability of a simplex system can, in some cases, be reduced by orders of magnitude when redundancy is applied. Although the disadvantages of redundancy are not readily assessed quantitatively, it is recognized that this gain in reliability is at the expense of other design factors or operational procedures. Some of the problems encountered with the application of redundancy are enumerated and the effect of redundancy on the system is indicated.

The most significant disadvantage of redundancy is the increased complexity, both in terms of component parts and system organization. In the simplest forms, i.e., series or parallel components, the number of components is twice that of a simplex system. In a duplex modular system, the number of components is more than doubled to provide a means of sensing and switching. In the triple-modular redundant digital system, the voters and failure isolation and detection circuits require almost as many component parts as a single channel; therefore, a system contains between three and four times as many parts as a simplex system. In the PRS circuitry of the control system, the component count also ranges from three to four times that of a simplex channel, depending on the relative complexity of the comparator required. In the example of the quadruplex redundancy cited in the auxiliary control valves, no sensing or voting was required so the system is four times as complex. The only application of redundancy which does not add additional components to the system is the MPE gimbal system; the complexity of this system was imposed by other design considerations and the benefits of redundancy are achieved without additional complexity. The gain in reliability through redundancy is, in this case, a bonus rather than the primary purpose of the multiple parallel elements.

Other major problems inherent in redundant applications are failure detection and isolation. Failures in the redundant element must be detected and removed before flight. Failure to verify that all channels are operating can actually result in a degradation of the system compared to a simplex system. For instance, consider one trio of a TMR system. If the vehicle is launched with one of the units out, the system would fail if either of the other two malfunctioned. Since there are two remaining units, either of which could result in a system failure, the unreliability of the system is nearly twice that of the simplex system. Failures occurring during flight must be detected so that corrective action can be taken for future flights. Because more component parts are employed in redundant systems, the number of component part failures can be expected to be greater than those in a simplex system by a factor of the ratio of the number of component parts in a redundant system to the number of component parts in a simplex system.

The LVDC, LVDA, and control system illustrate how the failure detection and isolation problem is approached in the Saturn V guidance and control system. In the LVDC and LVDA, disagreement detectors indicate when a failure has occurred in either of these units, each of which consists of over 100 detectors. Several detectors are "OR'ed" together and fed to a bit in a 26-bit register, storing failure indications which can be read by the ground launch computer before flight and telemetered during flight. Sixteen bits of the register are used to store LVDC failure information while the remaining 10 bits are used for the LVDA. Because of the "OR'ing" operation, however, it is not always possible to pinpoint the cause of failures.

To assist in failure isolation before flight, means to switch in and out various redundant paths must be provided. For example, in checking the LVDA power supplies, switching both the feedback amplifiers and the converters is necessary. In the TMR logic, module as well as channel switching is desirable such that a failure can be isolated to two or three logic pages. These

features have been incorporated in the computer system and means are available for checking all alternate paths. The presence of the multiple channels within the redundant system, along with the isolation capabilities incorporated, considerably enhances the troubleshooting possibilities. This is a significant by-product of redundancy, particularly in a complex system such as the Saturn digital system.

Signals from the ground can be substituted during checkout for each of the three inputs to the PRS systems employed in the control system. The comparator's ability to switch can consequently be checked for various combinations of inputs, and the standby units can be exercised. Means are available to switch back from the standby to the prime unit from ground control in case the redundant circuit switches because of an intermittent condition during prelaunch checkout. In addition, the state of the comparators is telemetered such that switching to the standby is detectable during flight; however, the switch-back capability is not present during flight.

The necessity for failure detection, isolation, and removal of failed units is perhaps obvious; however, a more subtle problem arises in using these schemes in an operational prelaunch checkout system. For example, if a failure in a redundant flight item occurs hours before the flight, a spare may be substituted without impact on the countdown or launch. However, should a failure in a redundant item occur just seconds before the scheduled liftoff, the removal of the failed item would require a hold or a scrub, possibly resulting in a costly schedule delay. A tradeoff must be made between the effect of the failed unit upon mission success and the cost, schedule, and other critical considerations brought about by a hold or scrub. It is imperative then that redundancy considerations be included in launch ground rules, where practical. When applied, such considerations complicate launch procedures; when not applied, considerable pressure is brought to bear on engineering judgement.

To derive maximum benefit from the redundancy employed in the Saturn vehicle system, the computer system is utilized to the greatest extent possible because it is the only item within the vehicle capable of making logical choices and decisions. The Saturn V flight program is designed to make maximum use of the existing redundancies in the vehicle hardware. It is generally accepted that a major effort in any guidance and control system is the preparation and checkout of the flight program. This is particularly true in space vehicles where each mission is different from the previous one. Consequently, the "canned" programs cannot be used. Adding redundant features to system hardware complicates flight programs since backup paths or redundant loops must be incorporated. Examples have previously been cited of the value of the computer system in determining "reasonable" values for accelerometer and gimbal angle readings. If it is determined that these values are not "reasonable," alternate modes of operation are followed. Therefore, means must be provided in the various program checkout facilities where failures can be induced and alternate program modes can be checked in a manner similar to that employed in hardware checkout. A problem also exists in determining "reasonable" values, both in terms of which quantities should be used as well as the limits applied to each quantity.

Other disadvantages of redundancy, which are a direct outgrowth of increased complexity, are the physical quantities of increased power, weight, and cost. These quantities have not been, and probably cannot be, accurately assessed, but estimates can be made. The most straightforward of the above quantities to consider is power, since it is reasonable to assume that the power requirements of a system are directly proportional to the number of component parts; i.e., the ratio of the power required by a redundant system as compared to a simplex system may be estimated to be directly proportional to the ratio of the number of components in the two systems.

The weight penalty of a redundant system is not as easy to estimate, for consideration must be given to packaging density and efficiency, heat dissipation, and type of packaging technique employed. In general, weight ratio is estimated to be less than the component part ratio. How much less depends on factors such as type of redundancy employed, failure detection and isolation schemes, packaging techniques, and type of cooling method utilized.

The impact of redundancy upon cost is most difficult to analyze for it runs the gamut of the aforementioned problems. Cost is influenced by the number of parts, system design, checkout, programing, and launch costs. Cost is also greatly dependent upon the type of redundancy employed. From the initial design phase through the launch phase, the cost of a redundant system is probably from 3 to 10 times that of an equivalent simplex system.

Conclusions

The various types of redundancy employed in the Saturn guidance and control system and typical numbers demonstrating the improvements gained have been presented. Although the various types of redundancy show a theoretical difference in the relative improvements, the choice of the type employed in each case is in actuality dependent on the practical implementation aspects. In the design of the Saturn guidance and control system, the following approach was employed: Those portions of the system to which redundancy could be readily applied were first identified and then the type of redundancy was selected by numerical analysis and engineering tradeoff with emphasis on the latter.

Table X summarizes the unreliabilities of the guidance and control system, consisting of the three major systems.

Table X. Summary of Guidance and Control Subsystem Reliability

	U_r	U_s	U_s/U_r
Stabilized platform system*	8,669	15,408	1.77
Digital computer system	282	12,498	44.3
Control system	10,775	56,959	5.3
Total	19,726	84,865	4.3

*U_r includes considerations of backup out of orbit, while U_s refers to a totally simplex system (no subsystem redundancy and no backup).

The digital system, which is almost totally redundant, has a significantly lower unreliability than the other two systems. This should not be interpreted to mean, however, that incorporating redundancy in the other systems is to no avail. Actually, significant improvements are made in all three systems through redundancy. The fact that the three major systems have significantly different reliability and that the most reliable system (in simplex form) employs the highest degree of redundancy emphasizes the philosophy employed in the design of the Saturn system. The approach did not attempt to enforce equal reliability for subsystems of similar significance and complexity; it was instead to benefit to the maximum reasonable extent in those areas where redundancy could be readily applied while relying on simplex elements where redundancy would have resulted in undue complexity or other significant penalties. This philosophy results in significant differences in the extent to which redundancy is applied not only within the various portions of the guidance and control system but also throughout the total Saturn launch vehicle.

In the stabilized platform and control systems, the unreliability remains high compared to the digital system because each contains major simplex electromechanical elements. However, compared to other major systems in the launch vehicle, where little or no redundancy is incorporated, the systems look very favorable. The overall guidance and control system reliability is considered acceptable for the Apollo mission. The continuing investigations of backup schemes and design modifications being considered are merely to enhance the reliability further.

It should be reiterated that the unreliability numbers shown represent the predicted number of component or subsystem malfunctions in a million flights and not the number of mission failures. The latter, sometimes referred to as the criticality number, is derived by considering the individual failure modes and corresponding effects. The criticality numbers for the various subsystems are considerably lower than the unreliability numbers quoted.

Note that several subsystems closely related to the guidance and control system are not included in the analysis. Principal examples are the vehicle primary power source, the auxiliary propulsion system propellant source, the switch selectors which provide vehicle sequencing, and the digital command system. While these elements support the guidance and control system, they also perform other vehicle functions and support other major subsystems.

The benefits of redundancy must be traded off against the resulting penalties in weight, power, cost, and operational complexity; but the application of redundancy cannot be utilized as a substitute which permits relaxation of basic reliability design principles. High reliability component parts programs and tight quality controls must be maintained; to derive practical benefits, redundancy must be applied to a basically highly reliable system.

The Saturn guidance and control system is an inherently reliable system because major emphasis has been placed on design conservatism and simplicity, use of carefully selected component parts, and extensive testing. In addition, through judicious application of redundancy, the overall result is a system of very high reliability and flexibility. The dependability of the system has been demonstrated through three successful Saturn IB flights without a functional failure and many thousands of hours of ground testing. Weighing the results against the problems and disadvantages, we conclude that the design approach is justified and has been verified to be basically sound.

Acknowledgment

The authors express their appreciation to the various personnel within the Guidance and Control Division and the System's Engineering Office of Astrionics Laboratory and to the reliability analysts at IBM-Huntsville and IBM-Owego for their contributions. Special thanks are due Mr. John Gonsowski of IBM-Huntsville for his advice and assistance in the preparation of this paper.

Bibliography

1. Haeussermann, Dr. Walter; and Duncan, Dr. Robert C.: Status of Guidance and Control Methods, Instrumentation, and Techniques as Applied in the Apollo Project. Presentation to the Advisory Group for Aeronautical Research and Development, North Atlantic Treaty Organization, Duesseldorf, Germany, October 21-22, 1964.

2. Decher, Dr. Rudolph: The Astrionics System of Saturn Launch Vehicles. NASA TM X-53384, February 1, 1966.

3. Navigation, Guidance, and Control System Description, IBM Technical Manual, no. 66-966-0003, MSFC No. III-5-509-2, April 15, 1966 (changed May 1, 1966).

4. Thomason, Herman E.: A General Description of the ST-124-M Inertial Platform System. R-ASTR-G, NASA TN D-2983, December 1965.

5. White, Paul R.: ST-124-M 250VA AC Power Supply. R-ASTR-G-WP-10-65, April 19, 1965.

6. Kalange, M. A.; and Alcott, R. J.: Saturn V S-IC Stage Engine Gimbal Actuation System, R-ASTR-NF, May 18, 1965.

7. McGillen, V. W.; and Jacobs, M. R.: The Saturn S-II Stage Engine Actuation System. Space and Information Systems Division, North American Aviation, Inc., 650305, Undated.

8. Hamilton, M. J.: Design of a Hydraulic Gimbal System for a Moon Mission Booster Stage. Douglas Missile and Space Systems Division, Huntington Beach, California, Douglas Paper no. 3110, May 1965.

9. Control-EDS Rate Gyro Package, IBM Technical Manual, no. 66-966-0013, MSFC no. III-5-510-13, March 1, 1966.

10. Control Signal Processor. IBM Technical Manual, no. 66-966-0014, MSFC no. III-5-510-14, March 1, 1966.

11. Flight Control Computer. IBM Technical Manual, no. 66-99-0015, MSFC no. III-5-510-15, March 15, 1966.

12. Failure Effect and Reliability Analysis ST-124-M Three Gimbal Platform for Saturn C-5, R. E. File no. 7346, Bendix Corp., Teterboro, N.J., May 9, 1965.

13. Failure Mode, Failure Effect, and Criticality Analysis for S-IU-203, IBM no. 66-383-0004, MSFC no. III-2-220-4, April 1, 1966.

14. Saturn V Thrust Vector Control Failure Analysis. Boeing Document no. D5-11390, August 1964.

15. LeRoy, G. B.: Preliminary Reliability Analysis and Prediction, Moog Model-17-200A, Mechanical Feedback Servoactuator. Moog Report no. MR 975, September 11, 1964.

16. Reliability Report of Servoactuator, Mechanical Feedback (P/N 301100), Revision A. Hydraulic Research and Manufacturing Company, Burbank, California, June 8, 1966.

17. Shimizu, A.; and Schleich, W. T.: Stability and Criticality Analysis of the S-II Flight Control System. Space and Information Systems Division, North American Aviation, Inc. Report no. SID 64-1594, accession no. 66174-64, August 31, 1964

18. Reliability Engineering Model Saturn S-IVB-501 Stage. Vol. II, Failure Effect Analysis, Douglas Report SM-47406, Douglas Missile and Space Systems Division, Huntington Beach, Calif., March 1966.

19. Reliability Assessment Report for Saturn V Guidance Computer and Data Adapter. IBM Document no. 65-394-061, IBM Owego, New York, October 18, 1965.

20. Gonsowski, J. A.: Utilization of Monte Carlo Technique for TMR Reliability Predictions. IBM Document no. 63-394-059, IBM Owego, New York, Aug. 15, 1963.

21. White, J. B.: Improvement of Computer System Reliability Through Redundancy. MSFC Technical Publication, MTP-G&C-N-61-36, August 30, 1961.