Experimental Strapdown Redundant Sensor Inertial Navigation System

F. A. EVANS*
TRW Systems Group, Houston, Texas

AND

JAMES C. WILCOX†
TRW Systems Group, Redondo Beach, Calif.

An experimental strapdown redundant sensor package, assembled at the NASA Electronics Research Center (ERC), Cambridge, Mass., contains six gyros and six accelerometers whose input axes are perpendicular to the faces of a regular dodecahedron. The sensor signals are processed in real time by a digital computer. Program logic compares the performance of the gyros and accelerometers, and detects failed instruments. Accepted data are then combined to yield attitude, velocity and position. A calibration routine, used with a precision test table, yields sensor compensation data. An alignment routine employs sensed accelerations and rotations to determine initial attitude orientation in a sway environment. Simulations and analyses of the system are performed. The results show hard sensor failures are quickly detected. Soft failures present difficulties to the failure detection logic. The reliability of the redundant sensor system depends on the relative magnitudes of normal sensor performance, degraded sensor performance, and specified system performance.

Nomenclature

A = 6 × 3 direction cosines matrix
B = 3 × 6 least-squares solution matrix
C = 15 × 6 test matrix
c = $\cos\alpha$
f = 15 vector of prefilter outputs
K_f = prefilter gain
K_p = performance specification
K_1, K_2 = digital filter parameters
$p(m,n)$ = probability of m out of n instruments failing
q = probability of one instrument failing
s = $\sin\alpha$
T = sampling period
u = 15 vector of unfiltered test signals
v = 15 vector of threshold outputs
x = 3 vector of sensed quantity
$\hat{x}$ = 3 vector estimate of x
$\tilde{x}$ = 3 vector error in $\hat{x}$
x' = 3 vector used in least squares solution
y = 6 vector of instrument outputs
α = angle defining instrument orientation
Δt = reliability period
ϵ = 6 vector of instrument errors
λ = single instrument failure rate
σ = standard deviation of error of unfailed instrument
σ_F = standard deviation of error of failed instrument
τ_f = prefilter time constant

Subscripts

i,j = elements of matrix or vector

Presented as Paper 69–851 at the AIAA Guidance, Control, and Flight Mechanics Conference, Princeton, N. J., August 18–20, 1969; submitted August 21, 1969; revision received May 11, 1970. This work was partially supported by the Electronics Research Center under NASA Contract NAS 12-645.

* Manager, Mission Trajectory Control Program. Associate AIAA.

† Staff Engineer, Avionics Systems Department. Member AIAA.

Introduction

GUIDANCE and control reliability requirements have led to increasing emphasis on redundancy in system design. Redundancy can be provided at the system, subsystem, and component levels. In addition, there may be options as to which elements in the system should operate concurrently and which should be placed in standby. The standby concept may be extended to that of replacement wherein the redundant element is not constrained to be a fixed item in the system configuration, but may be used where a failure has occurred.

In principle, the aforementioned choices and concepts can be implemented either on a gimballed platform or a strapdown system. However, the use of multiple instruments on a gimballed platform raises questions regarding the mechanical, thermal, and electrical design, and failure isolation methods for removing faults before attitude reference is lost. In practice, redundancy in gimballed platforms occurs at the system level, as witness the triplicated systems being planned for large commercial and military aircraft. In the case of strapdown mechanization, instrument level redundancy becomes attractive since attitude reference is accomplished within a computer. Reasonableness checks may be performed on the redundant sensor data before it is used in the control and navigation loops. Such a redundant strapdown system would be compact, lightweight, and theoretically highly reliable.

The experimental strapdown configuration assembled at ERC contains six gyros (Kearfott King II) and six accelerometers (Kearfott 2412), all of which operate (none in standby). The instruments are oriented so that their input axes are perpendicular to the faces of a regular dodecahedron. Thus, no three gyros (accelerometers) are coplanar and the system can operate as long as any three gyros and any three accelerometers are unfailed. The concept of this configuration was originated by Ephgrave[1] and Gilmore.[2–4]

Although one cannot precisely compare triplicated platform systems with redundant strapdown systems without taking many factors into account, it is interesting to make a much simplified reliability comparison. If it is assumed that

the gyros are the only sources of failure, all gyros operate concurrently (no standby elements) for a period Δt, each has the same failure rate λ [reciprocal of mean time between failures], and perfect failure detection methods exist, then, for a $\lambda\Delta t$ of 0.1, the triplicated platform system has a reliability of 0.98 while the redundant strapdown system has a reliability of 0.999. (System failure occurs at the point where all three of the triplicated systems fail or where four gyros fail in the redundant strapdown configuration.) This gain in reliability through instrument redundancy is one reason for the evident interest in strapdown systems.

Experimental Configuration

A functional block diagram of the experimental strapdown redundant sensor inertial navigation system is shown in Fig. 1. The experimental strapdown redundant sensor package feeds trains of pulses to the real-time navigation computer. The computer, a Honeywell DDP-124, maintains an analytical attitude reference via its attitude reference algorithm and transforms and integrates accelerometer data to determine velocity and position. Before any sensor data are used, failure detection logic examines the data for reasonableness and rejects those instruments deemed to have failed. Alignment and calibration routines and a vehicle flight simulator (driver routine) are provided in the computer program. The simulator produces sensed data corresponding to simulated trajectories and simulated instrument bias, scale factor, mass unbalance, and misalignment errors. Instrument errors can also be simulated in the redundant sensor assembly hardware.

Computer program development, undertaken at TRW Systems Group under contract to ERC, was completed in May 1969. The attitude reference and navigation equations were taken from previous work on the TRW Abort Guidance System, a strapdown space guidance system flown on board the Apollo Lunar Module spacecraft during the recent Earth and Lunar missions. The attitude reference equations consist of second order Taylor series updating of a direction cosine matrix every minor compute cycle. A 40-msec minor cycle period was chosen for the redundant sensor experiment. This rather long period allows the complete computation of the failure detection equations every minor cycle in the DDP-124 computer. In an operational system where high vehicle rotation rates can occur, a shorter minor cycle period will be desirable.

The navigation equations are expressed in an Earth-centered inertial frame. This leads to simple equations at the risk of round-off errors in the fixed-point DDP-124 computations.

The driver equations employ analytic functions to represent the desired position and attitude of a simulated aircraft. The functions are differentiated to produce velocity, acceleration, and angular rates. The acceleration and angular rates are used to construct the simulated accelerometer and gyro pulse trains which can be used to drive the navigation program. When the driver routine is employed, navigation errors are measured by comparing the navigation outputs with the original driver quantities.

Calibration, alignment and failure detection are new functions specifically designed for the strapdown redundant sensors experiment. Calibration requires that the redundant sensor assembly be sequentially placed in specific orientations and also rotated at controlled rates. This is accomplished on a precision rate table. The alignment routine consists of a Kalman filter which estimates the elements of the direction cosine (attitude) matrix without external aids (gyrocompassing). The filter state variables are the misalignment angles about the local vertical, east, and north axes. The observations are the east and north components of sensed velocity.

The calibration and alignment functions will not be discussed in this paper since space does not permit. The emphasis will be on the important question of failure detection, diagnosis, and correction (FDDC) design and analysis.

Methods of Failure Detection and Diagnosis

The Experimental Redundant Sensor Assembly (ERSA) consists of six gyros and six accelerometers mounted on a fixture along with the necessary thermal control devices. The dodecahedron configuration is the optimal one for six instruments where failures are independent and equally likely; this minimizes the effects of errors on performance.[1-4] As long as no more than three gyros and three accelerometers have failed, the ERSA is capable of operation.

The detection and diagnosis of failures of the gyros and accelerometers can be accomplished in at least three ways: 1) comparison of the instrument output with the outputs of the other inertial instruments of the same type; 2) sensing some of the internal states of the inertial instrument; and 3) comparison of the instrument output with the outputs of electromagnetic radiation sensors [such as star trackers, Doppler radars, LORAN(long range navigation), etc.].

If three instruments of the same type have failed, systems using methods 2 and 3 can continue to operate, whereas method 1 needs at least four unfailed instruments of the same type to diagnose which instruments are failed. (Method 1 does detect the third failure.)

Method 2 does not sense the most significant state of the instrument—its output. If some internal state of the instrument exceeds its predetermined threshold, the instrument is classed as failed, whether or not its output exceeds the system specification. Also, a failure may cause the specification to be exceeded without causing any of the monitored internal states to exceed their threshold.

Method 3 has the disadvantage that the electromagnetic radiation sensor output signal and noise are in different frequency regions from those of the inertial instrument. Method 3 is not considered herein. Methods 1 and 2 are discussed in the subsequent sections.

Methods of Failure Correction

The correction of failures of the gyros and accelerometers can be accomplished in at least two ways: 1) combining the outputs of the unfailed instruments by the method of least squares, or 2) estimating the variances of the errors of the failed instruments and combining the outputs of all of the instruments by the method of weighted least squares (equivalent, in this case, to minimum variance estimation).[5]

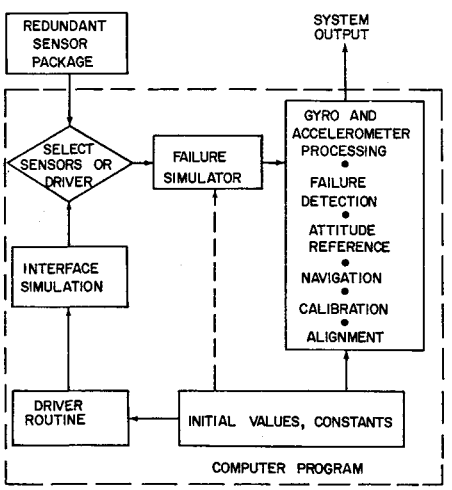

Fig. 1 Functional block diagram.

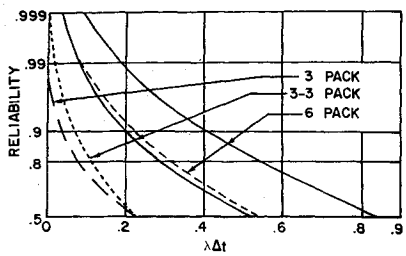

Fig. 2 Reliability for various system configurations.

The first method may be considered as a special case of the second, in which the variances of the errors of the failed instruments are taken as infinite. Although the second method is capable of better performance than the first, it requires much more computation. The first method was chosen for the experiment.

Reliability and Performance

The reliability and performance of the ERSA are related through the FDDC operation. If the FDDC is not perfect, a false alarm (unfailed gyro classed as failed) or missed alarm (failed gyro classed as unfailed) may occur, causing a reduction in reliability or an increase in system error or both, depending upon the definitions of reliability and performance. Reliability is defined here as the probability that the ERSA will operate for a given period of time without exceeding the specified error. Performance is defined in terms of the magnitude of the small angle error vector (for gyros) or the velocity error vector (for accelerometers) at the end of a flight. Thus, a change in the performance specification will cause a change in the reliability. In the immediate discussion it is assumed that the FDDC is perfect, so that ERSA reliability and performance can be examined in a simple manner.

If q is the probability of a given instrument failing during a specified time interval, then the probability of m out of n instruments failing in the specified time interval is given by

$$p(m,n) = [n!/m!(n-m)!]q^m(1-q)^{n-m} \tag{1}$$

When a constant failure rate λ and a time interval Δt are assumed, the probability of a given instrument failing is

$$q = 1 - e^{-\lambda\Delta t} \tag{2}$$

The reliability of the dodecahedron configuration (6 pack) is compared with the reliability of three 3-instrument units (three 3 packs) in Fig. 2. If any failure occurs in a 3 pack it is considered failed. The short-dashed curves are for the output comparison case where two unfailed 3-packs or four unfailed instruments in the 6 pack are needed for diagnosing the failure. The solid curves are for the case where external diagnostic information is available. Only one unfailed 3 pack or three unfailed instruments in the 6 pack are needed for successful operation. The long-dashed curve shows the reliability of a single 3 pack for reference. If there are any series elements (common power supplies, clocks, heaters, or computer) with significant failure rates, the actual reliability will be much less than that shown.

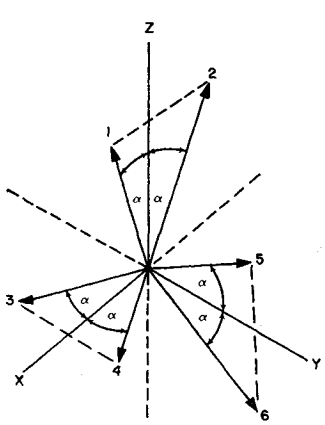

Fig. 3 Instrument input axis orientations.

As the number of failures increases, the system error increases. Let us assume that the errors of the instruments are statistically independent, with zero mean and unit variance. Thus the instrument error covariance matrix $\langle\epsilon\epsilon^T\rangle$ is the 6×6 identity matrix. Let

$$y = Ax + \epsilon \tag{3}$$

where y = instrument output 6 vector, A = direction cosines 6 by 3 matrix, x = sensed quantity 3 vector in package axes, and ϵ = instrument error 6 vector, and

$$A = \begin{bmatrix} s & 0 & c \\ -s & 0 & c \\ c & -s & 0 \\ c & s & 0 \\ 0 & c & s \\ 0 & c & -s \end{bmatrix} \tag{4}$$

where

$$c = \cos\alpha = [0.5 + (0.05)^{1/2}]^{1/2} \tag{5}$$

$$s = \sin\alpha = [0.5 - (0.05)^{1/2}]^{1/2} \tag{6}$$

where α is defined in Fig. 3.

If no instruments are failed, the optimal estimate of the sensed quantity is given by the least-squares solution

$$\hat{x} = (A^TA)^{-1}A^Ty = By \tag{7}$$

The error in the estimate of the sensed quantity is

$$\tilde{x} = \hat{x} - x = B\epsilon \tag{8}$$

The covariance matrix of the error is, from Eqs. (3, 7, and 8)

$$\langle\tilde{x}\tilde{x}^T\rangle = B\langle\epsilon\epsilon^T\rangle B^T \tag{9}$$

$$\langle\tilde{x}\tilde{x}^T\rangle = (A^TA)^{-1} \tag{10}$$

If one or more instruments have failed and have been properly switched out, the optimal estimate of the sensed quantity is given by Eq. (7) with the appropriate rows of A set equal to zero. Similarly, the resultant error covariance matrix is found by setting the appropriate rows of the A matrix to zero in Eq. (10).

For zero instruments failed, the system error ellipsoid axes may be taken in any direction (spherical symmetry). For one instrument failed, axis A (longest axis of the error ellipsoid) is along the input axis of the failed instrument. Axis B may have arbitrary orientation about axis A. Axis C, equal in length to axis B, completes the triad.

For two instruments failed, their input axes form two acute and two obtuse angles. Axis A bisects the acute angles. Axis B bisects the obtuse angles. Axis C, the shortest of the error ellipsoid axes, is perpendicular to both input axes. For three instruments failed there are two equally probable possibilities. The orientation of the error ellipsoid may be described for each situation. However, the discussion is somewhat involved.[6]

Average errors for a given number of failures are computed by adding together all of the covariance matrices and dividing by the number of matrices. The result turns out to be equal to the identity matrix multiplied by a scalar, the square root of which is called the average error. Thus, when averaged over-all possible failure modes, the errors are spherically symmetric. Table 1 presents the standard deviations of the errors in the error coordinate system and the average errors.

The average error of a subset of four instruments (two instruments failed) is seen to be equal to the error of three instruments in the orthogonal configuration (1.0).

Table 1 Accuracy vs failures

No. instruments failed	Error coordinate system axes A	B	C	Average error
0	0.707	0.707	0.707	0.707
1	1.000	0.707	0.707	0.816
2	1.345	0.831	0.707	1.000
3 (a)	1.345	1.345	0.727	1.581
3 (b)	3.068	0.831	0.831	

ERSA Failure Detection Logic

Output Comparison Failure Detection and Diagnosis

The output of any given instrument in the ERSA configuration can be computed from the outputs of any other three instruments in the assembly. This forms a subset of four instruments whose combined output should always equal zero. If the comparison results in disagreement (combined output not zero), it is not known which instrument has failed. However, if all the subsets of four instruments that include the given instrument are in disagreement and it is assumed that no more than two instruments have failed, it can be concluded that the given instrument has failed. Thus output comparison failure detection and diagnosis is accomplished by means of 15 test signals (6 gyros taken 4 at a time). The test signals (nominally zero) are linear functions of the instrument outputs

$$u = Cy \tag{11}$$

where u = test signal 15 vector, and $C = 15 \times 6$ test matrix. Each row of C performs a test on a different subset of four instruments. Thus a different pair of elements in each row is zero. From Eqs. (3) and (11)

$$u = CAx + C\epsilon \tag{12}$$

The ideal test signal should depend on the error and not on the sensed quantity. Therefore

$$CA = 0 \tag{13}$$

We require arbitrarily that

$$\sum_{j=1}^{6} C_{ij}^2 = 2 \tag{14}$$

This establishes the absolute magnitude of the test signals and does not affect the relative magnitudes. C is determined (except for the sign of each row, which is unimportant) by the distribution of zeros, Eqs. (13), and (14). For the nominal A matrix

$$C = \begin{bmatrix} 0 & 0 & -c & c & -s & -s \\ 0 & c & 0 & s & -c & s \\ 0 & c & s & 0 & -s & c \\ 0 & -s & -c & s & 0 & -c \\ 0 & s & -s & c & -c & 0 \\ c & 0 & 0 & -s & -s & c \\ c & 0 & -s & 0 & -c & s \\ -s & 0 & -s & c & 0 & -c \\ s & 0 & -c & s & -c & 0 \\ -s & -s & 0 & 0 & c & -c \\ c & -s & 0 & -c & 0 & s \\ -s & c & 0 & c & -s & 0 \\ -s & c & c & 0 & 0 & s \\ c & -s & -c & 0 & -s & 0 \\ c & -c & -s & -s & 0 & 0 \end{bmatrix} \tag{15}$$

In practice, the nonzero elements of C will differ slightly from Eq. (15) because of misalignments. Separate A and C matrices must be supplied for gyros and accelerometers, which may be misaligned slightly from each other.

In order to reduce the frequency of false and missed alarms, each component of u is filtered with a first-order low pass filter to remove quantization and other high-frequency noise. The digital filter is represented by the equation below, the 15 vector f containing the smoothed test signals as elements

$$f \leftarrow K_1 f + K_2 u \tag{16}$$

where

$$K_1 = e^{-T/\tau_f} \tag{17}$$

$$K_2 = K_f(1 - K_1) \tag{18}$$

T is the sampling period, τ_f is the filter time constant, and K_f is the filter gain.

Each element of f is compared with a threshold level of unity. A vector v is used to store, in binary form, the results of the comparison of f to the threshold, with a "0" corresponding to unfailed and a "1" to failed. At the start of the mission, v is initialized to zero. At each minor cycle time, f is scanned. If the threshold is exceeded by f_i, then v_i is set equal to 1. If an element of v is 1, it means only that one or more of the four instruments contributing to that element is failed. If an element of v is 0 it means that all four instruments are good (or at least consistent). Therefore, an instrument is considered failed only if all v_i to which it makes a contribution are 1. If a v_i is judged as failed, and later appears to be within tolerance, it is still classed as failed (v_i not reset to 0). This procedure is necessary because a failed tetrad may pass the aforementioned test on occasion. For example, if two instruments have failed, their errors could nearly cancel, causing an element of f to be less than tolerance.

If all of the v_i are 1, three or more instruments have failed and internal monitoring must be employed.

Internal monitoring failure detection and diagnosis

The internal monitoring FDD is very simple in concept. Discrete signals are received from hardware thresholds in each instrument. If any of the signals from a particular instrument indicate failure, that instrument is classed as failed. In practice, to implement internal monitoring, it is important that an accurate, detailed failure model be available. This type of information is usually difficult to obtain.

Failure correction

Once the decision has been made of which instruments are failed and which are not, it is necessary to compute rapidly an estimate of the sensed quantity from the outputs of the unfailed instruments. The optimal estimate is given by Eq. (7), where the rows of A corresponding to the failed instruments are replaced with zeros. The matrix B need be calculated only when a change in the number of failures occurs. If this is done the estimate of x is found from

$$\hat{x} = By \tag{19}$$

each minor cycle. The calculation of B in Eq. (7) is lengthy and a hard failure might cause the system performance specification to be exceeded before the computer could calculate B. One alternative would be to precalculate and store the B matrices for all 42 possible combinations of failed and unfailed instruments. This would require considerable computer memory. The alternative employed for ERSA is to solve each minor computer cycle the three linear equations in three unknowns

$$(A^T A)\hat{x} = x' \tag{20}$$

where

$$x' = A^T y \tag{21}$$

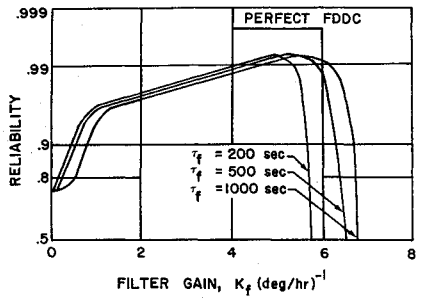

Fig. 4 Reliability for $K_p = 3$, $\sigma_F = 10°/hr$.

Equation (21) requires the same computer time as Eq. (19), and solving Eq. (20) by Gauss-Jordan reduction, taking advantage of the symmetry of the coefficient matrix, takes considerably less time than calculating B. Hard failure can thus be corrected before any erroneous data is used.

Analysis of ERSA Failure Detection

An analysis (extracted from Ref. 6) is presented for the selected FDDC logic, for the gyros only. The error of the failed gyros is considered to be an angular velocity step of gaussian distributed magnitude with standard deviation σ_F. The system performance specification is defined by K_p. If σ is the standard deviation of the accumulated error of a single gyro at the end of the flight, then the system is considered failed if the magnitude of the system angular error vector at the end of the flight exceeds $K_p\sigma$. Figure 4 shows the variation of the 1 yr reliability with filter gain for various filter time constants. A 10-hr flight and gyro failure rate of 5.4×10^{-6}/hr are assumed. The gyro errors are such that σ is 13.25 arcmin at the end of 10 hr.

Table 2 presents the peak reliability for combinations of σ_F and K_p. The table shows that increased reliability can be obtained by relaxing the performance specification. It also shows that reliability increases with the standard deviation of the error of the failed gyro; that is, the system works better for hard failures than for soft failures. The maximum reliability for a perfect FDDC of the type considered is 0.9982. This is essentially the reliability for hard failures. For example, if half of the failures are hard and half soft, then (for $\sigma_F = 10$ and $K_p = 3$),

$$R = 0.5 \times 0.9925 + 0.5 \times 0.9982 = 0.9954 \quad (22)$$

Although the reliability achieved is a major improvement over that achieved by a three instrument package, it is seen that the theoretical reliability for a perfect FDDC is not attained. For example, for $\sigma_F = 10$ deg/hr and $K_p = 3$, the unreliability is 0.0075. The unreliability corresponding to three or more gyros failing is ideally only 0.0018. Thus unreliability of 0.0057 is due to FDDC imperfection. Part of this unreliability is caused by false alarms (switching out a good gyro) and part by missed alarms (a failed gyro not switched out).

Table 2 Reliability vs σ_F and K_p

σ_F, deg/hr	K_p = 2	K_p = 3	K_p = 4
5	0.9713	0.9844	0.9871
10	0.9792	0.9925	0.9954

Summary

This paper has reported work accomplished in support of the ERC Strapdown Redundant Sensor Experiment. The redundant system as implemented and analyzed here should offer considerable improvement in reliability over a nonredundant system. It was determined that failure detection effectiveness is an important factor in redundant system reliability. Important findings were as follows.

1) Ideal reliability cannot actually be attained because of missed and false alarms.

2) Reliability depends on the relative levels of normal and failed instrument performance and specified system performance requirements. Reliability increases with the margin between system requirements and expected instrument performance. Hard failures are more reliably detected than soft failures.

3) Output comparison of redundant measurements provides a general method for detecting failure. Additional information sources are required to identify a failed instrument when redundancy is lost but sufficient unfailed instruments remain in the system for successful, albeit nonredundant system operation. Hence, output comparison alone cannot realize the full reliability potential of a redundant system.

References

[1] Ephgrave, J. T., "Optimum Redundant Configurations of Inertial Sensors," TOR-1001(9990)-5, Sept. 1966, Aerospace Corp., El Segundo, Calif.

[2] Gilmore, J. P., "A Non-Orthogonal Gyro Configuration," M. S. thesis, Jan. 1967, Massachusetts Institute of Technology, Cambridge, Mass.

[3] Gilmore, J. P., "A Non-Orthogonal Multi-Sensor Strapdown Inertial Reference Unit," E-2308, Aug. 1968, Massachusetts Institute of Technology Instrumentation Lab., Cambridge, Mass.

[4] Crisp, R., Gilmore, J. P., and Hopkins, A., Jr., "SIRU—A New Inertial System Concept for Inflight Reliability and Maintainability," E2407, May 1969, Massachusetts Institute of Technology, Cambridge, Mass.

[5] Ephgrave, J. T., "Redundant Adaptive Strapdown Inertial Navigation System," TOR-0066(5306)-10, Oct. 1969, Aerospace Corp., El Segundo, Calif.

[6] Wilcox, J. C., "Failure, Detection, Diagnosis, and Correction Design and Analysis," 09665-6012-R0-00, Jan. 1969, TRW Systems Group, Redondo Beach, Calif.