TABLE OF CONTENTS

PROGRAM

Wednesday, June 2

8:00- 8:30 Registration

8:30-10:00 Session I A

Welcome - Norman Keith Womer, Dayton Chapter of the American Statistical Association and Air Force Institute of Technology

"The Effect of WIPICS on the F4-B to N Conversion Program"

Norman Keith Womer

10:99-10:30 Break

10:30-12:00 Session I B

Chairman G. C. Saul Young, Air Force Institute of Technology

"The Effect of Renewal Processes Upon Stochastic Reliability Models"

Joseph E. Boyett, L. A. Dugas, and D. H. Hartmann, Air Force Institute of Technology

"Some Generic Properties of a Logic Model for Analysis of Hardware Maintenance and Design Concepts"

James P. Wong and William L. Andre, NASA

12:00- 1:30 Lunch

PROGRAM--Continued

1:30 - 3:30 Session II

Chairman Dwight Collins, Life Cycle Cost Working Group, Aeronautical Systems Division

"A Methodology for Analysis of Alternatives in the Acquisition and Support of Automatic Test Equipment Software"

E. James Dunne-Air Force Institute of Technology, Robert W. Morton-Aeronautical Systems Division, James L. Wilson-Electronic Systems Division

"An Experimental Design for Assessment of Test Repeatability"

Girard Levy and Horace Ray, Battelle Columbus Laboratories

3:30 NO HOST Coctail Party

Thursday, June 3

8:30-10:00 Session III A

Chairman Jon R. Hobbs, Management Science Center, Air Force Logistics Command

"Failure Detection Aids for Human Operator Decisions in Precision Inertial Navigation Systems"

Thomas Kerr, Analysis Sciences Corporation

"Analytical Models of Maintenance Decision Processes"

W. Stephen Demmy, Wright State University

10:00-10:30 Break

10:30-12:00 Session III B

Chairman Robert Gough, U.S. Air Force Academy

"Statistical Classification Methods with Special Emphasis on Growth Curve Data"

Jack C. Lee, Wright State University

"Diagnosis of Reliability Repair Stage and Remedies"

Edward Bilikam, Air Force Avionics Laboratory and Albert H. Moore, Air Force Institute of Technology

12:00- 1:30 Lunch

1:30- 3:30 Session IV

Chairman Norman Keith Womer

"Data Base Requirements for Distribution Studies"

Andrew Lai, Wright State University

SUMMARY AND COMMENTS - Norman Keith Womer

FAILURE DETECTION AIDS FOR HUMAN OPERATOR DECISIONS IN A PRECISION INERTIAL NAVIGATION SYSTEM COMPLEX

Thomas H. Kerr

Member of the Technical Staff
The Analytic Sciences Corporation
Reading, Massachusetts

An existing redundant standby system consisting of two identical Inertial Navigation Systems (INS) may be improved by using a third INS of higher precision as a monitor. The monitor INS provides internal reset corrections which allow the time between external reference position fixes to be extended. Conventional failure detection aids have evolved to enable a human operator to select the best standby INS for navigation. A new method for detecting failures in the monitoring INS has been developed and its performance has been evaluated. A 54 discrete state Markov probability model of the total three-INS complex as a function of the respective Mean-Time-To-Failure and Mean-Repair-Times is presented in this paper. A technique is included for identifying and modeling the human operator's decisions as non-ideal switches, with/without the new method of failure detection for the monitoring INS. This Markov probability model is used as an intermediate step in explicitly specifying how the new failure detection method should interface with the total three-INS complex. This is accomplished by quantitatively evaluating the total system availability. Then the policy which results in the greatest system availability is selected as the most desirable.

1. INTRODUCTION

A simplified block diagram of a navigation system, consisting of three Inertial Navigation Systems (INS), is portrayed in Fig. 1. This configuration represents an improvement to the previously developed standby redundant INS1/INS1' navigation system through the use of the higher precision INS2 as a monitor to enable internal reset corrections between external position fixes. Although the INS contains precision gyros, they incur sufficient drift to necessitate a periodic corrective action consisting of an external position fix. Use of the higher precision INS2 for internal corrections allows a longer time between external fixes to maintain the same or better total system navigation accuracy. The monitoring INS2 is assumed to only have the higher accuracy needed to supply corrective resets to INS1 gyro drift-rates and not to have full navigation capabilities. A more detailed view of the operation and sampling times of this three INS complex is afforded in Fig. 2 where both the Inertial Navigation Unit and its associated controlling software consisting of Kalman filters based on linear error models of the component gyros are shown. (The use of Kalman filters in this role is standard as discussed in Ref. 1.)

An operator (navigator) oversees the operation of this three INS complex. This human operator makes the following decisions which are respectively represented by switches S' and S of Figs. 1 and 2:

- operator selects the mode of operation (either prime mode or back-up mode)
- operator selects the master on-line INS1.

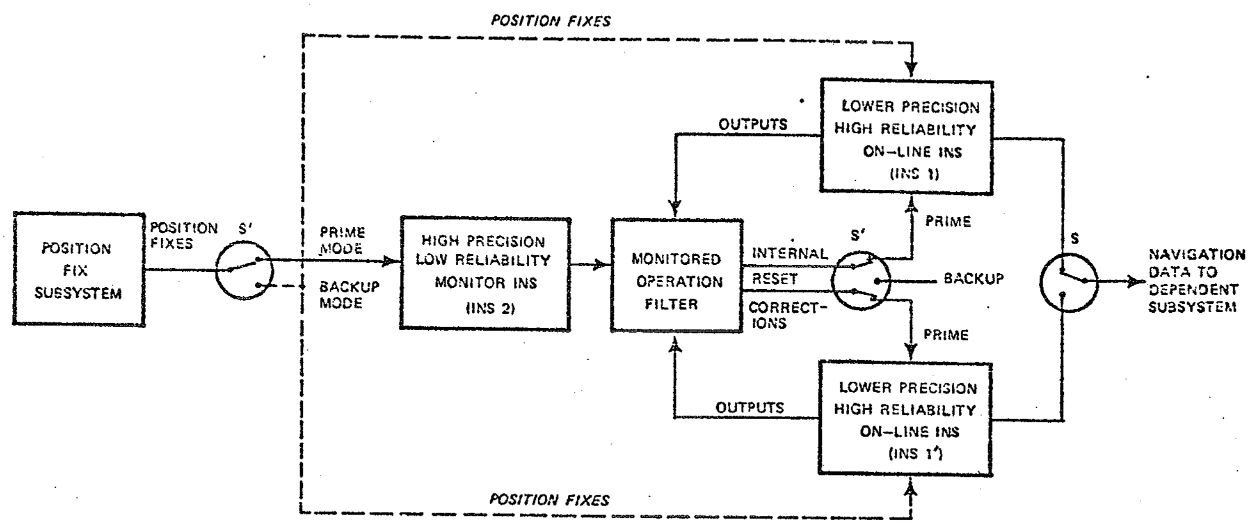


Figure 1 Simplified Block Diagram Overview of the Three INS Complex

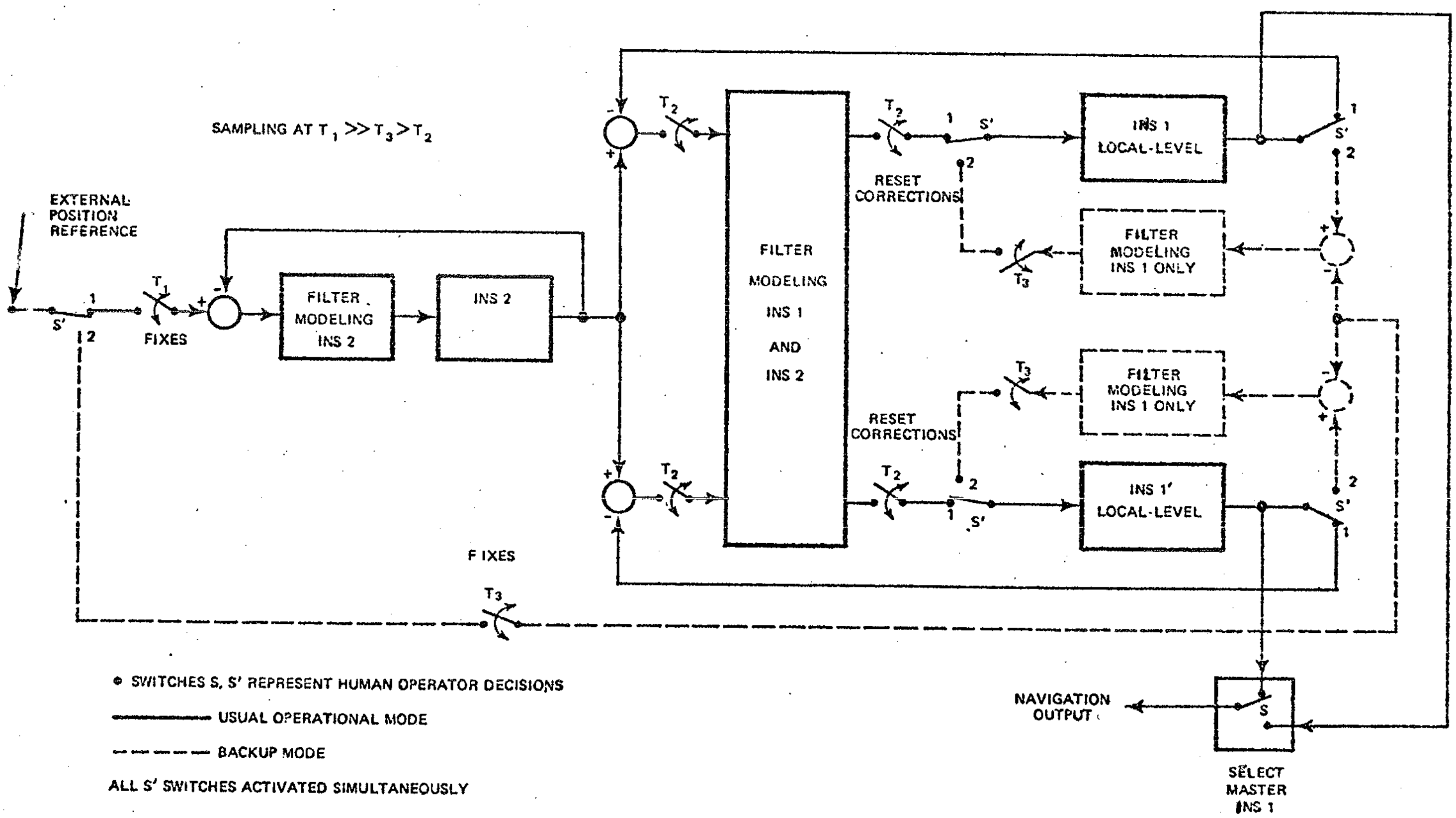


Figure 2 More Detailed View of the INS1/INS2 System

The prime mode uses the newly configured INS1/INS2 while the back-up mode (represented by the dashed lines in Figs. 1 and 2) uses only the standard INS1/INS1'. However, both modes require the selection of the master on-line INS1. The operator's selection of the master INS1 is based on the following information on each INS1 as obtained from a computer or technician's graph:

- plots of the divergence of INS1 (INS1') from external fixes
- plots of INS1 (INS1') gyro bias correction histories
- plots of INS1 (INS1') comparisons to any available reference.

After the total problem of implementation had been partitioned into tractable sub-problems, our primary objective was to specify a method for detecting failures in the INS2. It is critical to detect any INS2 failures, otherwise, faulty internal reset corrections are provided to both INS1 and INS1'. Once the method for detecting failures in the INS2 had been specified and the performance had been evaluated, a natural consequence of the completion of the primary objective is encountered as the secondary objective of specifying how the INS2 failure detector will interface with the entire system. The interface should also include any additional INS2 failure detection aids that are subsequently developed to help the navigator decide in what mode he should operate the system.

The underlying framework of an analysis of the three INS system of Figs. 1 and 2 is presented herein in terms of the simplified representation of Fig. 3, using the standard reliability theory techniques of Ref. 2. The use of more realistic non-ideal switches to represent the human operator's function gives rise to 54 discrete states of a Markov

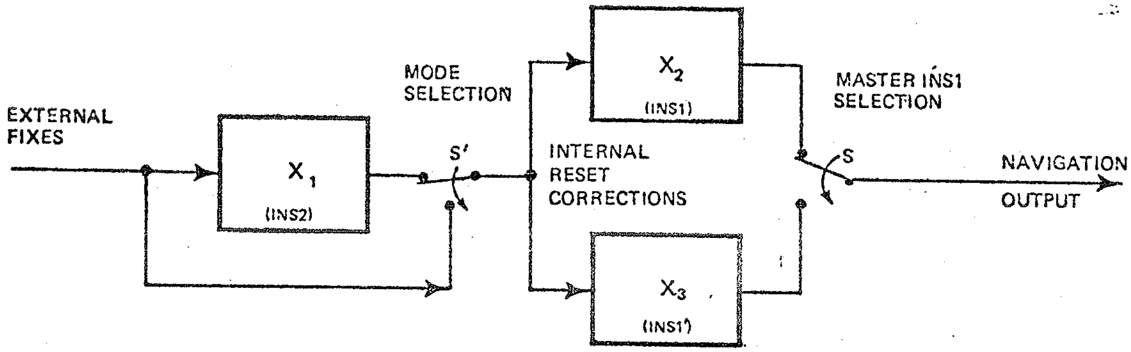


Figure 3 Block Diagram of Three INS Complex as Used in the Availability Analysis

probability model of the system as is discussed in Section 3. A technique is proposed for relatively weighting the failure monitoring test results of the specified INS2 failure detection method with those of any other INS2 failure detection aid (manual or automatic) that is subsequently developed. A quantification of the total system availability (i.e., reliability with repair) is then obtained and the best interfacing policy for integrating the proposed INS2 failure detector into the total system is the policy (corresponding to a weighting) that yields the greatest system availability.

2. AN INS2 FAILURE DETECTION METHOD

A summarizing overview is given in Fig. 4 of how this failure detection approach works. The theoretical basis of the so-called CR2* failure detection approach is a generalization of the use of confidence intervals. The three main ideas that serve as the foundation for CR2 failure detection are shown as three different diagrams in Fig. 4 and are discussed below. These diagrams are shown in juxtaposition to facilitate a comparison of how the relative overlapping of the confidence regions affects the scalar test statistic at three specific check times, t_1, t_2, and t_3. These confidence regions are portrayed in the top diagram of Fig. 4. At each check time, these confidence regions are elliptical. A failure is declared when the two confidence regions do not overlap.

At each check time, t_i, the two elliptical cross sections of the confidence regions, shown in the top diagram of Fig. 4, are fixed levels of two paraboloids, shown in the middle diagram. The problem is to determine whether these two ellipses overlap. In developing the real-time detection algorithm, the test for the presence or absence of overlap was formulated as the solution of a minimization problem. The relative position of $\ell(t_i)$, the minimum point of the intersection of the two paraboloids, to $K_1(t_i)$, the level that corresponds to the elliptical cross section of the confidence regions, determines if there is overlap and,

*CR2 is an acronym for Two (2) Confidence Regions.

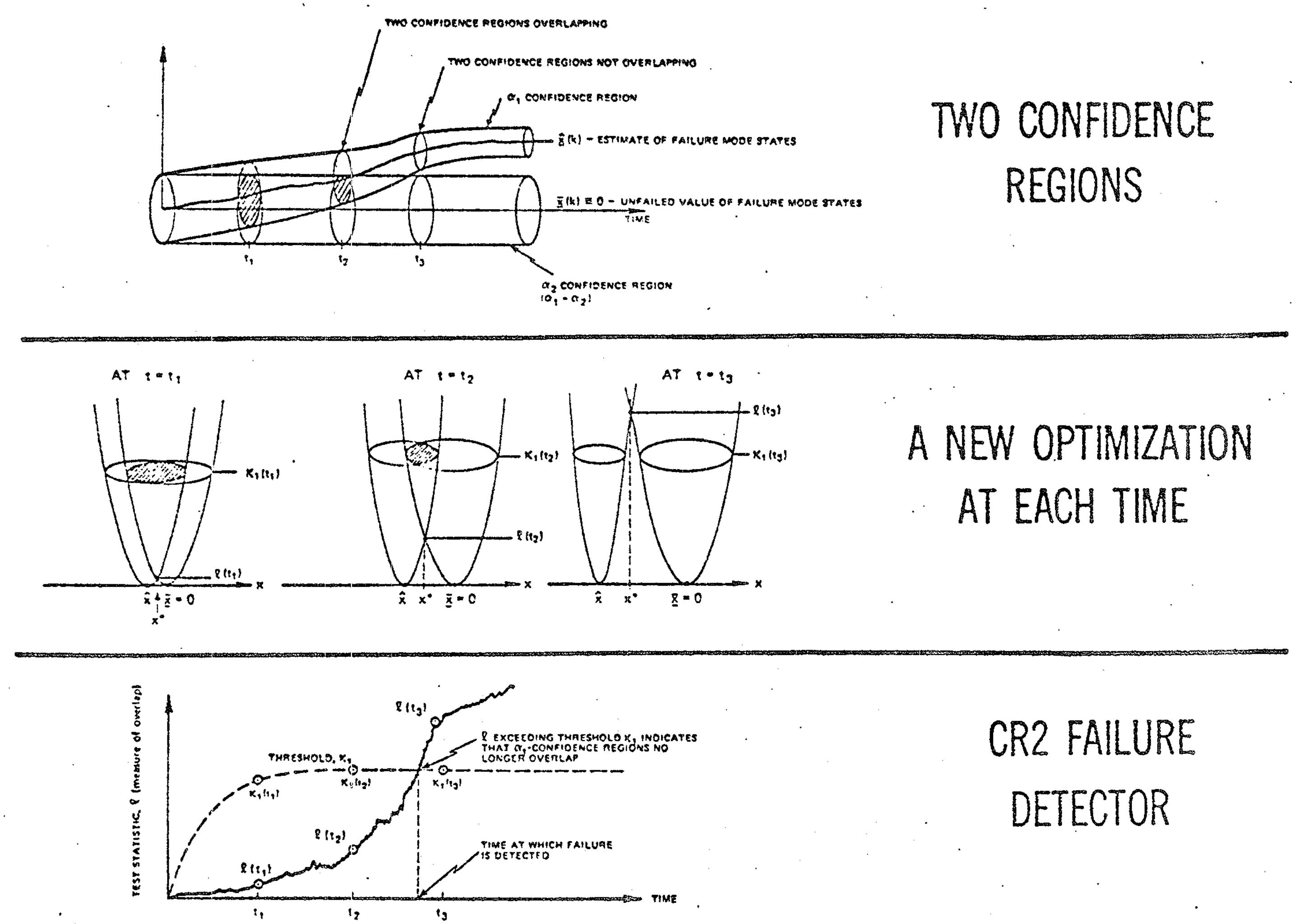


Figure 4 Overview Shows How Comparison of Scalar Test Statistic to Decision Threshold Relates to Test for Confidence Region Overlap Through Artifice of Optimization Problem

if so, the amount of overlap. As long as $\ell(t_i)$ is below $K_1(t_i)$ there is overlap, but when $\ell(t_i)$ exceeds $K_1(t_i)$, <u>then the confidence regions are disjoint and a failure is declared.</u> The relationship between the test statistic $\ell(t_i)$ and the decision threshold $K_1(t_i)$ is summarized in the bottom diagram of Fig. 4. <u>It is sufficient to observe only the test statistic $\ell(t_i)$, and to declare failures when $\ell(t_i)$ exceeds $K_1(t_i)$.</u>

In the CR2 failure detector, a higher level of the threshold K_1, to which the test statistic $\ell(t_i)$ is compared, effectively raises the heights of the ellipses in the associated optimization problem; this corresponds to stouter confidence regions. Analytic expressions have been derived which are used for pre-specifying the time-varying decision threshold K_1 and for evaluating the instantaneous probabilities of the test statistic exceeding the threshold under H_0 (no-failure) and H_1 (a particular magnitude failure), respectively, as P_{fa} and P_d. The expressions are used in the setting of the threshold K_1 in a characteristic trade-off of instantaneous probability of false alarm P_{fa} versus the probability of correct detection P_d* associated with hypothesis testing detection decisions. Early derivations of the CR2 failure detection approach may be found in Refs. 3 and 4, while the most recent theoretical refinements and convergence and convergence-rate proofs are in Ref. 5. The mathematical techniques of confidence regions used in these derivations are similar to those used in Ref. 6.

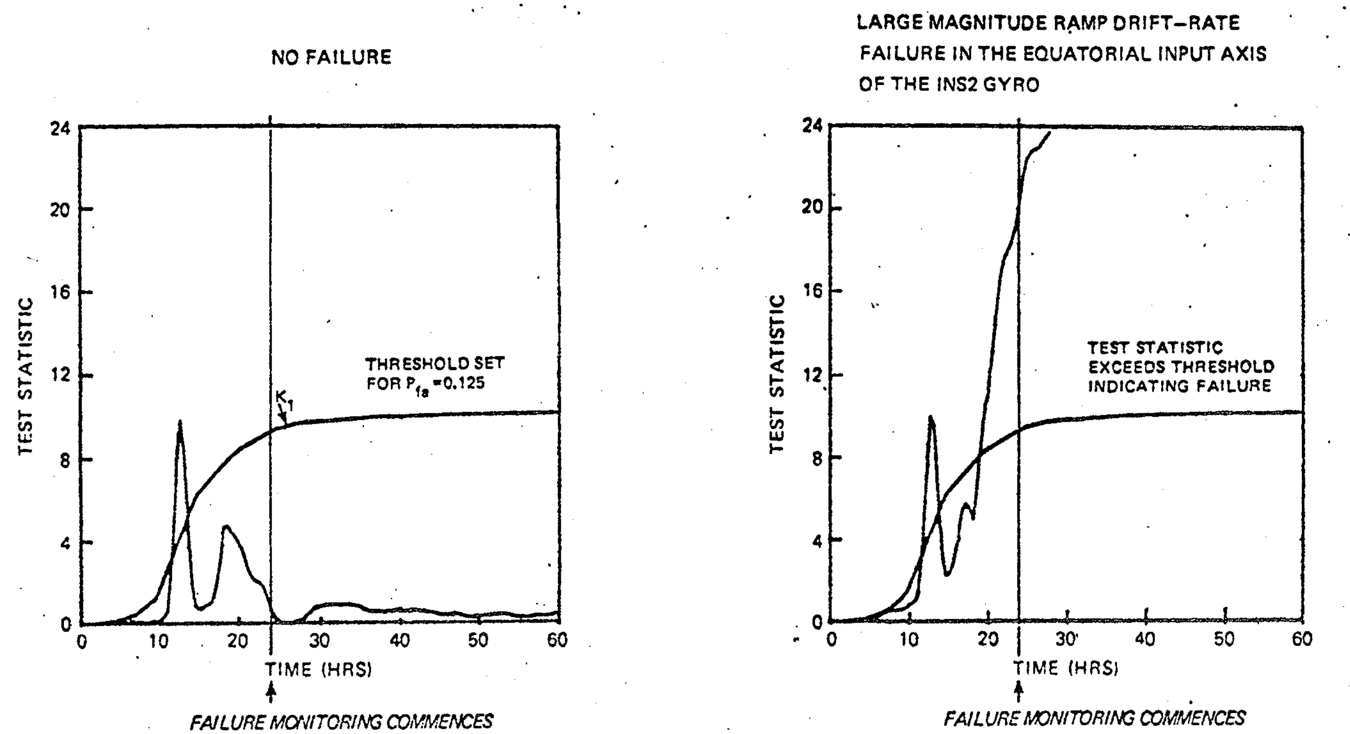
*The probability of miss is $P_m=1-P_d$.

Unlike the situations where the usual likelihood ratio is a Uniformly Most Powerful (UMP) test in that it is as good as or better than any other decision test, an INS2 failure represents a random event that occurs at a random or unknown time. There is little special justification for using a likelihood ratio as a decision function (Ref. 7, p. 96; Ref. 8, p. 315) since it is not UMP for this situation and there may be other decision functions that are as good or better. Confidence region tests serve as one alternative. Recently, confidence region approaches have been developed for other detection applications as well (Ref. 9).

When external position fixes are available to the three-INS complex, failures in the individual INS are more easily detected by a comparison to this more accurate external fix as a standard. The CR2 failure detector is used to detect failures (of a certain critical magnitude corresponding to a certain critical Signal-to-Noise Ratio associated with the resulting failure signal response) between external fixes.

The CR2 failure detection performance on real INS2 data is presented in Fig. 5. The plot on the left of Fig. 5 represents the CR2 test statistic and the pre-specified decision threshold K_1 under a no-failure condition. After an initial 24 hrs,* the test statistic is well below the decision threshold, confirming that no failure is present. The plot on the right of Fig. 5 represents the CR2 test statistic and decision threshold for a large magnitude ramp drift-rate failure in one of the INS2 gyros. Following the initial 24 hr waiting period, the CR2 test statistic quickly exceeds the threshold correctly indicating a failure.

*The error dynamics of a gyro reflect the 24 hr earth rotation rate; consequently, approximately one full 24 hr period is required for the filter to lock onto the cycle of the underlying sinusoid.



- SIMULATED FAILURE AT t = 0 HRS
- IGNORING INITIAL TRANSIENTS DURING FIRST 24 HRS FOLLOWS POLICY SPECIFICATION

Figure 5 INS2 (CR2) Failure Detection Performance Using Real Data

3. AVAILABILITY ANALYSIS OF THE THREE INS COMPLEX

3.1 THE MARKOV MODEL FOR THE DISCRETE STATE PROBABILITIES

The configuration of Fig. 3 is now analyzed using the standard reliability theory techniques and failure/repair models of Ref. 2. These standard failure and repair models are illustrated in Fig. 6. A representative failure density and its normalization as the more useful "bathtub" hazard rate are depicted in the upper two diagrams of Fig. 6. For each INS, it is assumed that operation is between the times t_1 and t_2 and that here the hazard rate is a constant* (consistent with the usual model for these modular components as an exponential failure density with specified Mean-Time-To-Failure). The lower diagram in Fig. 6 is the standard Erlang or gamma distributed repair model. Here again the official Navy model is an exponential repair model with specified Mean-Repair-Time.

In performing the availability analysis, the following notation and conventions will be used.

Modular INS components have two states:

$X_i \triangleq$ component i is navigating within specifications

$\overline{X}_i \triangleq$ component i is not navigating within specifications.

*A constant hazard rate is reasonable assuming that infant mortality failures have been weeded out through initial acceptance testing and that wear-out failures are avoided through periodic preventive maintenance.

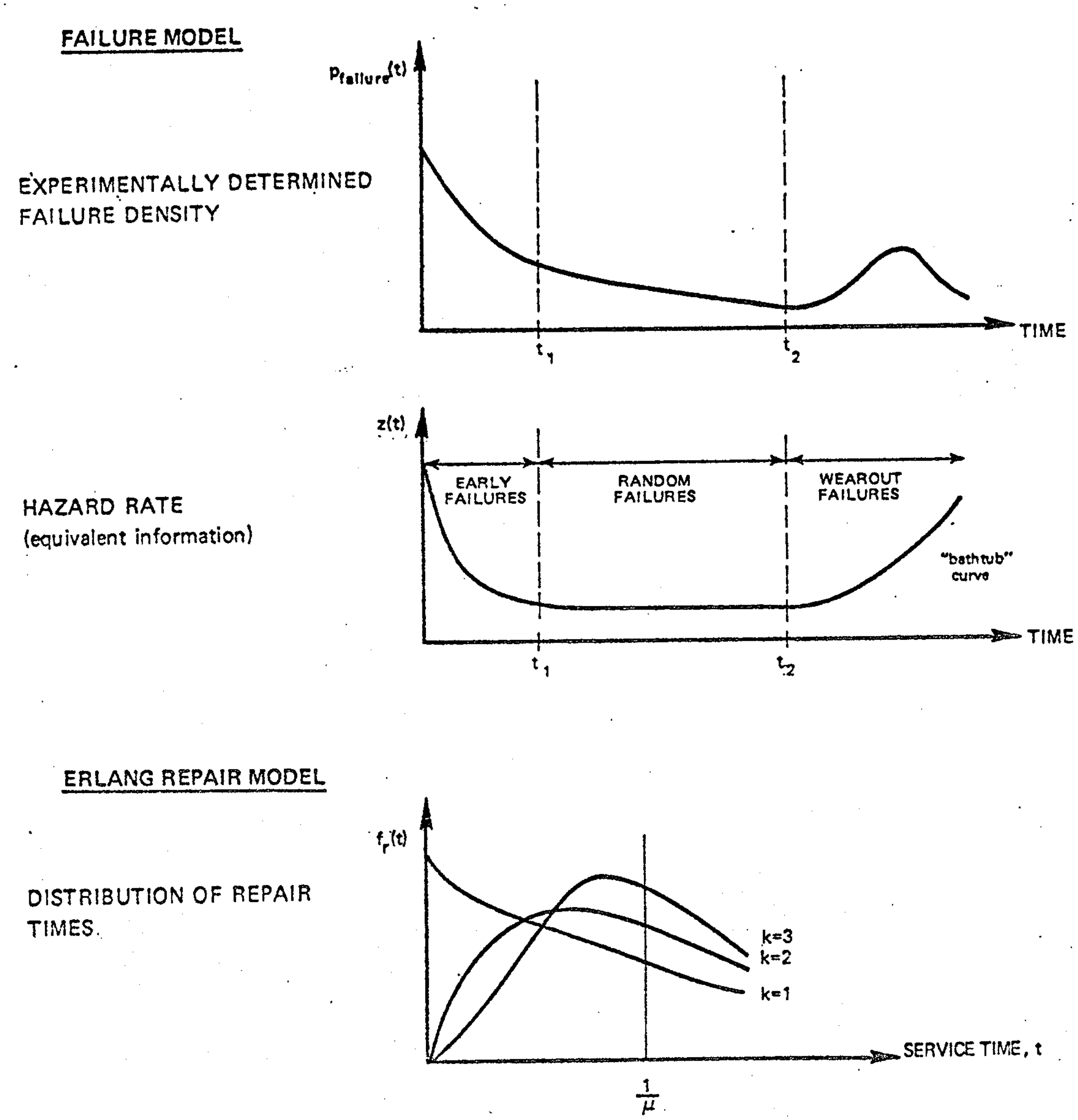


Figure 6 Standard Failure and Repair Models Used in the Availability Analysis

The non-ideal switches representing the human operator decisions have three states:

$S \triangleq$ switch S is performing perfectly

$\overline{S} \triangleq$ switch S does not respond to a failed INS1 (i.e., $P_M \equiv 1-P_d < 1$)

$\overline{\overline{S}} \triangleq$ switch S actuates by mistake while INS1 is good (i.e., $P_{fa} > 0$) .

Similarly*

$S' \triangleq$ switch S' is performing perfectly

$\overline{S}' \triangleq$ switch S' does not respond to a failed INS2 (i.e., $P'_M \equiv 1-P'_d < 1$)

$\overline{\overline{S}}' \triangleq$ switch S' actuates by mistake while INS2 is good (i.e., $P'_{fa} > 0$) .

The number of discernable discrete states in a totally exhaustive enumeration of the possible combinations of failed and unfailed INS and satisfactory/false-alarming/missing switches in the 5-element model of Fig. 3 is $(2)^3(3)^2 = 72$. Since X_2 (INS1) is identical to X_3 (INS1') as a warm stand-by system, the total number of states may be collapsed to 54 as indicated in Ref. 2 and explicitly enumerated in Table 1. The following further superscript notation is used in Table 1:

† $\triangleq$ Total System Failure. No good navigation information is available.

* $\triangleq$ Partial System Failure. Only good INS1 or INS1' navigation information is available.

*This reliability analysis is applicable to any INS2 failure detection method that uses the same filter inputs as used by the CR2 test as long as the P'_d and P'_{fa} which characterize it have been evaluated.

TABLE 1

AN EXHAUSTIVE ENUMERATION OF THE DISCRETE STATES IN THE STANDBY/SERIES 5 ELEMENT SYSTEM OF FIG. 3

$S_1 = S'X_1X_2X_3S$	$S_{19} = S'X_1X_2X_3\bar{S}$	$S_{37} = \bar{\bar{S}}'X_1X_2X_3\bar{S}^*$
$S_2 = S'\bar{X}_1X_2X_3S^*$	$S_{20} = S'\bar{X}_1X_2X_3\bar{S}^*$	$S_{38} = \bar{\bar{S}}'\bar{X}_1X_2X_3\bar{S}$
$S_3 = S'X_1\bar{X}_2X_3S+S'X_1X_2\bar{X}_3S$	$S_{21} = S'X_1\bar{X}_2X_3\bar{S}+S'X_1X_2\bar{X}_3\bar{S}^\dagger$	$S_{39} = \bar{\bar{S}}'X_1\bar{X}_2X_3\bar{S}+\bar{\bar{S}}'X_1X_2\bar{X}_3\bar{S}^\dagger$
$S_4 = S'\bar{X}_1\bar{X}_2X_3S+S'\bar{X}_1X_2\bar{X}_3S^*$	$S_{22} = S'\bar{X}_1\bar{X}_2X_3\bar{S}+S'\bar{X}_1X_2\bar{X}_3\bar{S}^\dagger$	$S_{40} = \bar{\bar{S}}'\bar{X}_1\bar{X}_2X_3\bar{S}+\bar{\bar{S}}'\bar{X}_1X_2\bar{X}_3\bar{S}^\dagger$
$S_5 = S'X_1\bar{X}_2\bar{X}_3S^\dagger$	$S_{23} = S'X_1\bar{X}_2\bar{X}_3\bar{S}^\dagger$	$S_{41} = \bar{\bar{S}}'X_1\bar{X}_2\bar{X}_3\bar{S}^\dagger$
$S_6 = S'\bar{X}_1\bar{X}_2\bar{X}_3S^\dagger$	$S_{24} = S'\bar{X}_1\bar{X}_2\bar{X}_3\bar{S}^\dagger$	$S_{42} = \bar{\bar{S}}'\bar{X}_1\bar{X}_2\bar{X}_3\bar{S}^\dagger$
$S_7 = \bar{S}'X_1X_2X_3S$	$S_{25} = S'X_1X_2X_3\bar{\bar{S}}$	$S_{43} = \bar{S}'X_1X_2X_3\bar{\bar{S}}$
$S_8 = \bar{S}'\bar{X}_1X_2X_3S^\dagger$	$S_{26} = S'\bar{X}_1X_2X_3\bar{\bar{S}}^*$	$S_{44} = \bar{S}'\bar{X}_1X_2X_3\bar{\bar{S}}^\dagger$
$S_9 = \bar{S}'X_1\bar{X}_2X_3S+\bar{S}'X_1X_2\bar{X}_3S$	$S_{27} = S'X_1\bar{X}_2X_3\bar{\bar{S}}+S'X_1X_2\bar{X}_3\bar{\bar{S}}^\dagger$	$S_{45} = \bar{S}'X_1\bar{X}_2X_3\bar{\bar{S}}+\bar{S}'X_1X_2\bar{X}_3\bar{\bar{S}}^\dagger$
$S_{10} = \bar{S}'\bar{X}_1\bar{X}_2X_3S+\bar{S}'\bar{X}_1X_2\bar{X}_3S^\dagger$	$S_{28} = S'\bar{X}_1\bar{X}_2X_3\bar{\bar{S}}+S'\bar{X}_1X_2\bar{X}_3\bar{\bar{S}}^\dagger$	$S_{46} = \bar{S}'\bar{X}_1\bar{X}_2X_3\bar{\bar{S}}+\bar{S}'\bar{X}_1X_2\bar{X}_3\bar{\bar{S}}^\dagger$
$S_{11} = \bar{S}'X_1\bar{X}_2\bar{X}_3S^\dagger$	$S_{29} = S'X_1\bar{X}_2\bar{X}_3\bar{\bar{S}}^\dagger$	$S_{47} = \bar{S}'X_1\bar{X}_2\bar{X}_3\bar{\bar{S}}^\dagger$
$S_{12} = \bar{S}'\bar{X}_1\bar{X}_2\bar{X}_3S^\dagger$	$S_{30} = S'\bar{X}_1\bar{X}_2\bar{X}_3\bar{\bar{S}}^\dagger$	$S_{48} = \bar{S}'\bar{X}_1\bar{X}_2\bar{X}_3\bar{\bar{S}}^\dagger$
$S_{13} = \bar{\bar{S}}'X_1X_2X_3S^*$	$S_{31} = \bar{S}'X_1X_2X_3\bar{S}$	$S_{49} = \bar{\bar{S}}'X_1X_2X_3\bar{\bar{S}}^*$
$S_{14} = \bar{\bar{S}}'\bar{X}_1X_2X_3S^*$	$S_{32} = \bar{S}'\bar{X}_1X_2X_3\bar{S}^\dagger$	$S_{50} = \bar{\bar{S}}'\bar{X}_1X_2X_3\bar{\bar{S}}^*$
$S_{15} = \bar{\bar{S}}'X_1\bar{X}_2X_3S+\bar{\bar{S}}'X_1X_2\bar{X}_3S^*$	$S_{33} = \bar{S}'X_1\bar{X}_2X_3\bar{S}+\bar{S}'X_1X_2\bar{X}_3\bar{S}^\dagger$	$S_{51} = \bar{\bar{S}}'X_1\bar{X}_2X_3\bar{\bar{S}}+\bar{\bar{S}}'X_1X_2\bar{X}_3\bar{\bar{S}}^\dagger$
$S_{16} = \bar{\bar{S}}'\bar{X}_1\bar{X}_2X_3S+\bar{\bar{S}}'\bar{X}_1X_2\bar{X}_3S^*$	$S_{34} = \bar{S}'\bar{X}_1\bar{X}_2X_3\bar{S}+\bar{S}'\bar{X}_1X_2\bar{X}_3\bar{S}^\dagger$	$S_{52} = \bar{\bar{S}}'\bar{X}_1\bar{X}_2X_3\bar{\bar{S}}+\bar{\bar{S}}'\bar{X}_1X_2\bar{X}_3\bar{\bar{S}}^\dagger$
$S_{17} = \bar{\bar{S}}'X_1\bar{X}_2\bar{X}_3S^\dagger$	$S_{35} = \bar{S}'X_1\bar{X}_2\bar{X}_3\bar{S}^\dagger$	$S_{53} = \bar{\bar{S}}'X_1\bar{X}_2\bar{X}_3\bar{\bar{S}}^\dagger$
$S_{18} = \bar{\bar{S}}'\bar{X}_1\bar{X}_2\bar{X}_3S^\dagger$	$S_{36} = \bar{S}'\bar{X}_1\bar{X}_2\bar{X}_3\bar{S}^\dagger$	$S_{54} = \bar{\bar{S}}'\bar{X}_1\bar{X}_2\bar{X}_3\bar{\bar{S}}^\dagger$

* = Partial System Failure

† = Total System Failure

It may be summarized from Table 1 that there are

- 9 states for good INS1/INS2 navigation information
- 11 states for good INS1 (or INS1') navigation information only
- 34 states for having no* good navigation information

for a total of 54 discrete states.

*It is considered that no good navigation information is available when both INS1 and INS1' are failed even though the INS2 may be unfailed because the INS2 is assumed to only have higher precision gyros and not to have full navigation capabilities. Therefore, as indicated in Fig. 3, it may <u>not be used alone</u> for navigation.

Associated with this 5-element system is a vector of probabilities corresponding to the likelihood that the system of Fig. 3 will be found in a particular state of the 54 discrete states enumerated in Table 1 at a specified time. In general, the probabilities of occupying a particular state change as a function of time and the specific manner of interconnection and satisfy a linear difference equation of the following form:

$$\begin{bmatrix} P_{S_1}(t+\Delta) \\ P_{S_2}(t+\Delta) \\ \cdot \\ \cdot \\ \cdot \\ P_{S_{54}}(t+\Delta) \end{bmatrix} = \begin{bmatrix} \mathrm{T} \\ \\ \text{TRANSITION} \\ \text{PROBABILITIES} \\ \\ \end{bmatrix} \begin{bmatrix} P_{S_1}(t) \\ P_{S_2}(t) \\ \cdot \\ \cdot \\ \cdot \\ P_{S_{54}}(t) \end{bmatrix} \qquad (1)$$

This equation characterizes the time evolution of the absolute probability of each of the 54 possible states being assumed by the system as determined by the transition probabilities. An exhaustive enumeration of the 54 states in Table 1 which the system of Fig. 3 can assume is needed as a necessary intermediate step in specifying the elements of the associated transition probability matrix, T in Eq. (1), that characterizes the specific system interconnections and manner of use.

Two representative examples are presented here to demonstrate how the elements of the transition probability matrix are determined. Consider the following state as the focus of attention

$$S_{16} = \bar{\bar{S}}'\bar{X}_1\bar{X}_2X_3S+\bar{\bar{S}}'\bar{X}_1X_2\bar{X}_3S \qquad (2)$$

which represents switch S' in a mode where it would be prone to false alarm (whether X_1 is failed or not), but with X_1 (INS2) in a condition of failure, and either X_2(INS1) or X_3(INS1') in a failed condition (but not both). The state S_{16} is one designated as a partial systems failure because there is one INS1 available and switch S is neither in the false alarm mode nor in the miss mode so the selection of the proper INS1 (INS1') to use in navigation is correctly made and good navigation information <u>is</u> available but only from an INS1 (INS1').

In the flow diagram of Fig. 7,* the state S_{16} may be entered at time = t+Δ (notation: $S_{16}(t+\Delta)$) only through the paths shown from the five states S_4, S_{14}, S_{15}, S_{16}, S_{18} if they were occupied at time = t† (notation: $S_4(t)$, $S_{14}(t)$, etc.). The transition probability, t_{ji}, of going from one state S_i to a distinctly different state S_j is the feed-forward hazard rate times the time step Δ, e.g., the transition probability of going from state $S_{14}(t)$ to $S_{16}(t+\Delta)$ is

$$t_{16,14} = 2\lambda_1 \cdot \Delta \qquad (3)$$

The probability of occupying the same state at time = t+Δ, $S_i(t+\Delta)$, as was occupied on the previous step at time = t, $S_i(t)$, is‡

---

*Reciprocals of MTTF and <u>M</u>ean-<u>R</u>epair-<u>T</u>ime for the INS1 and INS2 are, respectively, λ_1, μ_1 and λ_2, μ_2.

†This model uses the standard reliability assumption of only one allowable change in status during one transition step=Δ.

‡These are elements along the principal diagonal of the transition probability matrix, T.

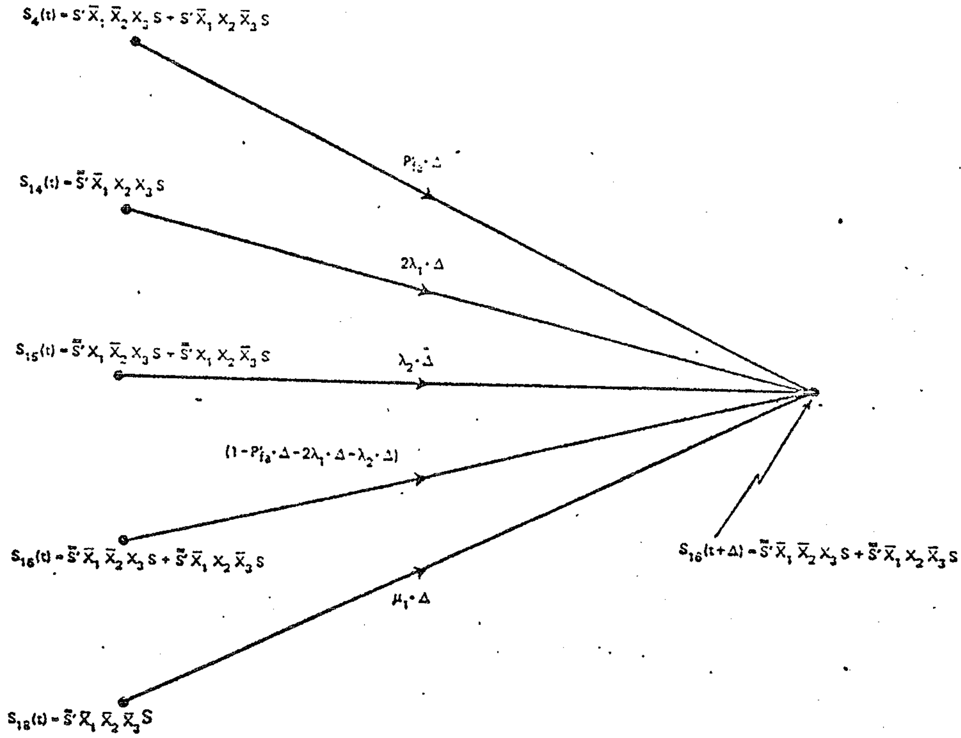


Figure 7 Allowable States at Time=t That May Enter State S_{16} at Time=t+Δ

$$t_{i,i} = 1 - \sum (j^{th} \text{ hazard rate}) \cdot \Delta \tag{4}$$

j ranges over all feedforward paths for switches and failures connecting with state S_i, $j \neq i$

e.g., the transition probability of being in state S_{16} at time = t+Δ given that state S_{16} was occupied at time = t is

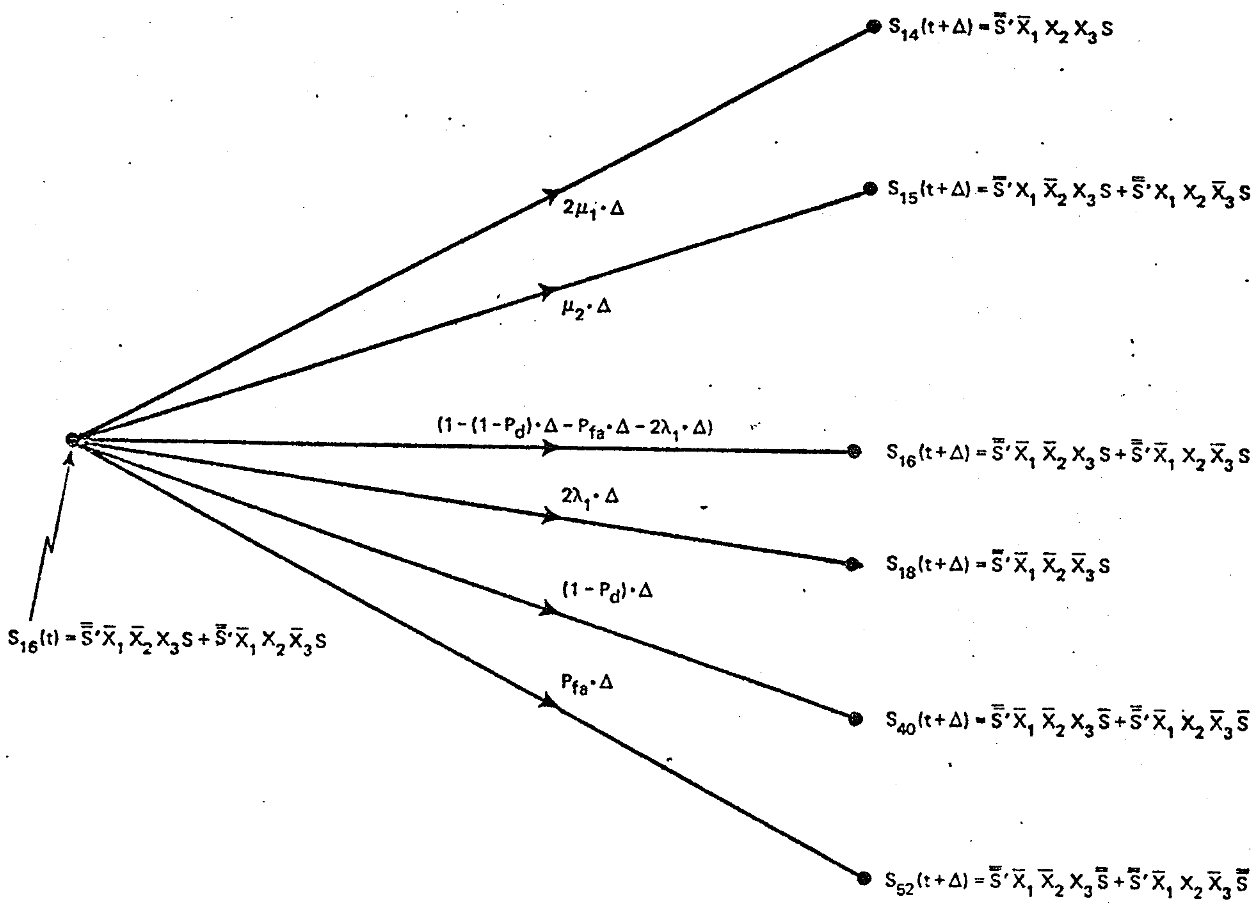
$$t_{16,16} = 1-P'_{fa}\cdot\Delta - 2\lambda_1\cdot\Delta-\lambda_2\cdot\Delta \tag{5}$$

The scalar iteration equation for the probability of being in state S_{16} at time = t+Δ, as obtained from Fig. 7, is

$$P_{S_{16}}(t+\Delta) = P'_{fa}\cdot\Delta\ P_{S_4}(t) + 2\lambda_1\cdot\Delta\ P_{S_{14}}(t) + \lambda_2\cdot\Delta\ P_{S_{15}}(t)$$
$$+ (1-P'_{fa}\cdot\Delta-2\lambda_1\cdot\Delta-\lambda_2\cdot\Delta)\ P_{S_{16}}(t) + \mu_1\cdot\Delta\ P_{S_{18}}(t) \tag{6}$$

From Fig. 8, the state S_{16} at time = t is an allowable entry state for states S_{14}, $S_{15}, S_{16}, S_{18}, S_{40}, S_{52}$ at time = t+Δ. Therefore, the column of the transition probability matrix T, to be multiplied by $P_{S_{16}}(t)$ in Eq. (1), has non-zero path entries only on the rows corresponding respectively to $S_{14}, S_{15}, S_{16}, S_{18}, S_{40}, S_{52}$. This same type of analysis is performed for each of the other 54 states in order to completely specify the transition probability matrix T.*

As indicated by the above representative example of state S_{16}, T is a rather sparse matrix. Also, notice that the elements of T are the constants $P_d, P_{fa}, P_d', P_{fa}', \lambda_1, \lambda_2, \mu_1, \mu_2$; this result is a consequence of the exponential repair models



*A consistency check on T is that for $\mu_1 = \mu_2 = 0$, the elements in each column sum to one.

and the constant hazard functions of the exponential failure models. Since the transition probabilities are all independent of time and depend only on Δ, the underlying Markov process is termed homogeneous. Since the homogeneous process of this analysis does not have the property that any state may be reached directly from any other state with positive probability at each time, this system is not ergodic (Ref. 2). The vector iteration equation of Eq. (1) is linear and time invariant for the system of this analysis and is therefore extremely convenient to work with.

3.2 FORMULATING TWO APPROPRIATE AVAILABILITY EXPRESSIONS

As indicated in Section 3.1 and in Table 1 by * and † there are two types of good navigation information that are available from this three-INS complex. When the three-INS complex is operating in a well-functioning state representing the primary mode, there is high quality INS1/INS2 navigation information. When the three-INS complex is operating in a well-functioning state representing the back-up mode, there is lower quality INS1/INS1' navigation information (with more frequent external reference position fixes required). To reflect the two different, but successful, operational modes of the system, the former being more desirable as the principal objective than the latter, two different availability functions are defined. Availability functions which are, by definition, the probability of operating successfully with repair (in contradistinction to reliability which consists of the same probabilities but without allowing the policy of repair) were chosen to correspond to the situations of

(1) having only successful INS1/INS2 navigation information

(2) having any successful navigation information, either INS1/INS2 or just INS1/INS1'.

These two availability expressions corresponding, respectively, to 1 and 2 above, are

$$A_{1/2}(t) \triangleq P_{S_1}(t) + P_{S_3}(t) + P_{S_7}(t) + P_{S_9}(t) + P_{S_{19}}(t) + P_{S_{25}}(t) + P_{S_{31}}(t) + P_{S_{38}}(t) + P_{S_{43}}(t) \qquad (7)$$

$$A_{1/1'}(t) \triangleq A_{1/2}(t) + P_{S_2}(t) + P_{S_4}(t) + P_{S_{13}}(t) + P_{S_{14}}(t) + P_{S_{15}}(t) + P_{S_{16}}(t) + P_{S_{20}}(t) + P_{S_{26}}(t) + P_{S_{37}}(t) + P_{S_{49}}(t) + P_{S_{50}}(t) \qquad (8)$$

where the $P_{S_i}(t)$ are the unconditional probabilities of being in the states S_i at time t, with the evolution being completely specified by the iteration equation of Eq. (1). Notice that $A_{1/1}'$, the availability of any good navigation information whatsoever, wholly contains $A_{1/2}(t)$, the availability of the INS1/INS2, in addition to the non-negative quantities representing the unconditional probabilities of being in the states designated as partial failures.

3.3 A PROPOSED NEW MODEL FOR THE HUMAN OPERATOR DECISION

It is standard practice to model the decisions of a human operator as a switch (Ref. 2). When a more detailed and accurate analysis is warranted, it is also standard to acknowledge that the switch is not really perfect (Ref. 10) but inherently contains a detector which may sometimes miss (i.e., switch remains in position because of a failure to recognize that conditions are such that it should have been thrown) and false alarm (i.e., switch has flipped even though conditions do not warrant it). The ensemble statistics of the imperfect switch which completely characterize its behavior are its inherent probability of false alarm and its probability of miss.

Switch S represents the human operator's decision in the selection of the master INS1, as aided by the information from the accessible computer outputs and plots mentioned in Section 1. Switch S' represents the human operator's decision in the selection of the operational mode. To date, the only INS2 failure detection technique available for use as the detection element (between external position resets) is of the form of the CR2 technique and consequently, its P_d and P_{fa} characteristics apply directly to switch S' only if it is used exclusively. For the case where the CR2 technique is used exclusively, the effective characterizing ensemble statistics for switch S' are:

$$P'_{fa},eff = P^{OP}_{fa},CR2 \tag{9}$$

$$P'_{d},eff = P^{OP}_{d},CR2 \tag{10}$$

where P'_{fa},eff (P'_d,eff) represents the <u>eff</u>ective P_{fa}(P_d) of switch S' and P_{fa},CR2 (P_d,CR2) represents the particular characterizing statistic of the CR2 failure detector with the Operating Point (OP) being determined by the level of the pre-specified decision threshold K_1 that is used. However, other INS2 failure detection techniques (possibly manual) are currently under development and upon completion may also be used in the detection element of switch S'. If these new techniques are used exclusively, then the effective characterizing ensemble statistics for switch S' are

$$P'_{fa},\text{eff} = P_{fa}^{OP'},\text{manual} \tag{11}$$

$$P'_{d},\text{eff} = P_{d}^{OP'},\text{manual} \tag{12}$$

where the subscript "manual" is just used to distinguish these characteristics from those associated with the CR2 technique.

A natural question to ask is "can the two detection techniques be used together to enhance performance and if so, what would be an optimum mix?" Any attempt to answer this question requires a model for the effective P_d and P_{fa} of switch S' when both failure detection methods are used. The new model that is being proposed to effectively characterize switch S' when both failure detection techniques are being used simultaneously with relative weightings $(1-\lambda)$ and λ is

$$P'_{fa},\text{eff} = (1-\lambda)\cdot P_{fa}^{OP'},\text{manual} + \lambda\cdot P_{fa}^{OP},\text{CR2} \tag{13}$$

$$P'_{d},\text{eff} = (1-\lambda)\cdot P_{d}^{OP'},\text{manual} + \lambda\cdot P_{d}^{OP},\text{CR2} \tag{14}$$

where

$$0 \leq \lambda \leq 1 \tag{15}$$

Notice that this is a linear interpolative model which incorporates the following highly desirable properties:

- For $\lambda=1$, the proposed model of Eqs. (13), (14) reduces to the standard result of Eq. (9),(10).
- For $\lambda=0$, the proposed model of Eqs. (13), (14) reduces to the standard result of Eq. (11),(12).
- For any λ such that Eq. (15) is satisfied, the proposed model of Eqs. (13), (14) results in quantities that have all the requisite properties to be probabilities (i.e.,

$$0 \leq P'_{fa},eff \leq 1 \tag{16}$$

$$0 \leq P'_{d},eff \leq 1 \tag{17}$$

as a natural consequence of the same inequality being satisfied by P_{d},manual; P_{d},CR2; P_{fa},manual; and P_{fa},CR2).

- The combined use of both failure detection techniques corresponding to this proposed linear model may be implemented easily by using the linear weightings in the combined decision rule as discussed below.

A combined decision rule corresponding to the above proposed model is easily obtained. The combined decision rule is as follows:

(1) if

$$(1-\lambda)\cdot \ell_2 + \lambda\cdot \ell_1 \leq (1-\lambda)\cdot K_2 + \lambda\cdot K_1 \tag{18}$$

then choose H_0: no-failure

(2) if

$$(1-\lambda)\cdot \ell_2 + \lambda\cdot \ell_1 \geq (1-\lambda)\cdot K_2 + \lambda\cdot K_1 \tag{19}$$

then choose H_1: a failure (having the critical SNR magnitude) where ℓ_1 is the test statistic and K_1 is the pre-specified decision threshold of the CR2 failure detection technique while ℓ_2 is the test statistic and K_2 is the pre-specified decision threshold of the so-called manual failure detection technique. Notice that for the two extremes of $\lambda=0$ or $\lambda=1$, the decision rule of Eqs. (18) and (19) reduces to the usual decision rules for each separate detection technique.

This proposed model offers an additional appeal when the so-called Receiver Operating Characteristics (ROC) of Fig. 9, which underly all binary decision tests (Ref. 7), are considered. The two hypothetical solid curves in Fig. 9 represent the complete operating capability ranges of the two failure detection techniques. For each of the failure detectors, the usual practice is to trade-off P_d versus P_{fa} by deciding upon a compromise operating point (usually chosen to be in the vicinity of the "knee" of the curve). This operating point is fixed by fixing the decision threshold. The operating points of the two curves are represented by OP and OP' and are denoted by the corresponding two coordinates (P_{fa},P_d). In general, the plane cannot be ranked (only the real line R may be ordered); so, in general, it is impossible to say, unequivocally, that one operating point is better than another. In Fig. 9, OP has a desirably lower P_{fa} while OP' has a desirably higher P_d. Use of the proposed model of Eqs. (13), (14), (15) would result in an effective OP" somewhere on the dotted line between OP and OP'. For $\lambda=0.5$, the effective OP" would be the mid-point of this line segment. The selection of the preferred weighting λ and consequently the associated operation point is discussed in Section 3.5.

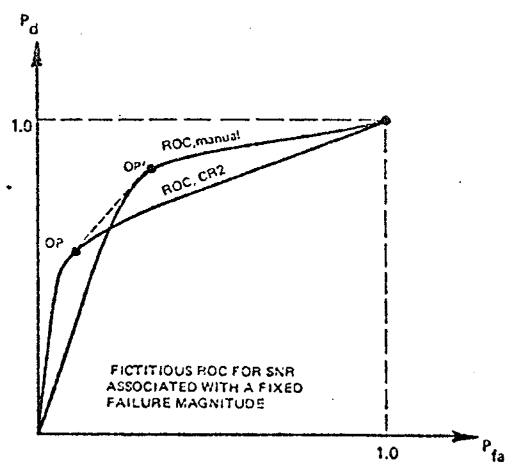


Figure 9 Representative ROC Underlying all Binary Detection Tests

3.4 USE OF OPERATOR TO INTERPRET RESULTS OF FAILURE DETECTION TESTS

Even though the decision rules of the INS2 failure detector, as presented in Section 3.3, are instantaneous rules, it is a common practice to allow a human operator to intervene in the interpretation of the outcome of the test before a switch is thrown. This procedure is followed for conservatism to exploit the useful adaptive capability of a human operator to pick out strong trends over a time interval and, in effect, to create a test with memory, rather than to let an automatic instantaneous computerized test, which could be subject to spurious noise transients, control the throwing of a switch. Use of the human operator in this way would change the effective P_d and P_{fa} characteristics of switch S' from what would be dictated by considering only the instantaneous P_d and P_{fa} characteristics of the CR2 INS2 failure detector. However, once the effective P_d and P_{fa} of the human operator interpreting the results of the CR2 test over a time interval are evaluated, they may be substituted for P_{d}, CR2 and P_{fa}, CR2 in the availability analysis of Sections 3.1 and 3.2.

More realistic effective characteristic P_d and P_{fa}, which are associated with the human operator's use of the instantaneous CR2 INS2 failure detector test results to recognize trends over a time interval, may be obtained by solving an associated level-crossing problem (i.e., the crossing of the Gaussian-related scalar test statistic above the deterministic decision threshold level over a time interval). Usually level-crossing problems are not very tractable (Ref. 11); however, these interval probability calculations are presently being pursued with an analytically tractable upper bound (Ref. 12) which can be optimized to be as tight as possible to the objective interval probabilities through the vehicle of a standard quadratic programming problem (Ref. 13, 14). The quadratic programming problem arises naturally in a discrete-time mechanization of the upper bound.

The close connection between level-crossing problems and the test statistic crossing above a decision threshold was also recognized in Ref. 15, where a completely different failure detection approach was investigated. However, only the calculation of the expected level-crossing times were attempted there.

3.5 MECHANICS OF OPTIMAL POLICY SELECTION BASED ON ASYMPTOTIC AVAILABILITY

It is well-known that the reliability function (without repair) asymptotically goes to zero with increasing time (Ref. 2). It is also well-known that the availability function asymptotically goes to some constant positive value as time increases (Ref. 2). Applying this principle to $A_{1/2}(t)$* of Eq. (8) with the switch S' characterized by the proposed model of Eqs. (13), (14), (15) allows the evaluation of the asymptotic levels of $A_{1/2}(t)$ over a range of λ weightings between 0 and 1. The value of λ that yields the largest asymptotic $A_{1/2}(t)$ would be chosen and used in the decision rule of Eqs. (18), (19) as the optimal interfacing of the two techniques.

*$A_{1/2}(t)$ rather than $A_{1/1}(t)$ was chosen since it represents the principle objective of operating in the primary mode. The methodology is equally applicable to $A_{1/1}'(t)$ however and it is conceivable that $A_{1/1}'(t)$ would be used for the evaluation when interest is in having <u>any</u> good navigation information available.

4. SUMMARY AND CONCLUDING DISCUSSION

The principal objective was to specify and evaluate an INS2 failure detection method. The CR2 failure detection method was specified and its performance was first evaluated theoretically, then demonstrated through simulations. Finally, the CR2 failure detection method was used on real system data to demonstrate that the algorithm is robust enough to handle real world/model mismatches without false alarming while still maintaining the ability to detect failures that occur. The performance of the CR2 failure detection method on real data was consistent with the theoretical predictions. An abridged view of the CR2 failure detection technique and the milestone of achieving satisfactory performance with real data were given in Section 2.

Upon completion of the primary objective, it was then necessary to specify how the CR2 INS2 failure detector* should interface with the entire system, including any additional INS2 failure detection aids (manual or automatic) that are subsequently developed to help the navigation operator decide in what mode he should operate the system. It is also necessary to evaluate how the CR2 failure detector affects the whole three-INS complex. A rigorous theoretical framework was detailed in Section 3 for using the standard techniques of reliability theory to determine the effect of the characteristic P_d and P_{fa} of the CR2 failure detector on the

*Method applicable to any INS2 failure detection method that uses the same filter inputs as used by the CR2 test as long as the characterizing P_d and P_{fa} have been evaluated.

overall asymptotic availability of the three-INS complex. When interfacing with another INS2 failure detection method is required, the proposed new model of the effective P_d and P_{fa} characteristics associated with the switch, used as a standard model for human operator decisions, may be used to determine the optimum relative weightings between the two methods that achieves the highest asymptotic availability. The same relative weightings are also inherited by the two INS2 failure detection techniques in a joint implementation as discussed in Section 3.3.

When only one INS2 failure detector is used, the proposed new model for effective P_d and P_{fa} (for switch S' in mode selection) reduce to the standard model without controversy. Presently, there appears to be a scarcity of ROC data on human operator decisions on master INS1 selection. Hopefully, this void will be filled in the future through the compilation of adequate performance data and/or statistical design of experiments to quantitatively evaluate the effect of man-in-the-loop. The theoretical framework for quantitatively evaluating the effect of the CR2 INS2 failure detector has been completely worked out, but is waiting on the specification of P_d, P_{fa} characteristics for switch S since this switch (operator decision) is depended upon in both the primary and back-up mode of the three-INS complex and availability results obtained by proceeding without this critical information may be very misleading.

One methodology, recently proposed for modeling man-machine availability as an allocation problem (Ref. 16), allows several levels of complexity and additional realism such as:

- grade level and years of experience of each repairman
- number of repairmen assigned to each repair action
- time spent by each repairman on the repair .

However, dynamic programming is required to solve even the most simple non-degenerate problems within this framework. In spite of some relatively recent theoretical strides in the area of implementing dynamic programming algorithms (Ref. 17, 18, 19) to reduce the so-called "curse of dimensionality" associated with dynamic programming problems (Ref. 20), the implementation of a dynamic programming algorithm still remains a rather formidable problem and usually requires a large computer allotment. In contrast, the main computation required for the availability analysis of Section 3 is a relatively minor iteration of a sparse, constant coefficient, linear difference equation of medium order. A more detailed model may be obtained, using the technique of Section 3, by modeling more elements.

Theoretical strides have been made recently in applying the techniques of modern control to the problem of modeling the effect of the operator-in-the-loop on the performance of the overall system. Two different approaches which both make use of Kalman filters are:

(1) human operator modeling within the theoretical framework of an optimal stochastic regulator (Ref. 21, 22, 23)

(2) modeling of human operator remnants using maximum likelihood methods for parameter identification (Ref. 24, 25).

It is anticipated that these new modeling approaches will yield more accurate final evaluations of the effective P_d and P_{fa} of the human operators.

The methodology discussed in this paper may also have potential application to those USAF situations in which a human operator must decide between two or more INS or navigation aids such as in:

- the C-141 dual IMU installation
- the C-5 planned retrofit
- the B-1 .

REFERENCES

1. Nash, R.A., Kasper, J.F., et al, "Applications of Optimal Smoothing to the Testing and Evaluation of Inertial Navigation Systems and Components," IEEE Transactions on Automatic Control, Vol. AC-16, No. 6, 1971.

2. Shooman, M.L., Probabilistic Reliability: An Engineering Approach, McGraw-Hill Book Company, New York, 1968.

3. Kerr, T.H., "A Two Ellipsoid Overlap Test for Real-Time Failure Detection and Isolation by Confidence Regions," Proceedings of the Fifth Annual Pittsburgh Conference on Modeling and Simulation, Part 2, p.1003, 1974, (a short working paper).

4. Kerr, T.H., "A Two Ellispoid Overlap Test for Real-Time Failure Detection and Isolation by Confidence Regions," Proceedings of the Conference on Decision and Control, pp.735-742, 1974.

5. Kerr. T.H., "Real-Time Failure Detection: A Static Nonlinear Optimization Problem That Yields a Two Ellipsoid Overlap Test," to appear in the Journal of Optimization Theory and Applications.

6. Kerr, T.H., "Applying Stochastic Integral Equations to Solve a Particular Stochastic Modeling Problem," Ph.D. Thesis, University of Iowa, 1971.

7. Van Trees, H.L., Detection, Estimation and Modulation Theory; Part I: Detection, Estimation, and Linear Modulation Theory, John Wiley and Sons, Inc., New York, 1968.

8. Schweppe, F.C., Uncertain Dynamic Systems, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1973.

9. Hartman, P.D., "On the Theory of Confidence Set Estimation and Detection," Ph.D. Thesis, Polytechnic Institute of Brooklyn, 1972.

10. Nakagawa, T. and Osaki, S., "Stochastic Behavior of 2-Unit Standby Redundant Systems with Imperfect Switch-Over," IEEE Transactions on Reliability, Vol. R-24, No. 2, June 1975.

11. Wong, E., "Recent Progress in Stochastic Processes - A Survey," IEEE Transactions on Information Theory, Vol. IT-19, No. 3, May 1973.

12. Gallager, R.G., and Helstrom, C.W., "A Bound on the Probability that a Gaussian Process Exceeds a Given Function," IEEE Transactions on Information Theory, Vol. IT-15, No. 1, January 1969.

13. Boot, J.C.G., Quadratic Programming: Algorithms-Anomalies-Applications, Rand McNally and Company, Chicago, Illinois, 1964.

14. Fletcher, R., "A FORTRAN Subroutine for General Quadratic Programming," Harwell Report, No. AERE.6370, United Kingdom Atomic Energy Research Group, June 1970.

15. Hines. W.G.S., "A Simple Monitor of a System with Sudden Parameter Changes," IEEE Transactions on Information Theory, Vol. IT-22, No. 2, March 1976.

16. LaSala, K.P., Siegal, A.I., et al, "Allocation of Man-Machine Reliability," Proceedings of 1976 Annual Reliability and Maintainability Symposium, Las Vegas, Nevada, 1976.

17. Larson, R.E., State Increment Dynamic Programming, American Elsevier Press, New York, 1967 .

18. Larson, R.E. and Korsak, A.J., "A Dynamic Programming Successive Approximations Technique with Convergence Proofs," Automatica, Vol. 6, No. 2, March 1970.

19. Bertsekas, D.P., Dynamic Programming and Stochastic Control, Academic Press, New York, 1976.

20. Bellman, R., Introduction to Matrix Analysis, McGraw-Hill Book Company, New York, 1970.

21. Kleinman, D.L., Baron, S., et al, "An Optimal Control Model of Human Response, Part I: Theory and Validation," Automatica, Vol. 6, 1970.

22. Kleinman, D.L., Perkins, T.R., "Modeling Human Performance in a Time-Varying Aircraft Tracking Loop," IEEE Transactions on Automatic Control, Vol. AC-19, No. 4, August 1974.

23. Broussard, J.R., Stengel, R.F., "Stability of the Pilot Aircraft System in Maneuvering Flight," to appear in Proceedings of the Twelfth Annual Conference on Manual Control, University of Illinois at Urbana-Champaign, May 25-27, 1976.

24. Sheridan, T.B., Ferrell, W.R., Man Machine Systems, MIT Press, Cambridge, Mass., 1974.

25. Repperger, D.W., Junker, A.M., A Maximum Likelihood Approach for Identifying Human Operator Remnant in a Tracking Task," Proceedings of the Conference on Decision and Control, Houston, Texas, 1975.