NASA CONTRACTOR REPORT 166594

(NASA-CR-166594) RELIABILITY ANALYSIS OF AN ULTRA-RELIABLE FAULT TOLERANT CONTROL SYSTEM (Search Technology, Inc.) 55 p HC A04/MF A01 CSCL 01C

N84-31219

Unclas G3/08 21246

Reliability Analysis of an Ultra-Reliable Fault Tolerant Control System

R. E. Curry
W. E. VanderVelde
P. R. Frey

Contract A16966C
July 1984

NASA

NASA CONTRACTOR REPORT 166594

Reliability Analysis of an Ultra-Reliable Fault Tolerant Control System

R. E. Curry
W. E. VanderVelde
P. R. Frey

Search Technology
540 University Avenue
Palo Alto, California 94301

Prepared for
Ames Research Center
under Contract A16966C

NASA
National Aeronautics and
Space Administration

Ames Research Center
Moffett Field, California 94035

SUMMARY

High system reliability in computer and control systems is necessary to meet the requirements of mission success. Using fault tolerant computers, rather than extremely reliable components, can be a more effective method of acheiving the desired system reliability. The architecture of NASA's Ultra-reliable Fault Tolerant Control System (UFTCS) is based on a larger number of redundant components and static redundancy management. This approach, as applied to vehicle control, consists of parallel and redundant paths of sensor modules, computation modules, and voter modules to acheive the fault tolerant operation.

This report analyzes the reliability of the NASA UFTCS architecture as it is currently envisioned for helicopter control. The analysis is extended to air transport and spacecraft control using the same computational and voter modules applied within the UFTCS architecture. The system reliability is calculated for several points in the helicopter, air transport, and space flight missions when there are initially 4, 5, and 6 operating channels. Sensitivity analyses are used to explore the effects of sensor failure rates and different system configurations at the 10 hour point of the helicopter mission. These analyses show that the primary limitation to system reliability is the number of flux windings on each flux summer (4 are assumed for the baseline case). Tables of system reliability at the 10 hour point are provided to allow designers to choose a configuration to meet specified reliability goals.

INTRODUCTION

High system reliability in computer and control systems is necessary to meet the requirements of mission success. Even with the most reliable components envisioned to be available in the near future, a fault tolerant system architecture is required to meet system reliability goals.

There are many approaches to implementing fault tolerant computing. Several of these which are newly available in the commercial market place are described in [1]. Two approaches for aircraft control are described in [2] and [3]. These two methods, which were developed before the dramatic reductions in size, power requirements, and weight of microelectronics, depend on complex logic and system reconfiguration to minimize the amount of hardware.

The architecture of NASA's Ultra-reliable Fault Tolerant Control System (UFTCS) [4] relies on a larger number of redundant components and static redundancy management. This approach, as applied to vehicle control, consists of parallel and redundant paths of sensor modules, computation modules, and voter modules to achieve the fault tolerant operation. This architecture encourages spatial distribution of the modules and different hardware and/or software in the parallel paths to reduce the risk of common mode failures and common mode design errors.

The purpose of this report is to perform a reliability analysis for the NASA UFTCS architecture as it is currently envisioned for helicopter control. The analysis is extended to air transport and spacecraft control using the same computational and voter modules applied within the UFTCS architecture.

SYSTEM DESCRIPTIONS

Functional Description

The NASA Ultra-reliable Fault Tolerant Control System (UFTCS) is based on the concept of interconnected modules for sensing, computation, actuation, and voting, and these modules contain parallel and redundant processes running asynchronously. The outputs of each sensor module and each computation module are cross-strapped to voting elements; that is, the output of each sensor module and the output of each computation module is directed to all following voting elements.

A typical block diagram for the control of a helicopter is shown in Figure 1 which displays N_m sensor modules and their voters, N_c computation modules and their voters, and the voting flux summers for each of the N_a actuators. Each solid line in the diagram is a fiber optic communications path on which data are transmitted serially, and each dashed line is an analog signal path.

Each sensor module contains one sensor for each required measurement and thus the sensor module is capable of producing a complete measurement set. The sensor module sends the readings of all its sensors to all voters over the fiber optic link. It is possible to obtain a complete measurement as long as there is at least one valid sensor (and its corresponding transmitter) for each required measurement located somewhere within the N_m sensor modules. In other words, sensors may fail within all sensor modules and a complete measurement set can still be realized.

Each voter following the sensor modules passes a valid measurement set to a single computation module. The output of each computation module is cross-strapped to four voter modules

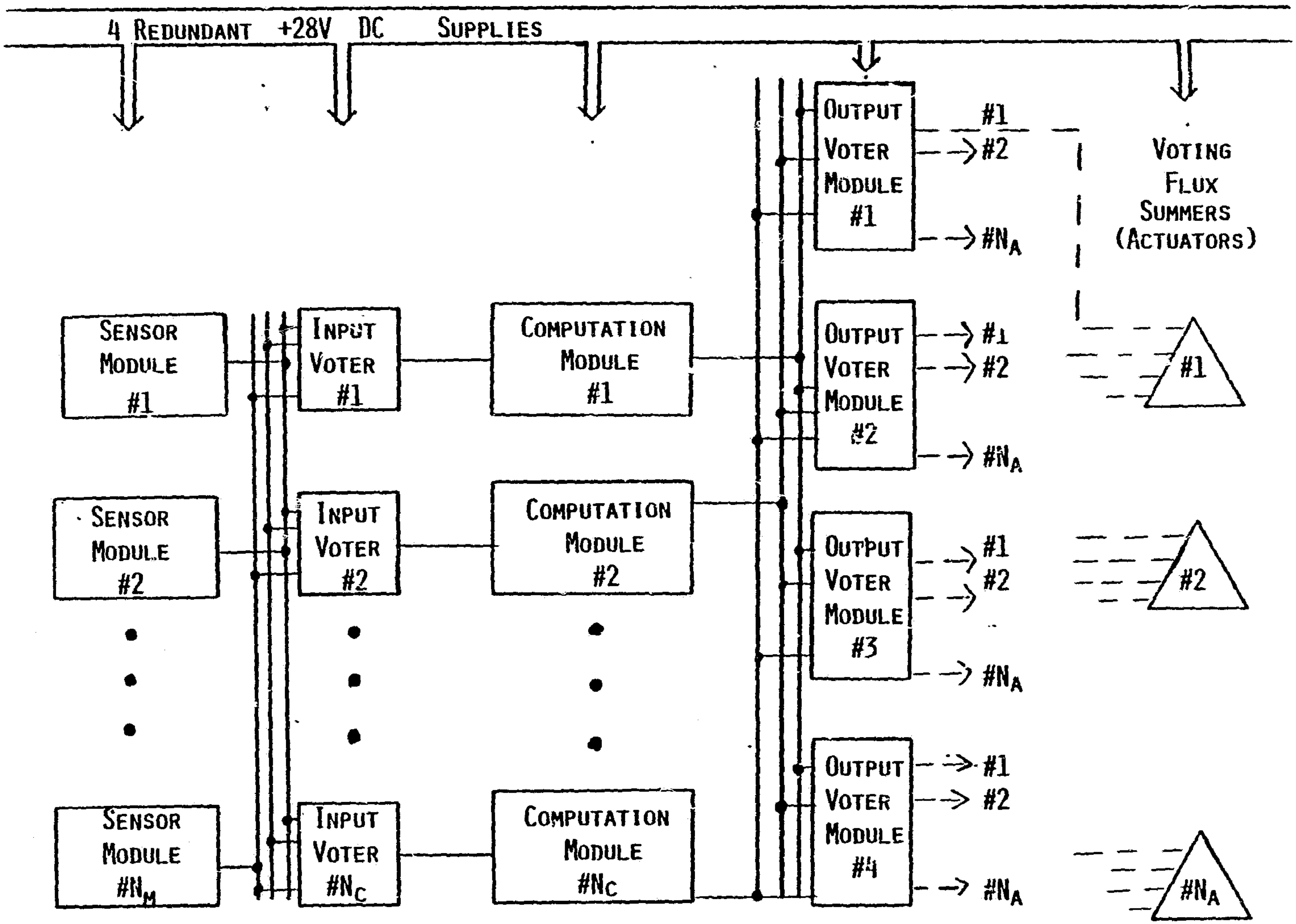

FIGURE 1. UFTCS DIAGRAM WITH N_M SENSOR MODULES, N_C COMPUTATATION MODULES, AND N_A ACTUATORS

which drive the actuators. These voters have one digital to analog converter (DAC) connected to every voting flux summer. Only four voters follow the computation modules because, in the system shown here, each voting flux summer requires four analog inputs each having limited authority. (The more general system configuration may have other than four voters, but there must be one for each analog input to the voting flux summers.)

Power Supplies

The ship's four redundant power supplies provide +28 volt DC unregulated power. These four supplies are cross-strapped to each circuit card and sensor (see the appendix for the circuit diagram).

Sensor Module

It is assumed for the analysis that each sensor module contains one sensor for each required measurement, and that all sensors are digitally encoded and feed into a computational element for transmission to the voter stage. (A computational element contains one 8086/8087 circuit card as shown on Drawing A14-82-235-101 supplied by NASA). The following assumptions have been made for the capabilities of the UFTCS:

Helicopter and Air Transport: The mission requires stability augmentation, altitude hold, and heading select. To meet these requirements, the following sensors are included in each sensor module:

1 Altimeter

1 Flux gate compass (long term heading reference)

2 Accelerometers (long term gravity reference)

3 Rate gyros

Space Flight: The mission requires maintaining inertial attitude; thus the assumed sensors are

3 Angular position sensors (optical)

3 Rate gyros

Input Voter Module

The computations within the input voter module are performed by an 8086/8087 design (adapted from NASA Drawing A14-82-235-102). The voter module receives an input from each sensor module via the optical fiber communications link (one link for each sensor module). This requires one optical receiver and one 8751 input/output processor for each link so that, in general, the failure rate of each voter depends on the number of parallel, redundant paths.

The logic of the voter modules has not been specified at this point, yet certain characteristics are likely to be incorporated. A voter logic which contains time history information will be useful in detecting hardover failures even with only two operating channels, allowing operation to one valid channel. With two channels operating, however, it would not be possible to unambiguously detect a drifting failure. See the Analysis Section for a further discussion of this point.

Computation Module

The computation modules are made up of three 8086/8087 computation elements (adapted from NASA Drawing A14-82-235-101) sharing the computational load. Thus the failure of any component in any one of the three computational elements constitutes a failure of the module.

Output Voter Module

Like the input voter module, the computations within the output voter module are performed by an 8086/8087 design (adapted from NASA Drawing A14-82-235-102). The voter module receives an input from each computational module via the optical fiber communications link (one link for each computational module). As with the input voter module, the failure rate of each output voter depends on the number of parallel, redundant paths.

The number of output voter modules is limited to four because of the quarter authority characteristics of the flux summer.

Voting Flux Summer Module

Each actuator is driven by four analog signals from output voter DACs, and each of these four signals has one quarter authority (flux summing). In addition, the voting flux summers can disconnect any of these drive signals if the error between the drive signal and the actuator feedback signal exceeds a specified threshold for a specified time. The UFTCS actuators will be considered operational if there are at least two of the four drive signals connected.

The following assumptions have been made for the actuator assignments in the three environments:

<u>Helicopter</u>: pitch, roll, yaw, collective

<u>Air Transport</u>: pitch, roll, yaw, ganged throttle quadrant

<u>Space Flight</u>: pitch, roll, yaw

ANALYSIS

Introduction

The reliability characteristics of the UFTCS are analyzed in this section leading to a computable expression for its predicted reliability over a given mission interval. The assumptions and approximations used in the analysis are stated. The formulation is general as to the number of power supplies, sensor modules, etc. employed in the system and it allows for different numbers of different modules. Thus, if the least reliable module should prove to be the sensor module, for example, the final reliability expression is applicable to a configuration that has more sensor modules than computation modules. This will permit the tailoring of a system to meet a reliability specification with a minimum number of components.

Assumptions

The assumptions used in this analysis are summarized in this section. These assumptions are common to most reliability analyses.

1) The failures we are analyzing, as reflected in the failure rates assigned, are permanent failures, not transient failures. This assumption seems especially well justified for the UFTCS because of its ability to return a component to active status after it had been declared failed for a transient reason.

2) The failure rate is assumed constant for all components. This nearly universal assumption is appropriate for high reliability systems in which a burn-in period is used to eliminate early failures due to manufacturing defects which have escaped inspection, and components which are subject to wearout effects are replaced on a scheduled basis.

3) Failures of individual components are considered independent. In a highly redundant system, it is important that the design of the components be such as to essentially guarantee this condition. This requires electrical isolation, spatial diversity and other measures to reduce the likelihood of one failure inducing others or single events causing several failures.

The combination of assumptions (2) and (3) means that the reliability of modules which have no redundancy within the module is given by the exponential form:

$$R(t_m) = P\ (\text{Module works at least as long as } t_m)$$
$$= \exp\ (-\lambda t_m)$$

with λ = Sum of the λ_i for all the components which are essential to the function of the module.

4) We assume all system components to be operational at the beginning of the mission. It may be useful, in future studies, to relieve this assumption, but in a combinatorial analysis such as is pursued here, it is very difficult to account for all combinations of system status at the beginning of the mission. The operational procedure for the system will surely be designed to approach this condition as closely as possible - and with the capacity for self-checking which is inherent in the structure of the system, it should be possible to do very well.

Approximation

One approximation is employed to facilitate this analysis. That is to associate failures of the fiberoptic communication links and optical receivers and input/output processors in the voters with the module that drives them - the sensor module in the case of the input voters and the computation module in the case of the output voters. The driving module is considered to function only if it and all the communication links, optical receivers and input/output processors it drives also function. This is a conservative assumption in that it underestimates the reliability of the system. Without this assumption, one has to consider all combinations of sensor modules, optical receivers, and voter processors which permit the system to function. This is a very difficult combinatoric task. With the assumption, the sensor modules and associated optical receivers and input/output processors can be treated separately from the voter processors, because under the assumption, if the required number of sensor modules are working, the sensor data is available to the voter processors. It is then an independent question whether the required number of voter processors are working.

With this approximate treatment of both the input voters and output voters, the components are associated for the purpose of the following analysis as shown in Figure 2.

Power Supply System

There are N_p unregulated power supplies tied to the power buss. Any one is capable of supplying the load of powering the flight control system. Failures of these supplies are considered independent which implies isolation such that failure of one cannot induce failures in other supplies or in other system components.

$$\begin{aligned} R_{pss} &= P(\text{At least one power supply works}) \\ &= P(\text{Not all power supplies have failed}) \\ &= 1 - (1 - R_{ps})^{N_p} \end{aligned}$$

where R_{ps} is the reliability of each unregulated power supply.

Sensor System

Even with the approximation stated above, which isolates consideration of the sensor modules from the input voters, the sensor system is somewhat complex to analyze because of the interaction of sensor failures and sensor module common component failures. It is assumed that the input voters vote on the data from the different sensors separately, so it may be possible for the system to function on good gyro data from module 1, good accelerometer data from module 2, etc. Thus the failure of any one sensor does not rule out use of the data from the other

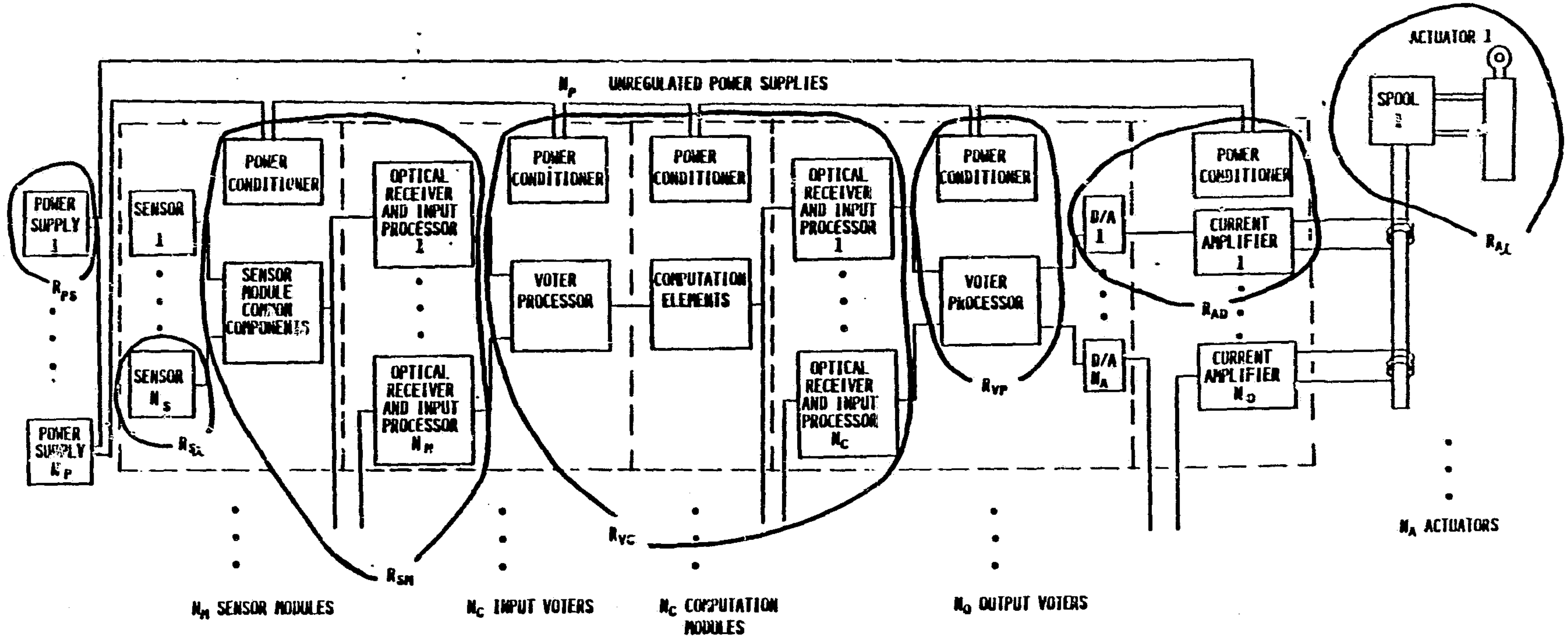

FIGURE 2. UFTCS SYSTEM COMPONENTS AS ASSOCIATED FOR RELIABILITY ANALYSIS.

sensors in that module. However, failure of the sensor module common components denies all of the sensor data from that module.

For economy of terminology, we will use the term "sensor module" in this section to refer to the sensor module common components and, under the stated assumption, all the communication links, optical receivers and input/output processors the module drives. As shown in Figure 2, the reliability of that combination of components is called R_{sm}. The reliability of the sensor system will be evaluated by decomposing on the mutually exclusive set of events that k sensor modules work - for $k = 0, 1, \cdots N_m$.

$$R_{ss} = \sum_{k=1}^{N_m} P(\text{k sensor modules work})P(\text{Correct sensor system data} \mid \text{k sensor modules work})$$

$$P(\text{k sensor modules work}) = \binom{N_m}{k} R_{sm}^{k}(1 - R_{sm})^{N_m-k}$$

where $\binom{N_m}{k}$ is the binomial coefficient.

$$\binom{N_m}{k} = \frac{N_m!}{k!(N_m-k)!}$$

If only 1 sensor module is working, we can derive good sensor data only if all the sensors in that particular module work and the input voters can decide which module is the working one.

P(Correct sensor system data | 1 sensor module works) =

$$= \left[\prod_{i=1}^{N_s} R_{si}\right] \text{ P(Last sensor module failure is covered)}$$

The probability that the last sensor module failure is covered is at least 0.5, which would result from a random choice of the two modules when the failure occurs, and could well be greater than that due to the fact that all the sensor data from the failed module go bad at once when the module fails.

For k greater than 1, the issue of covering module failures does not occur because the midpoint select logic reliably discriminates the failed module from among 3 or more.

P(Correct sensor system data | k sensor modules work) =

= P(Correct gyro data and correct accelerometer data and $\cdots |$ k sensor modules work)

$$= \prod_{i=1}^{N_s} \text{P(Correct sensor i data | k sensor modules work)}$$

P(Correct sensor i data | k sensor modules work) =

= P (Exactly 1 good sensor i in k modules and the last failure was covered, or exactly 2 good sensors i in k modules, or $\cdots$ or exactly k good sensors i in k modules)

Again, the question of failure coverage only arises when we fail from 2 good sensors to 1. Because these events are mutually exclusive,

P(Correct sensor i data | k sensor modules work) =

= P(Exactly 1 good sensor in k modules)P(Last failure was covered) + P(Exactly 2 good sensors in k modules) + $\cdots$ + P(Exactly k good sensors in k modules)

P(Exactly j good sensors i in k modules) = $\binom{k}{j} R_{si}^{j}(1 - R_{si})^{k-j}$

P(Last failure was covered) = P(Last failure was drifting type)xP(Failure was covered | Drifting failure)

+ P(Last failure was hardover type)P(Failure was covered | Hardover failure)

= f_{df}P(Failure was covered | Drifting failure)

+ $(1-f_{df})$P(Failure was covered | Hardover failure)

The expression for last failure coverage decomposes all sensor failures into drifting type and hardover type. In this context, "hardover" should be interpreted to mean "all failures other than drifting failures". The probability of covering these two modes of sensor failure could be different; the probability of covering a hardover failure should be close to 1 and the probability of covering a drifting failure may be only 0.5 which would result from a random choice from the two sensors.

The following identity can be used to simply the expression for the probability of having correct sensor i data given k good sensor modules.

$$\sum_{j=0}^{k} P(\text{Exactly j good sensors in k modules}) = 1$$

Therefore

$$\sum_{j=2}^{k} P(\text{Exactly j good sensors in k modules}) = 1 - P(\text{0 good sensors in k modules}) - P(\text{1 good sensor in k modules})$$

$$\begin{aligned}
&P(\text{Correct sensor i data} \mid \text{k sensor modules work}) = \\
&= P(\text{1 good sensor in k modules})P(\text{Last failure was covered}) \\
&\quad + 1 - P(\text{0 good sensors in k modules}) \\
&\quad - P(\text{1 good sensor in k modules}) \\
&= 1 - (1-R_{si})^k - P(\text{1 good sensor in k modules})[1 - P(\text{Last failure was covered})] \\
&= 1 - (1-R_{si})^k - kR_{si}(1-R_{si})^{k-1}P(\text{Last sensor failure not covered})
\end{aligned}$$

Both the fraction of drifting failures, f_{df}, and the probabilty of last failure coverage can be different for each type of sensor. This last expression for the probability of correct sensor i data with k good sensor modules applies only for k greater than or equal to 2. The expression for k equal to 1 was given earlier.

Input Voters and Computation Modules

We can fail to 2 of these channels without question because midpoint select in the output voters will distinguish 1 failed channel out of 3. Whether 1 failed channel out of 2 can be identified is unclear, but even if a random choice is made of the remaining two channels when one fails, there is probability 0.5 that the working channel will be selected and thus permit operation of the system with just one computational channel.

$$R_{cs} = P(\text{Exactly 1 channel works})P(\text{Last channel failure is covered}) + \sum_{k=2}^{N_c} P(\text{Exactly k channels work})$$

With the same approach used to simplify the expression for the probability of correct sensor i data given k good sensor modules, this can be restated as

$$R_{cs} = 1 - (1-R_{vc})^{N_c} - N_c R_{vc}(1-R_{vc})^{N_c-1} P(\text{Last channel failure was not covered})$$

As indicated in Figure 2, R_{vc} is the reliability of each channel of voter processor, computation module, and associated communication links, optical receivers and input/output processors. N_c is the number of those channels in the system which need not be the same as the number of sensor modules or output voters. The probability that the last channel failure was not covered should be no greater than 0.5.

Output Voters and Actuators

Because of the flux summing operation on the actuators, the output voters, actuator drivers, and actuators must be treated together. The term "actuator driver" is used here to designate the circuitry that connects the output voter processor to the current coil on the actuator servo valve. The principal components of the actuator driver are indicated in Figure 2 to be the D/A converter and the current amplifier. There are N_o output voters and the requirement for system operation will be taken to be the correct application of current to N_f of the N_o coils on each actuator. The number N_f of correct fluxes required on each actuator for proper operation depends on how well the effects of failed channels can be limited.

The reliability of the Voter-Actuator system will be decomposed on the number of working voter processors.

ORIGINAL PAGE IS
OF POOR QUALITY

$$R_{va} = \sum_{k=N_f}^{N_o} P(\text{Exactly k voter processors work})P(\text{Actuator 1 system works and actuator 2 system works and} \cdots \text{and actuator } N_a \text{ system works} \mid \text{k voter processors work})$$

$$= \sum_{k=N_f}^{N_o} \left[P(\text{Exactly k voter processors work}) \prod_{i=1}^{N_a} P(\text{Actuator i system works} \mid \text{k voter processors work}) \right]$$

$$P(\text{Exactly k voter processors work}) = \binom{N_o}{k} R_{vp}^{k}(1-R_{vp})^{N_o-k}$$

$$P(\text{Actuator i system works} \mid \text{k voter processors work}) =$$

$$= P(\text{Actuator i works})P(\text{At least } N_f \text{ fluxes on actuator i are correct} \mid \text{k voter processors work})$$

$$P(\text{Actuator i works}) = R_{ai}$$

$$P(\text{At least } N_f \text{ fluxes on actuator i are correct} \mid \text{k voter processors work}) = \sum_{j=N_f}^{k} P(\text{Exactly j actuator drivers from k voters work})$$

$$= \sum_{j=N_f}^{k} \binom{k}{j} R_{ad_i}^{\,j}(1-R_{ad_i})^{k-j}$$

Summary

The predicted reliability of the Ultra-reliable Fault Tolerant Control System with an arbitrary number of components is computed by the following series of calculations:

Component or module reliability:

For the given mission time, compute all component or module reliabilities as

$$R_i = \exp(-\lambda_i t_m)$$

Power supply system reliability:

$$R_{pss} = 1 - (1-R_{ps})^{N_p}$$

Sensor system reliability:

P(Last sensor failure was not covered) =

$$= 1 - f_{df} P(\text{Failure was covered} \mid \text{Drifting failure}) - (1-f_{df}) P(\text{Failure was covered} \mid \text{Hardover failure})$$

P(Correct sensor i data | k sensor modules work) =

$$= 1 - (1-R_{si})^k - kR_{si}(1-R_{si})^{k-1} P(\text{Last sensor failure was not covered}) \quad (k \geq 2)$$

$$R_{ss} = N_m R_{sm}(1-R_{sm})^{N_m-1} \left[\prod_{i=1}^{N_s} R_{si}\right] P(\text{Last sensor module failure is covered}) + \sum_{k=2}^{N_m} \left[\binom{N_m}{k} R_{sm}^k (1-R_{sm})^{N_m-k} \prod_{i=1}^{N_s} P(\text{Correct sensor i data} \mid \text{k sensor modules work})\right]$$

Input voter and computation system reliability:

$$R_{cs} = 1 - (1-R_{vc})^{N_c} - N_c R_{vc}(1-R_{vc})^{N_c - 1} P(\text{Last channel failure was not covered})$$

Output voter and actuator system reliability:

$$R_{va} = \sum_{k=N_f}^{N_o} \left\{ \binom{N_o}{k} R_{vp}^{k}(1-R_{vp})^{N_o - k} \left[\prod_{i=1}^{N_a} R_{ai} \left(\sum_{j=N_f}^{k} \binom{k}{j} R_{ad_i}^{j}(1-R_{ad_i})^{k-j} \right) \right] \right\}$$

UFTCS reliability:

$$R_{system} = R_{pss} R_{ss} R_{cs} R_{va}$$

The probabilities of detecting the last failure can be manipulated to determine the system reliabilities for the "failing to two" and "failing to one" cases. For the "failing to one" case, the probability of covering the last sensor module failure and the probability of covering the last input voter and computation system failures should be set to one. Likewise, the probability of covering the sensor failures should be set to some reasonable value (e.g. 0.5 for drifting failures and 1.0 for hard failures). For the "failing to two" case, the probability of covering the last failure should be set to 0.0 for all modules and sensors.

COMPONENT FAILURE RATES

Sensor Failure Rates

Obtaining failure rates for the sensors was one of the more difficult tasks of the analysis for several reasons. First, the sensor manufacturers were somewhat reluctant to provide information for the purposes of any analysis; they have been "blamed" for poor system performance in the past, and are therefore reluctant to participate in this manner. Second, several airframe manufacturers were contacted, but they buy combination sensor-computer subsystems (e.g., air data computers, and inertial reference systems), and they were not able to provide reliability figures for the specific sensors used in this analysis.

To circumvent these difficulties, we have evaluated the UFTCS with a "best guess" reliability estimate for each generic sensor and have supplemented these calculations with a sensitivity analysis for the sensors in the helicopter mission. These sensitivity analyses can be used to determine the sensor reliability requirements to achieve desired overall system reliability.

This analysis assumes that reliability is more important than cost and that mass-produced sensors are not used. Therefore, the reliability data used in this analysis is taken from the most reliable components found in the survey.

Converting Reliabilities Between Environments. In some instances the reliability estimates were obtained for the same sensor, but in different environments. These reliabilities were multiplied by scale factors, not only to convert the reliabilities to one environment for choosing the "best guess" reliability, but also to convert the reliabilities to the three environments of the analysis (helicopter, air transport, and space flight). The scale factors are based on the environmental parameters found in MIL-HDBK-217D [6], and are shown in Table 1.

Table 1

Scale Factors for Converting Failure Rates Between Environments

To convert from this environment	Multiply the failure rate by the indicated scale factor		
	Helicopter	Air Transport	Space Flight
Helicopter	1.0	0.2	0.04
Air Trnspt	5.0	1.0	0.2
Space Flight	25.0	5.0	1.0

Accelerometer Reliabilities. Four Mean Time Between Failures (MTBF) were obtained for accelerometers. When converted to the air transport environment they were 50,000, 30,000, 20,000, and 6,000 hours. Based on these estimates, a failure rate of 20 failures per million hours (air transport environment) was chosen for the generic accelerometer.

Gyro Reliabilities. Three MTBFs for gyros were obtained, and when converted to the air transport environment, they were 70,000, 60,000, and 11,000 hours. A failure rate of 15 failures per million hours (air transport environment) was chosen for the generic gyro.

Long Term Heading Reference. Only one MTBF for a flux gate compass, 50,000 hours for the air transport environment, was obtained. A failure rate of 20 failures per million hours (air transport environment) was chosen for the generic flux gate compass.

<u>Barometric Altimeter Reliability.</u> Four MTBFs for a barometric altimeter, 25,000, 10,000, and two at 7,000 hours for the air transport environment, were obtained. A failure rate of 40 failures per million hours (air transport environment) was chosen for the generic altimeter.

<u>Optical Position Sensors.</u> Attempts to obtain reliability estimates for optical position sensors were unsuccessful. Thus a generic sensor was conceived and consists of 10 photo transistors in a linear array. Based on this assumption and the failure rates of phototransistors in [6], the failure rate of the optical sensor is found to be 20 failures per million hours.

Table 2 summarizes the sensor failure rates used in the UFTCS reliability analyses.

Table 2

Sensor Failure Rates Used in UFTCS Analyses
(failures per million hours)

Sensor	Environment		
	Helicopter	Air Transport	Space Flight
Accel.	100	20	--
Gyro	75	15	3
Long Term Hdg Ref	100	20	--
Baro Alt	200	40	--
Opt. Pos.	--	--	20

Other Failure Rates

Failure rates for the computational elements and voter elements were computed from the circuit design of these elements as adapted from drawings supplied by NASA. These calcualations were performed according to the procedures outlined in MIL-HDBK-217D [6], and are detailed in the Appendix.

The ship's power supplies and the actuators are not considered as part of this analysis, and so it is assumed that they have zero failure rates. The analysis has been formulated so that their reliabilities can be incorporated at a later date.

RESULTS

Assumptions and Constants

Certain assumptions have been made, and certain parameters are held constant for all of the calculations unless explicitly stated otherwise.

o The baseline sensor failure rates are those shown in Table 2.

o There are four output voters and actuator drivers (flux windings) for each actuator. Valid signals are required on at least two windings for proper operation.

o The probability of "failing to two" means that there are at least two operating computation modules and there are at least two operating sensors for each measurement; each of these sensors feeds into an operating sensor module. The probability of "failing to one" means that there is at least one of each of these items in operation.

o When "failing to one", the probabilities of covering the last sensor module failure and the last voter/computation module failure is 1.0. The probability of covering the last sensor failure is 0.9 for all sensors. This result from assuming that 20% of the sensor failures are drifting failures; the probability of covering the last drifting failure is 0.5; and the probability of covering a hardover sensor failure is 1.0.

Mission Reliability Estimates

The primary objective of this report is to supply reliability estimates of UFTCS operation at various times in the helicopter, air transport, and space flight missions. Initial system configurations are 4, 5, and 6 redundant paths (with four output voters and flux windings), and failures are allowed to 1 or 2 operating paths.

The reliability estimates are shown in Table 3 assuming perfect sensors (all sensor failure rates equal zero), and Table 4 assuming the baseline sensors. The results with the perfect sensors are indicitive of the inherent reliability of the UFTCS itself, whereas the other table shows the reliability of the combination of sensors and control system. Note that there is a "floor" to the probabilities of failure which, as will be shown later, are due to the assumption of 4 flux windings on each actuator.

Sensitivity Analyses

This section describes the results of sensitivity analyses

Table 3

Predicted probabilities of failure for UFTCS
with perfect sensors

Helicopter environment (35C)

Fail to/ start with	Operating time (hours, no maintenance) 1	10	20
1/4	0.71E-13	0.73E-10	0.61E-09
2/4	0.10E-10	0.10E-07	0.80E-07
1/5	0.70E-13	0.70E-10	0.56E-09
2/5	0.72E-13	0.86E-10	0.81E-09
1/6	0.70E-13	0.70E-10	0.56E-09
2/6	0.70E-13	0.70E-10	0.56E-09

Air transport environment (25C)

Fail to/ start with	Operating time (hours, no maintenance) 1	10	20
1/4	0.20E-13	0.22E-10	0.19E-09
2/4	0.70E-11	0.69E-08	0.55E-07
1/5	0.20E-13	0.20E-10	0.16E-09
2/5	0.21E-13	0.29E-10	0.31E-09
1/6	0.20E-13	0.20E-10	0.16E-09
2/6	0.20E-13	0.20E-10	0.16E-09

Space craft environment (25C)

Fail to/ start with	Operating time (hours, no maintenance) 336	2190	4380
1/4	0.64E-07	0.73E-04	0.94E-03
2/4	0.13E-04	0.30E-02	0.20E-01
1/5	0.21E-07	0.11E-04	0.20E-03
2/5	0.24E-06	0.33E-03	0.41E-02
1/6	0.20E-07	0.61E-05	0.69E-04
2/6	0.24E-07	0.40E-04	0.86E-03

Table 4

Predicted probabilities of failure for UFTCS with baseline sensors

Helicopter environment (35C)

Fail to/ start with	Operating time (hours, no maintenance) 1	10	20
1/4	0.14E-10	0.14E-07	0.12E-06
2/4	0.15E-09	0.15E-06	0.12E-05
1/5	0.75E-13	0.11E-09	0.13E-08
2/5	0.12E-12	0.52E-09	0.77E-08
1/6	0.70E-13	0.70E-10	0.57E-09
2/6	0.70E-13	0.72E-10	0.61E-09

Air transport environment (25C)

Fail to/ start with	Operating time (hours, no maintenance) 1	10	20
1/4	0.77E-12	0.77E-09	0.62E-08
2/4	0.14E-10	0.14E-07	0.12E-06
1/5	0.20E-13	0.21E-10	0.18E-09
2/5	0.22E-13	0.41E-10	0.49E-09
1/6	0.20E-13	0.20E-10	0.16E-09
2/6	0.20E-13	0.20E-10	0.16E-09

Space craft environment (25C)

Fail to/ start with	Operating time (hours, no maintenance) 336	2190	4380
1/4	0.28E-05	0.82E-03	0.67E-02
2/4	0.39E-04	0.88E-02	0.55E-01
1/5	0.83E-07	0.11E-03	0.16E-02
2/5	0.84E-06	0.12E-02	0.14E-01
1/6	0.22E-07	0.20E-04	0.44E-03
2/6	0.38E-07	0.16E-03	0.35E-02

to explore some of the parameters of interest in the UFTCS. The 10 hour point in the helicopter mission was chosen for examination because of the greater liklihood that UFTCS will be applied to helicopters in the immediate future.

Coverage of Sensor Failures. When failing from two to one sensors, there is a chance that the failure will not properly be isolated, especially if it is a drifting failure. The parameter affecting system reliability is the probability of detecting this last sensor failure which is in the range of [0.5, 1.0]. Figure 3 shows the sensitivity of system reliability to this parameter when the initial configuration has 4 and 6 channels. Also shown for comparison purposes are the (constant) curves for failing to two for 4 and 6 channels. It can be seen that 4 channels failing to 1 is sensitive to this sensor coverage, and that the probability of system failure increases by a factor of 10 as the probability of sensor coverage drops from 1.0 to 0.9, the nominal value. However, the sensitivity to this coverage is less for the other configurations because of the floor effect of the number of flux windings.

Barometric Altimeter Reliability. The reliability of the barometric altimeter is of interest because it is the least reliable of all sensors. Figure 4 shows the effect of this failure rate on overall system reliability. It can be seen that there are two floor effects here. For the 6 channel case, the floor is .7E-10 which is determined by the number of flux windings. The two floors for the 4 channel case are determined by the reliability of the other sensors in each sensor module. These floors are reached when the barometric altimeter failure rate is near those of the other sensors at approximately 100 failures per million hours (FPM).

Gyro Reliability. The effect of the reliability of the

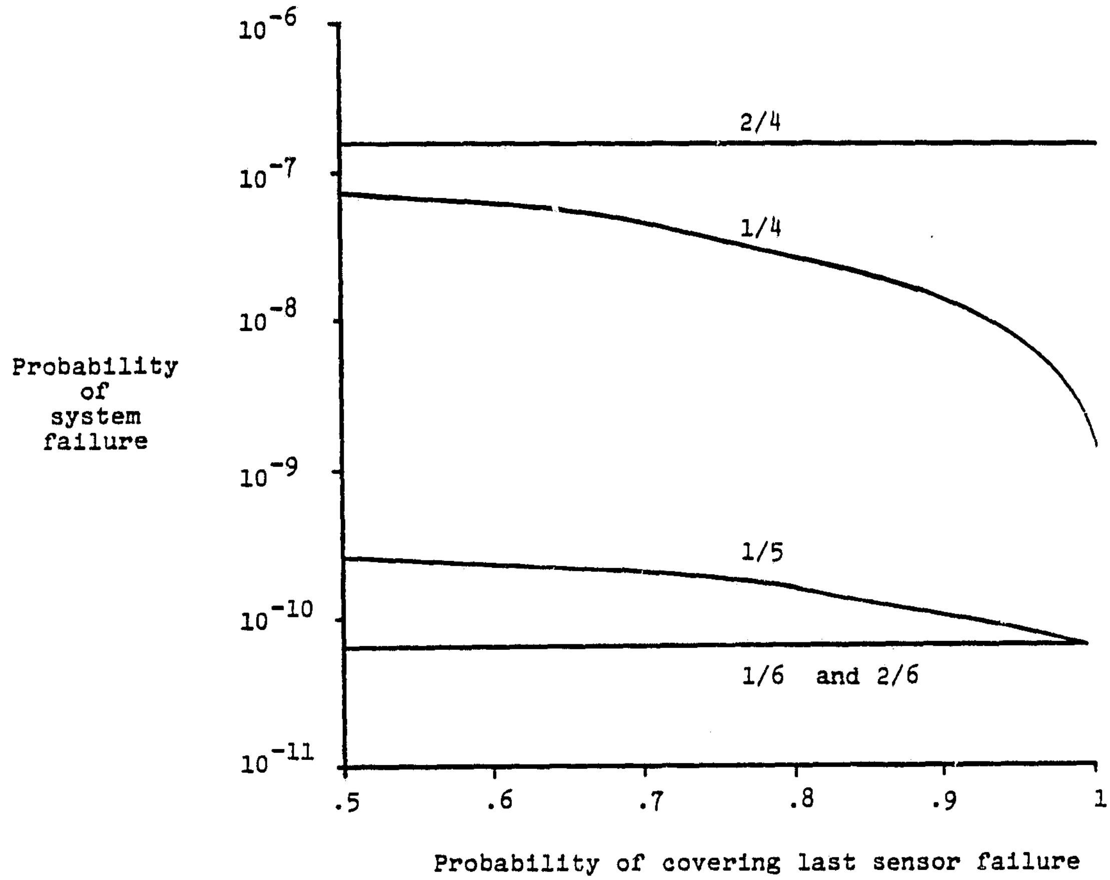

Figure 3. Probability of system failure as a function of the probability of covering the last sensor failure (baseline sensors).

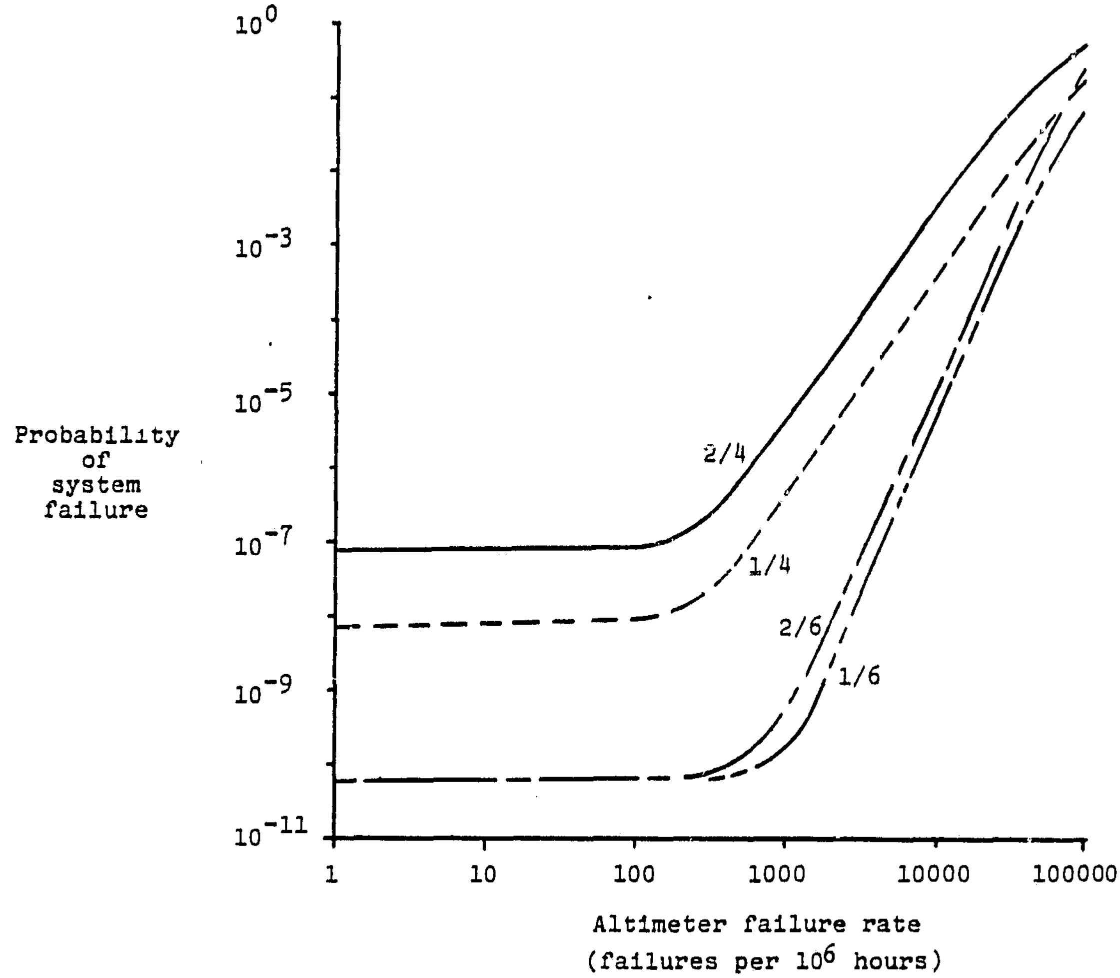

Figure 4. Probability of system failure versus barometric altimeter failure rate (baseline sensors).

gyros is examined because three of the 6 sensors in each module are gyros, thus possibly magnifying the effect of increases in gyro failure rates. Figure 5 shows the effect of gyro failure rate with the same general pattern as for the barometric altimeter.

<u>Number of Flux Windings</u>. It is not necessary within the UFTCS architecture to have 4 flux windings driven by 4 output voters. However, it should be assumed that at least half of the flux windings must operate properly to have an operational system because of the flux summing operation. Figures 6 and 7 show the effects on system reliability of 2 to 10 flux windings for each actuator. Figure 6 is for the special case of perfect sensors to see the effects of the UFTCS hardware alone; Figure 7 shows the effects of the number of flux windings on the reliability of the sensor control system combined. The most striking results are the removal of the "floor" at .7E-10 when the number of windings is 6 or more, verifying the limitation on system failure rate seen in previous results. (Figure 6 also shows that a large number of windings can penalize system reliability, although the penalty is slight.) It can be seen in Figure 6 that the floor can become very low for perfect sensors, but Figure 7 indicates that with the nominal sensors there is little value in increasing the number of windings beyond 6 when there are 6 sensor and computational modules.

<u>Sensor Modules vs. Computational Modules</u>. Although it is convenient to think of the UFTCS as having N channels, there is no requirement that the number of sensor modules must equal the number of computational modules or number of flux windings. The cross-strapping of information to the input voters and output voters removes the need for this constraint. In fact, it seems logical that there should be a large number of unreliable parts of the system and a small number of the reliable parts of the

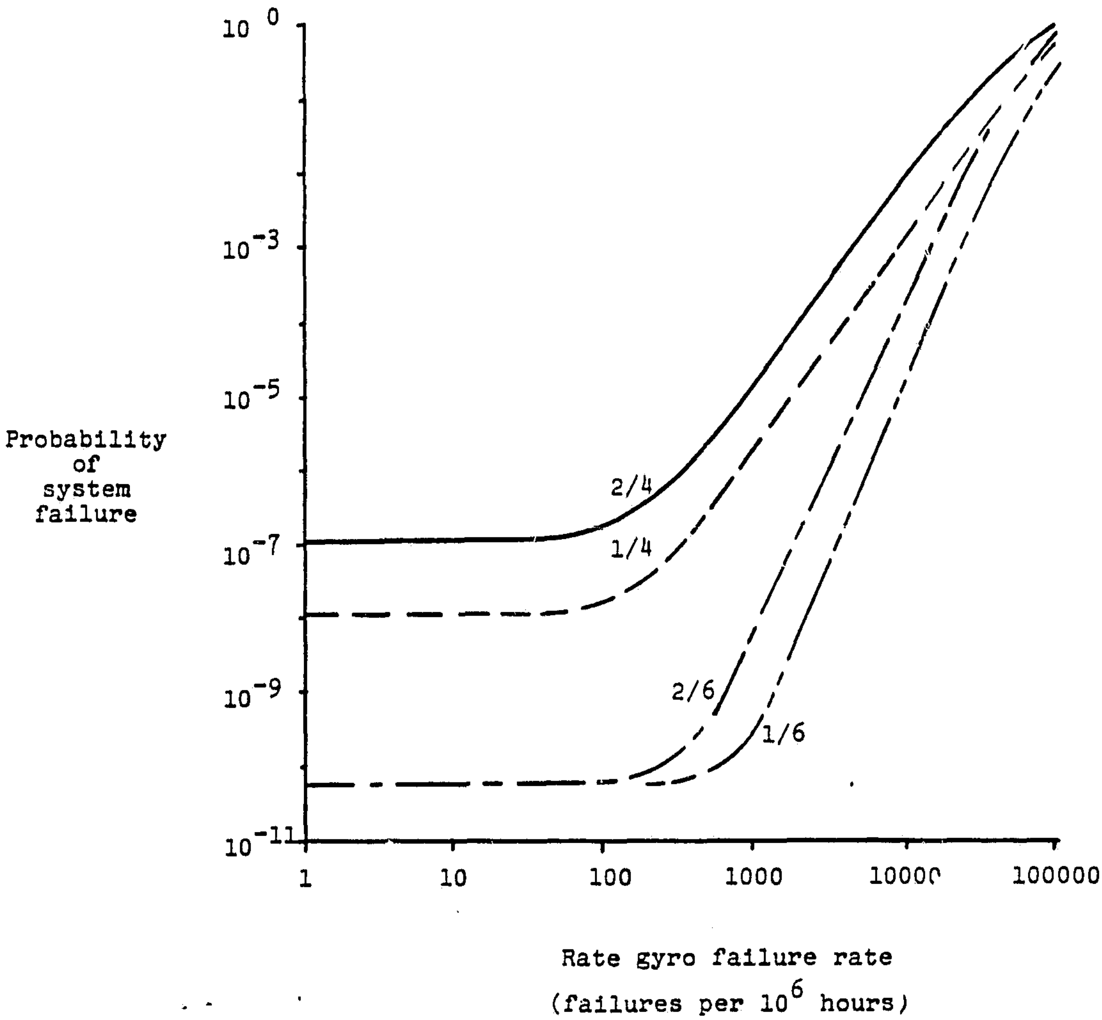

Figure 5. Probability of system failure versus rate gyro failure rate (baseline sensors).

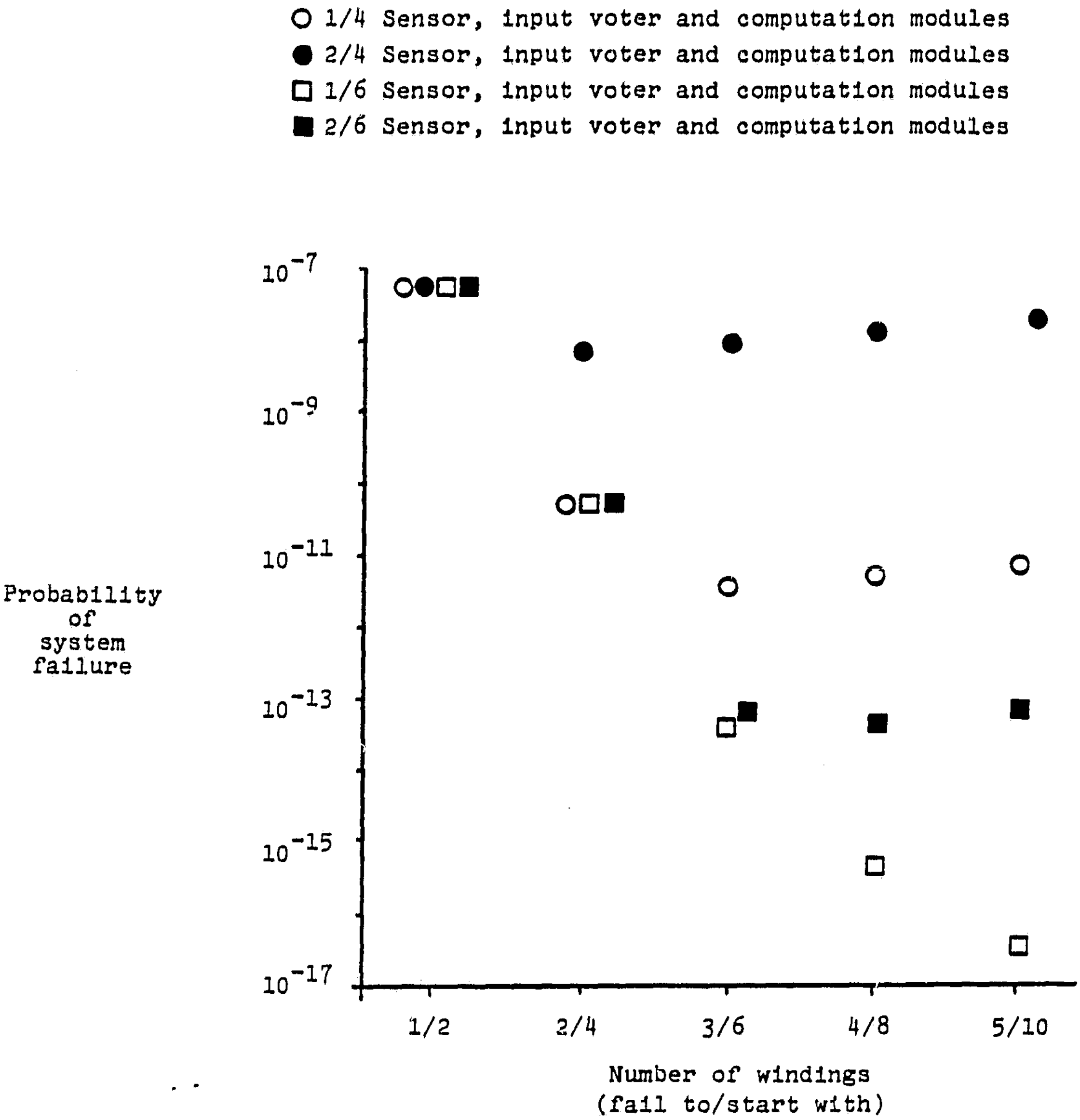

Figure 6. Probability of system failure versus number of flux summer windings requiring half of the windings for proper operation (perfect sensors).

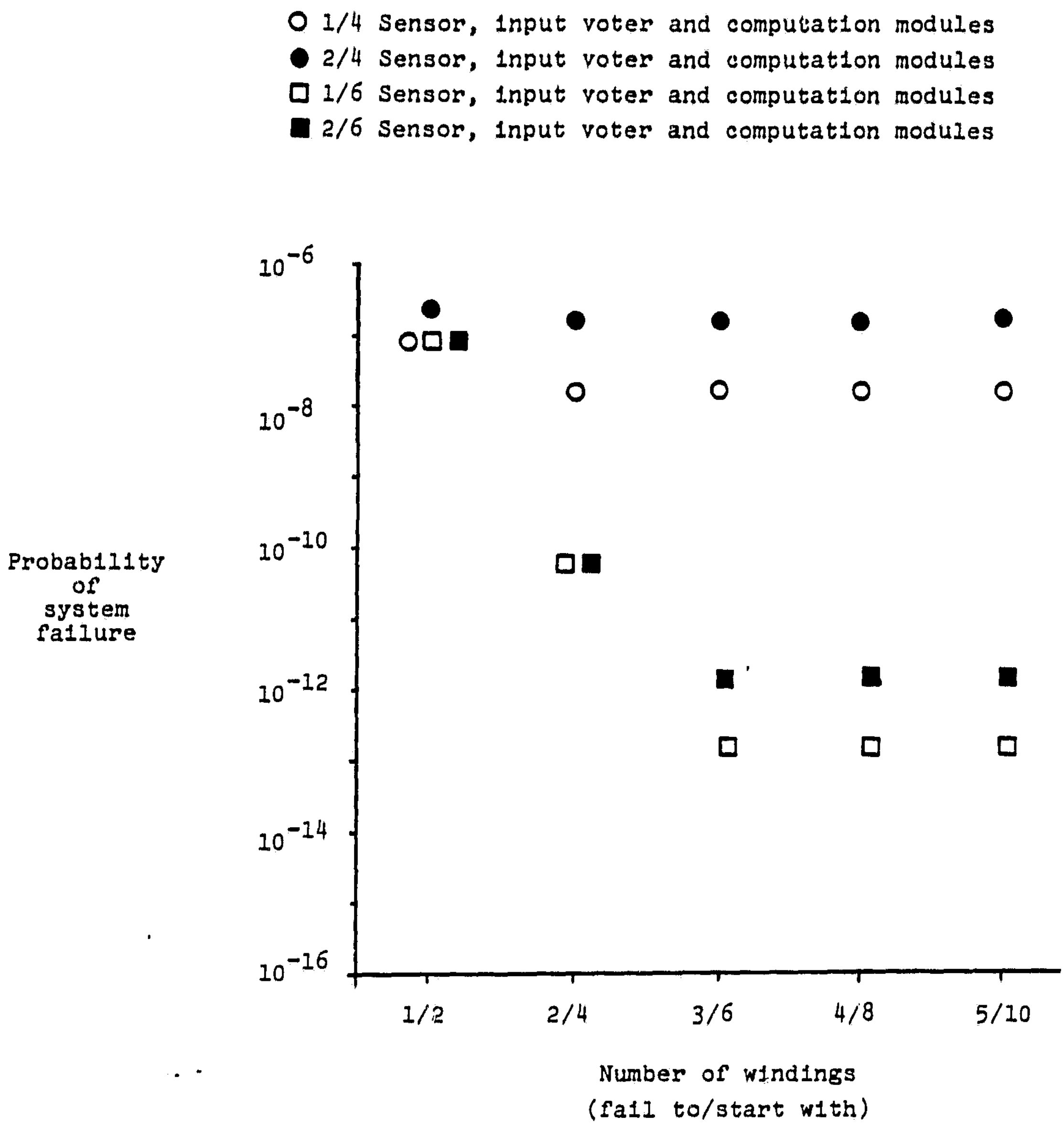

Figure 7. Probability of system failure versus number of flux summer windings requiring half of the windings for proper operation (baseline sensors).

system. Tables 5 and 6 show the system reliability as a function of the number of sensor modules, computation modules, and flux windings, failing to two and one. Table 5 assumes perfect sensors, in order to examine the effects of differing amounts of UFTCS hardware, and Table 6 assumes the baseline sensors, in order to examine the tradeoffs to obtain a reliable sensor/control system combination.

Tables 5 and 6 may be used to choose a system configuration to meet a desired system reliability goal at the 10 hour point of the helicopter mission. For example, Table 7 shows the system configurations that will meet a goal of system failure less than 1E-10 assuming both perfect and baseline sensors.

Even though a configuration with baseline sensors and "failing to one" requires six sensor modules, we feel that a configuration with only five sensor modules would be adequate because of the conservative nature of the approximation made in the analysis. The approximation requires that all input processors driven by a sensor module be operational for that sensor module to work properly, and the input processor is among the most unreliable components in the system (see component C8751 in Table A4 in the Appendix). A configuation consisting of four flux windings, four computation modules, and five sensor modules with baseline sensors results in a failure rate only slightly higher than 1E-10.

Table 5

Probability of system failure versus configuration (perfect sensors)

[Upper entry is failing to one; lower entry is failing to two]

Number of sensor modules	Number of input voter/computation modules 2	4	5	6	8
Four output voters and flux windings					
2	0.19E-05 0.35E-02	0.36E-06 0.12E-02	0.46E-06 0.14E-02	0.57E-06 0.15E-02	0.83E-06 0.18E-02
4	0.17E-05 0.26E-02	0.73E-10 0.10E-07	0.70E-10 0.13E-08	0.71E-10 0.18E-08	0.71E-10 0.31E-08
5	0.17E-05 0.26E-02	0.73E-10 0.91E-08	0.70E-10 0.86E-10	0.70E-10 0.72E-10	0.70E-10 0.74E-10
6	0.17E-05 0.26E-02	0.73E-10 0.91E-08	0.70E-10 0.85E-10	0.70E-10 0.70E-10	0.70E-10 0.70E-10
8	0.17E-05 0.26E-02	0.73E-10 0.91E-08	0.70E-10 0.85E-10	0.70E-10 0.70E-10	0.70E-10 0.70E-10
Six output voters and flux windings					
2	0.24E-05 0.38E-02	0.36E-06 0.12E-02	0.46E-06 0.14E-02	0.57E-06 0.15E-02	0.83E-06 0.18E-02
4	0.22E-05 0.29E-02	0.48E-11 0.13E-07	0.28E-12 0.13E-08	0.38E-12 0.17E-08	0.74E-12 0.30E-08
5	0.22E-05 0.29E-02	0.47E-11 0.13E-07	0.61E-13 0.24E-10	0.54E-13 0.17E-11	0.54E-13 0.35E-11
6	0.22E-05 0.29E-02	0.47E-11 0.13E-07	0.61E-13 0.23E-10	0.54E-13 0.96E-13	0.54E-13 0.58E-13
8	0.22E-05 0.29E-02	0.47E-11 0.13E-07	0.61E-13 0.23E-10	0.54E-13 0.95E-13	0.54E-13 0.54E-13

Table 6

Probability of system failure versus configuration (baseline sensors)

[Upper entry is failing to one; lower entry is failing to two]

Number of sensor modules	Number of input voter/computation modules: 2	4	5	6	8
Four output voters and flux windings					
2	0.15E-02 0.18E-01	0.15E-02 0.16E-01	0.15E-02 0.16E-01	0.15E-02 0.16E-01	0.15E-02 0.16E-01
4	0.17E-05 0.26E-02	0.14E-07 0.15E-06	0.16E-07 0.16E-06	0.18E-07 0.18E-06	0.22E-07 0.22E-06
5	0.17E-05 0.26E-02	0.11E-09 0.95E-08	0.11E-09 0.52E-09	0.12E-09 0.57E-09	0.13E-09 0.72E-09
6	0.17E-05 0.26E-02	0.73E-10 0.91E-08	0.70E-10 0.86E-10	0.70E-10 0.72E-10	0.70E-10 0.72E-10
8	0.17E-05 0.26E-02	0.73E-10 0.91E-08	0.70E-10 0.85E-10	0.70E-10 0.70E-10	0.70E-10 0.70E-10
Six output voters and flux windings					
2	0.15E-02 0.18E-01	0.15E-02 0.16E-01	0.15E-02 0.16E-01	0.15E-02 0.16E-01	0.15E-02 0.16E-01
4	0.22E-05 0.29E-02	0.14E-07 0.16E-06	0.16E-07 0.16E-06	0.18E-07 0.18E-06	0.22E-07 0.22E-06
5	0.22E-05 0.29E-02	0.42E-10 0.13E-07	0.43E-10 0.46E-09	0.50E-10 0.50E-09	0.65E-10 0.65E-09
6	0.22E-05 0.29E-02	0.48E-11 0.13E-07	0.18E-12 0.24E-10	0.19E-12 0.15E-11	0.24E-12 0.20E-11
8	0.22E-05 0.29E-02	0.47E-11 0.13E-07	0.61E-13 0.23E-10	0.54E-13 0.95E-13	0.54E-13 0.54E-13

	Perfect Sensors	Baseline Sensors
Failing to 1	4 flux windings 4 computation modules 4 sensor modules	4 flux windings 4 computation modules 6 sensor modules
Failing to 2	4 flux windings 5 computation modules 5 sensor modules	4 flux windings 5 computation modules 6 sensor modules

Table 7. System Configurations with probability of failure less than 1E-10

CONCLUSIONS

The reliability calculations for the baseline system clearly indicate that the 4 flux windings limit overall probability of system failure to no less than .7E-10 at the 10 hour point in the helicopter mission. The sensitivity analyses were also influenced by this limit. Tables for probability of failure at the 10 hour point in the helicopter mission are provided as a function of the number of computation modules, sensor modules, and flux windings; these tables allow the designer to choose a configuration which will meet a specified probability of failure at this point of the helicopter mission.

APPENDIX

Component and Module Reliability Calculations

The component reliability values were determined using references 5 and 6. Tables A1 through A3 list the component-specific data and assumptions used in the calculation. In addition, the following characteristics were assumed for all microelectronics:

1. Hermetically sealed,

2. Dual in-line packaging,

3. Eutectic die attach,

4. Glass seal,

5. MIL-M-38510, Class B, and

6. Learning factor = 1.

Ambient temperatures for the calculations were 25° C for the space craft and air transport environments and 35° C for the helicopter environment. Case temperatures were taken from reference 6, table 5.1.2.5-4, note 2 (space flight, 40° C; helicopter and air transport, 60° C).

Table A1

DATA USED TO DETERMINE COMPONENT FAILURE RATES - COMPONENTS NOT LISTED IN MIL-M-38510

Part No.	Description	Technology	Power Disipation(W)	Number of Pins	Circuit Complexity
C8751H-11	8 bit microprocessor with 128 X 8 RAM, 4K X 8 EPROM	NMOS	2.0	40	1K bits RAM 32K bits ROM 9K gates(1)
D8086	16 bit microprocessor	NMOS	2.5	40	10K gates(1)
C8087-3	Numeric co-processor	NMOS	3.0	40	25K gates(1)
D2764	8K X 8 EPROM	NMOS	0.5(2)	28	64K bits
HM6116P-3	2K X 8 RAM	CMOS	1.0	24	16K bits
MD8282/B	Octal latch	TTL	1.0	20	58 gates(3)
MD8284A/B	Clock generator and driver	TTL	1.0	18	63 gates(3)
MD8286/B	Octal bus transceiver	TTL	1.0	20	18 gates(3)
MD8288/B	Bus controller	TTL	1.5	20	230 gates(1)
HD1-6402A-9	8 Bit UART	CMOS	0.01	40	296 gates

Notes:
1. Approximated from transistor count and transistor to gate ratio of 3 (Ref. 6)
2. Approximated from 100mA active current at 5V (Ref. 5)
3. Approximated from circuit diagram (Ref. 5 and 6)

Table A2

CROSS REFERENCE OF COMPONENTS LISTED IN MIL-M-38510

Part No.	M38510/	Description
SNJ54LS02J	30301C	Quad 2 input positive NOR gates
SNJ54LS04J	30003C	Hex inverters
SNJ54LS10J	30005C	Triple 3 input positive NAND gates
SNJ54LS74AJ	30102C	Dual D-type flip flops
SNJ54LS125AJ	32301C	Quad bus buffer gates
SNJ54LS138J	30701E	3 to 8 line decoder
SNJ54LS139J	30702E	Dual 2 to 4 line decoders
SNJ54LS367AJ	32203E	Hex bus drivers
SNJ54LS368AJ	32204E	Hex bus drivers
SNJ55113J	10405E	Line driver
SNJ55115J	10404E	Line receiver
MC7805	10706Y	5V Voltage Regulator
MC7824	10709Y	24V Voltage Regulator
DAC08A	11302E	8 bit Digital to Analog Convertor
LM118	10107C	Operational Amplifier

Table A3

ASSUMPTIONS FOR DISCRETE COMPONENT RELIABILITY CALCULATIONS

Component	MIL-HDBK -217D	Assumptions
Resistors	5.1.6.1	Composition resistors MIL-R-39008 Level M Less than 100K ohms Ratio of operating to rated wattage = 0.5
Trimmer Resistors	5.1.6.7	Non wire wound resistors MIL-R-39035 Level M 10 to 50K ohms Ratio of operating to rated wattage = 0.5 Ratio of applied to rated voltage = 0.8 to 0.1
Capacitors	5.1.7.4	Ceramic capacitors MIL-C-39014 Level M Rated at 125° C Ratio of operating to rated voltage = 0.5
Zener Diodes	5.1.3.5	MIL-STD-19500 JAN Quality Level Max permissible junction Temperature = 175° to 200° C Max case temperature (100% rated load and max junction temperature not exceeded) = 25° C Ratio of (Power dissipated to max rated power) or (operating zener current to max rated zener current) = 0.5
Diodes	5.1.3.4	MIL-S-19500 JAN Quality Level Metallurgically bonded Current rating ≤ 1 amp Ratio of applied to rated reverse voltage ≤ 0.6 Max permissible junction temperature = 175° to 200° C

Table A3 (concluded)

Diodes (continued)		Ratio of operating forward current to maximum rated forward current = 0.5 Max case temperature (100% rated load and max junction temperature not exceeded = 25° C Power recifier application
Photodiodes	5.1.3.10	JAN Quality Level
Photodiode Detectors	5.1.3.10	JAN Quality Level
Quartz Crystals	5.1.15	MIL-C-3098
Relays	5.1.10	MIL SPEC Quality Level M Temperature rating = 125° C Ratio of operating load current to rated resistive load current = 0.5 Cycles per hour < 1 High speed application Dry reed construction SPST action
Fiber Optic Cables	5.1.15	Length < 1 Km Single fiber type
Fiber Optic Connectors	5.1.15	
Electrical Connectors	5.1.12	MIL SPEC Quality Type B insert material Number of active contacts = 3 5 to 50 mating/unmating cycles per 1000 hours
Printed Wiring Boards	5.1.13	MIL-P-55110 One two-sided board per module 500 plated through holes per module
Solder Connections	5.1.14	Reflow lap solder 500 solder connections per module

To implement the optical link between modules, the line driver/receiver indicated on NASA drawings A14-82-235-101 and -102 (part number 75118) was replaced. Each line driver was replaced by a SNJ55113 line driver and a photo diode, and each line receiver was replaced by a SNJ55115 line receiver, and a photo diode detector. The basis for this substitution was that reference 6 contained failure rate data for these devices, and no data related to currently available optical drivers/receivers could be obtained. However, these devices contain the basic hardware to implement the optical drivers/receivers, and the data should be reasonably accurate.

The design of the sensor voter module as described in NASA drawing A14-82-235-102 was modified slightly for the output voter module. To provide an analog output, the output driver for each actuator was replaced by an 8 bit digital-to-analog converter (DAC-08A), control logic (SNJ54LS02 quad NOR gates), and a differential driver as shown in figure A1.

The failure rate for the flux summer module was calculated based on the design as shown in figure A2. The module failure rates do not include the electrical/mechanical interface (in figure A2, the LVDT).

The analog circuits on both the actuator voter and flux summer modules require other than a +5V power supply. The design assumed for the power supplies is shown in figure A3.

The 8 bit microprocessor chip on all modules (C8751H-11) consists of a microprocessor and on-chip RAM (128 X 8) and ROM (4K X 8). The composite failure rate for the chip was calculated by determining the failure rates for each sub-component (processor, RAM, and ROM) and summing the three results.

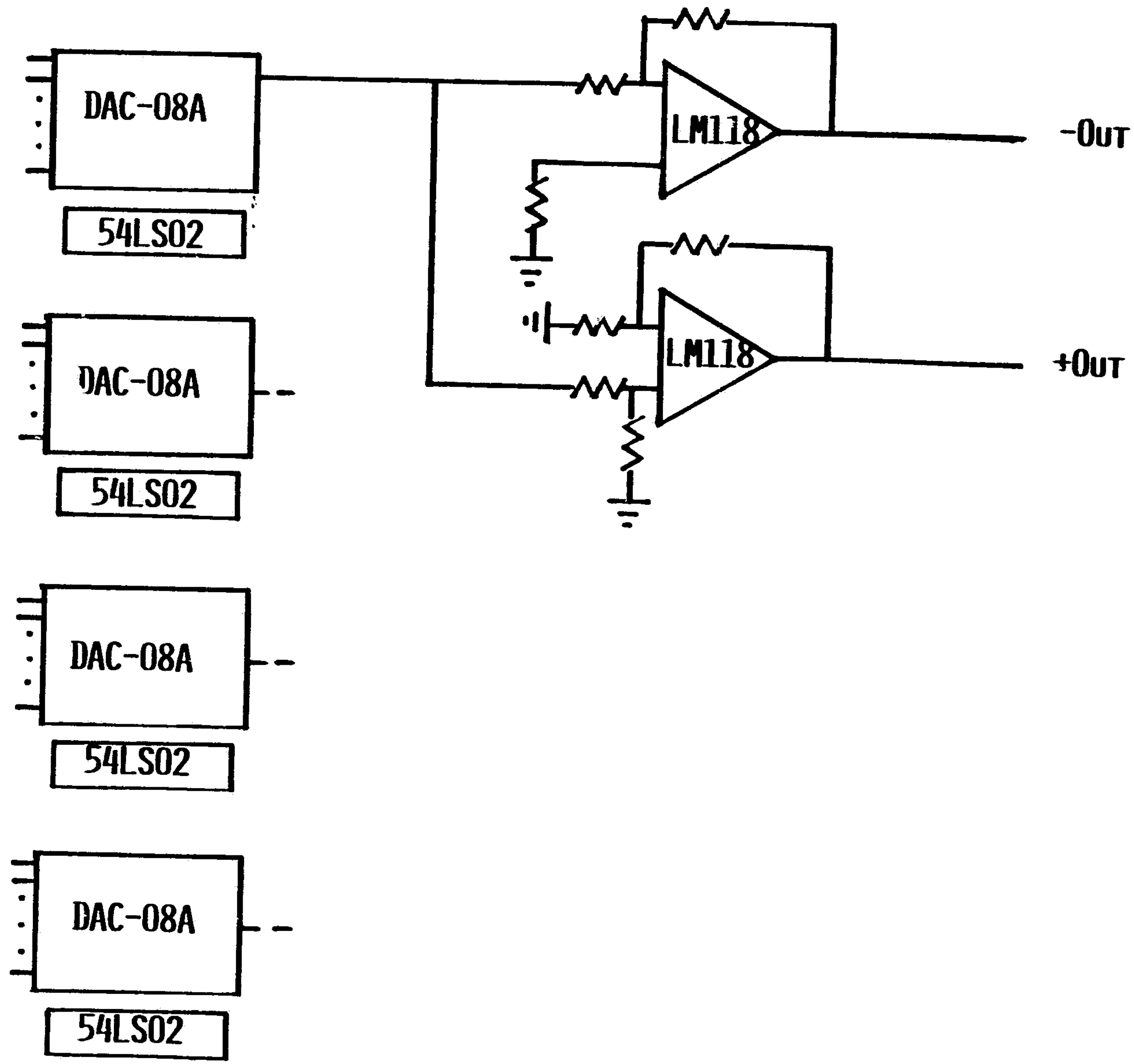

FIGURE A1. ACTUATOR VOTER DIFFERENTIAL OUTPUT STAGE.

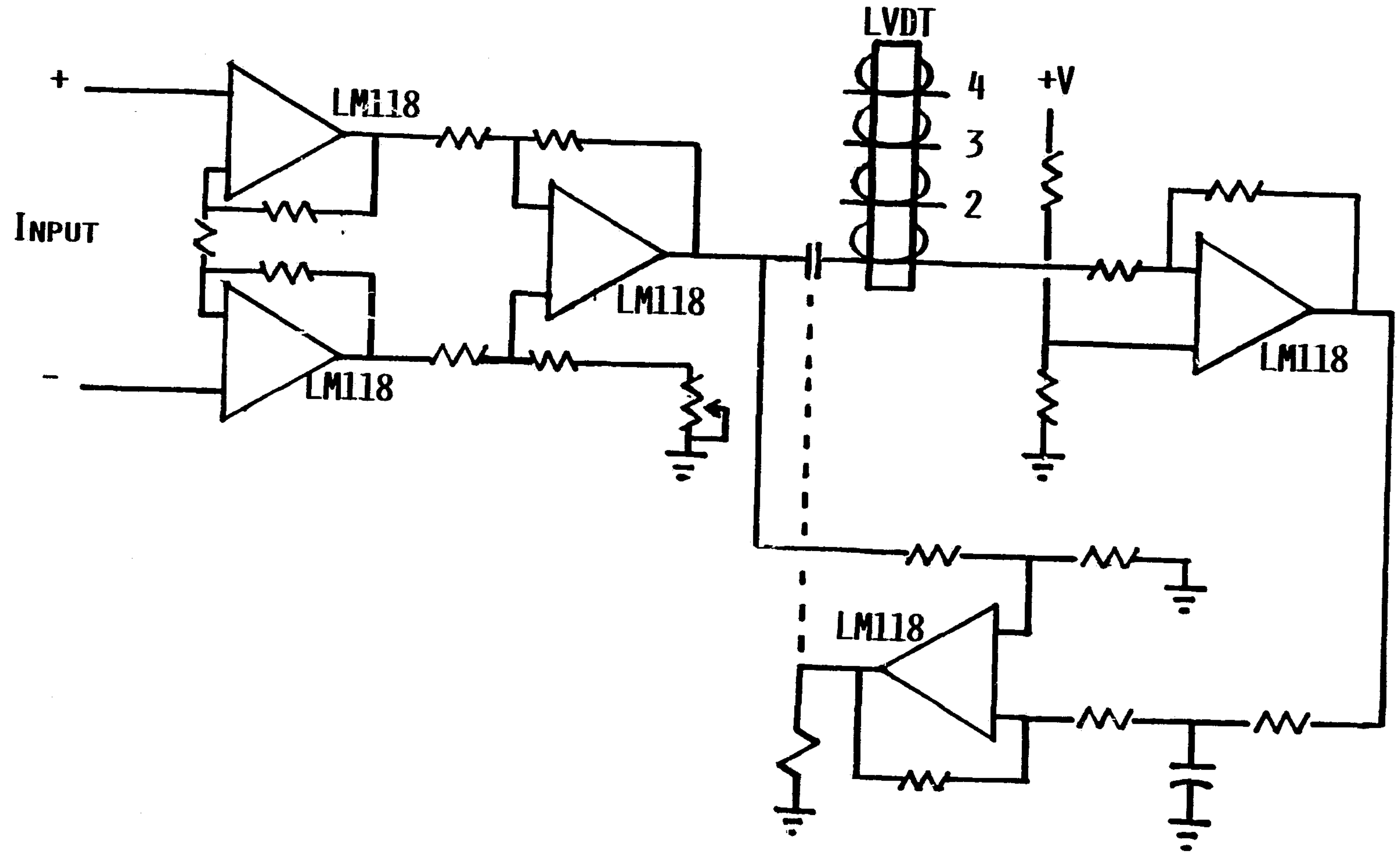

FIGURE A2. ONE CHANNEL OF FLUX SUMMER MODULE (FOUR PER MODULE).

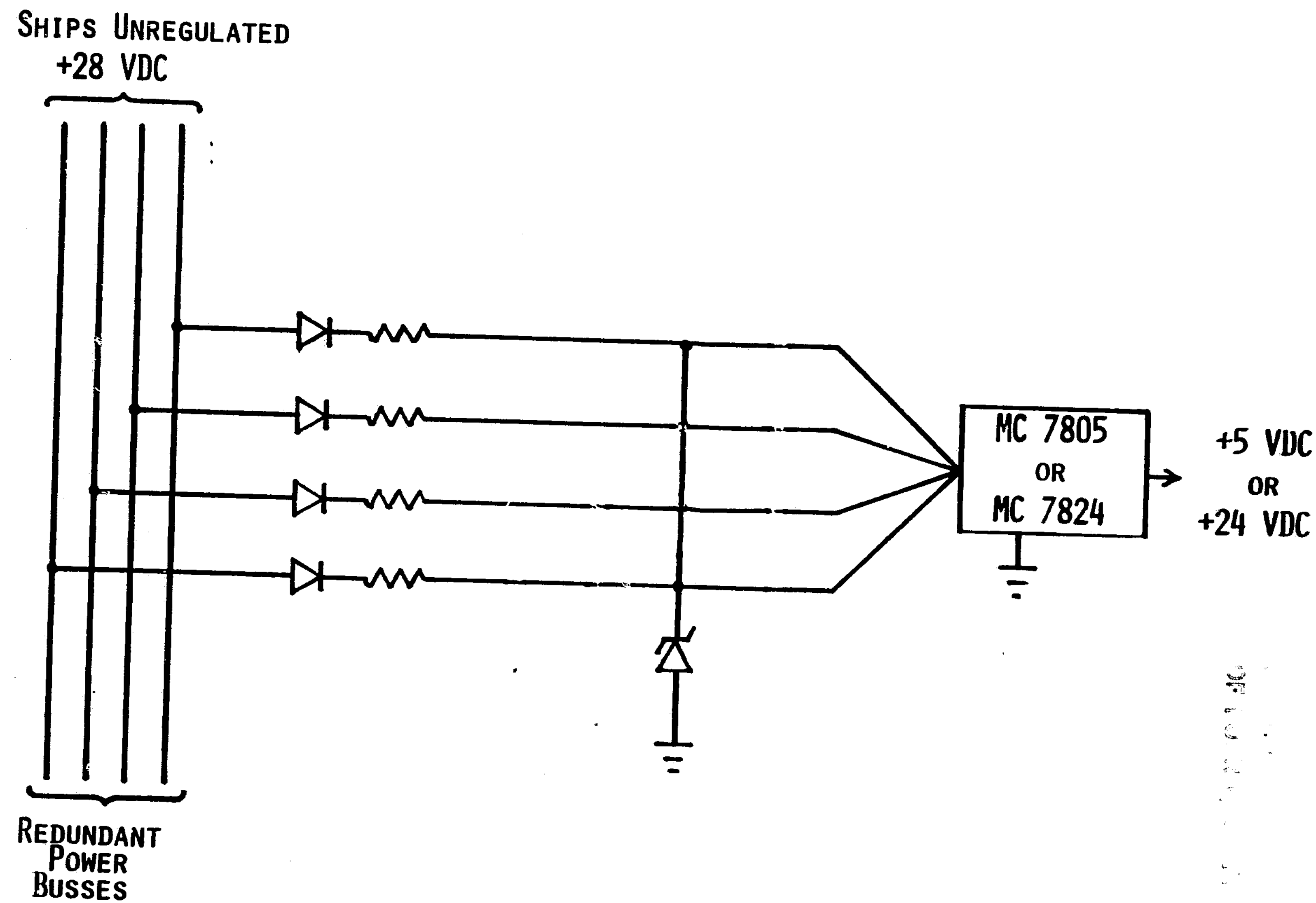

FIGURE A3. DC POWER SUPPLY

A summary of the failure rates for each of the components in each of the three environments under study is included in table A4. The component parts count for each module is shown in table A5.

Table A4
COMPONENT FAILURE RATES(FAILURES/10**6 HOURS)

COMPONENT	SPACE CRAFT	HELICOPTER	AIR TRANSPORT
C8751	2.059834	5.569568	5.410203
D8086	0.586990	1.595600	1.465600
C8087	1.430970	3.441400	3.309000
D2764	0.504830	1.659030	1.561530
HM6116P	0.389820	1.451700	1.352700
MD8282	0.016609	0.096705	0.050205
MD8284A	0.015914	0.087330	0.046830
MD8286	0.011860	0.083900	0.039400
MD8288	0.032147	0.132056	0.083231
HD1-6402	0.281900	0.235450	0.110950
54LS02	0.005231	0.045853	0.019853
54LS04	0.005400	0.046360	0.020360
54LS10	0.005128	0.045544	0.019544
54LS74	0.005986	0.048660	0.022160
54LS125	0.005497	0.046480	0.020480
54LS138	0.007414	0.059850	0.027350
54LS139	0.007550	0.060250	0.027750
54LS367	0.007123	0.058286	0.026286
54LS368	0.007051	0.058054	0.026054
MC7805	0.017420	0.085500	0.066500
MC7824	0.017420	0.085500	0.066500
DAC08A	0.055840	0.282300	0.212300
LM118	0.018710	0.157350	0.119850
OPT TRAN	0.063460	0.455150	0.219910
OPT RECV	0.178930	0.892950	0.662050
OPT CONN	0.100000	0.100000	0.100000
RESISTOR	0.000380	0.010450	0.001064
TRIM RES	0.016200	0.655200	0.081000
CAP 33	0.003744	0.244200	0.084150
CAP .036	0.003744	0.115440	0.039780
ZENER	0.002550	0.076140	0.030600
PWRDIODE	0.000929	0.030193	0.011151
CRYSTAL	0.200000	0.200000	0.200000
RELAY	0.016886	0.816242	0.067543
PC BOARD	0.003000	0.060000	0.012600
PC SOLDR	0.040000	0.640000	0.120000
ELEC CON	0.002325	0.058311	0.011625
OPT LINE	0.100000	0.100000	0.100000

Table A5
COMPONENT PARTS COUNT

	Sensor Module	Input Voter/ Comp. Module	Output Voter Module	Actuator Driver Module
C8751	NC+1	NO+3	0	0
D8086	1	4	1	0
C8087	1	4	1	0
D2764	2	8	2	0
HM6116P	8	26	2	0
MD8282	2	8	2	0
MD8284A	1	4	1	0
MD8286	3	11	2	0
MD8288	1	4	1	0
HD1-6402	1	2	0	0
54LS02	0	1	1	1
54LS04	0	1	1	0
54LS10	1	3	0	0
54LS74	3	12	3	0
54LS125	NC/4	(NO/4)+1	1	0
54LS138	2	6	0	0
54LS139	0	1	1	0
54LS367	1	4	1	0
54LS368	2	6	0	0
MC7805	1	4	1	1
MC7824	0	0	0	1
DAC08A	0	0	0	1
LM118	0	0	0	7
OPT TRAN	NC	NO+1	0	0
OPT RECV	NC	NO+1	0	0
OPT CONN	2*NC	(2*NO)+2	0	0
RESISTOR	NC+9	NO+20	5	23
TRIM RES	0	0	0	1
CAP 33	NC+1	NO+1	0	1
CAP .036	NC+1	NO+1	0	0
ZENER	1	4	1	2
PWRDIODE	4	16	4	8
CRYSTAL	(NC/2)+2	(NO/2)+7	1	0
RELAY	0	0	0	1
PC BOARD	2	4	1	1
PC SOLDR	2	4	1	1
ELEC CON	1	4	1	4
OPT LINE	NC	NO+1	0	0

NC = Number of input voter/computation modules
NO = Number of output voter modules

REFERENCES

1. Wilson, D., "New architectural designs push fault tolerance into the market", Digital Design, pp. 122-127, June 1984.

2. Wensley, J., et. al., "SIFT: design and analysis of a fault tolerant computer for aircraft control", Proc. IEEE, Vol. 66, No. 10, pp. 1240-1255, October 1978.

3. Hopkins, A., et. al., "FTMP--a highly reliable fault tolerant multiprocessor for aircraft", Proc. IEEE, Vol. 66, No. 10, pp. 1221-1239, October 1978.

4. Dunn, Johnson, Meyer, "A fault tolerant distributed microcomputer structure for aircraft navigation and control", Fourteenth Asilomar Conference on Circuits, Systems, and Computers, November 17-19, 1980.

5. Intel Military Products Handbook, Intel Corporation, 1984.

6. Military Handbook: Reliability Prediction of Electronic Equipment, MIL-HDBK-217D, USDOD, January 1982.